tyco | Software House

C•CURE 9000 Version 2.60 Service Pack 3

Release Note

Applicable Software	Product Data
C•CURE 9000 Version 2.60	Visit the C•CURE 9000 section of the Software House website http://www.swhouse.com/Support/SoftwareDownloads.aspx to download product critical updates, service packs, and release notes.

August 2019

NOTE: In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Contents

This release note provides important information for installing C•CURE 9000 Version 2.60 Service Pack 3, for server and client computers.

Service Pack Overview

This service pack provides software improvements for C•CURE 9000 Version 2.60, and can be applied as a minor version update, without the impact of major version upgrades. Service packs contain no database changes or modifications that can break external integrations. For further information refer to the Service Pack Improvements section.

This service pack contains the following categories of modifications:

- **Key Fixes** – applicable to the majority of installed systems.

Service pack content is driven by our Customer Support team and prioritized by severity, impact, and overall customer needs through our Software Problem Action Request (SPAR) process. Each modification contained in this Service Pack is identified with a SPAR number within the SPAR tables.

Requirements

This service pack for C•CURE 9000 Version 2.60 requires the following software:

- C•CURE 9000 Security and Event Management System version 2.60.
- iSTAR Ultra Firmware version 6.6.5 and ICU version 6.6.5.

Contents of the Service Pack

The installation media contains the following files:

- **2.60_SP3.exe** – the service pack software installer.
- **UnifiedLanguagePack.msi** – Unified language pack installer.
- **CC9K-v2-60-SP3-RN-8200-1367-65-A0-en.pdf** – this release note file.
- **CC9K-v2-60-SP3-RN-8200-1367-65-A0-en.pdf** – C•CURE Web release note file.
- **CC9K-v2-60-CumRN-8200-1367-00-A0-en** – C•CURE v2.70 cumulative release note file.

The Manuals folder contains all of the user guides for this release.

Installing the Service Pack

NOTE: C•CURE 9000 v2.60 must be properly installed for this service pack to install and run properly.

On the C•CURE 9000 Server:

1. Log off and exit the C•CURE 9000 Administration Workstation on the server and all clients.
2. Log off and exit the C•CURE 9000 Monitoring Station on the server and all clients.
3. On the server computer, use the Server Management application to stop the CrossFire Framework Service and the CrossFire Server Component Framework Service, and then exit the application.
4. Download the C•CURE 9000 service pack to the server computer.
5. Install the C•CURE 9000 service pack update by double-clicking on **2.60_SP3.exe** on the root level of the media.
6. Follow the installation instructions on screen to complete the C•CURE 9000 service pack install.

On the C•CURE 9000 Client:

1. Log off and exit the C•CURE 9000 Administration Workstation on the client.
2. Log off and exit the C•CURE 9000 Monitoring Station on the client.
3. Download the C•CURE 9000 service pack to the client.
4. Install C•CURE 9000 service pack update by double-clicking on **2.60_SP3.exe** on the root level of the media.
5. Click **Install** to complete C•CURE 9000 service pack install.

Uninstalling the Service Pack

NOTE: If you uninstall this service pack, both C•CURE 9000 Client and victor Application Server will be removed and the C•CURE 9000 installation will revert to its previous SP state. If critical updates were previously applied to this original SP state, they need to be reapplied.

1. Log off and exit the C•CURE 9000 Administration Workstation on the server and all clients.
2. Log off and exit the C•CURE 9000 Monitoring Station on the server and all clients.
3. Through the Server Management application, stop the CrossFire Framework Service and the Server Component Framework Service, then exit the application.
4. Run **2.60_SP3.exe** from the original C•CURE 9000 2.60 Service Pack 3 media.
5. Click **Remove**.

Alternatively, you can manually uninstall the client and server components of this service pack separately.

NOTE: If you uninstall the client and server components separately you must remove the Service Pack from both the client and server components to ensure the versions correspond correctly.

1. Log off and exit the C•CURE 9000 Administration Workstation on the server and all clients.
2. Log off and exit the C•CURE 9000 Monitoring Station on the server and all clients.
3. Through the Server Management application, stop the CrossFire Framework Service and the Server Component Framework Service, then exit the application.
4. Navigate to **Control Panel>Programs and Features>View Installed Updates**.
5. Select C•CURE 9000 Client 2.60 SP3 and click **Uninstall**.
6. Select victor Application Server 3.52 SP3 and click **Uninstall**.
7. If C•CURE GO Web Service is installed, select C•CURE GO Web Service 2.60 SP3 and click **Uninstall**.
8. If victor Client is installed, select victor Client 5.2 SP3 and click **Uninstall**.
   Rebooting may be required after uninstallation is complete.

Versions for C•CURE 9000 Software and Service Packs

Table 1: Version matrix shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help>About** for the Administration Client and Monitoring Workstation Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

C•CURE 9000 Version 2.60 Service Pack 3 includes all fixes released in prior updates listed in Table 1: Version Matrix.

Table 1: Version matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1236.442	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2
2.60 SP2 CU01	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU01
2.60 SP2 CU02	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU02
2.60 SP2 CU03	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU03
2.60 SP2 CU04	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU04
2.60 SP2 CU05	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU05
2.60 SP2 CU06	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU06
2.60 SP2 CU07	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU07
2.60 SP3	2.60.6008.0603	2.60.6008.0603	3.52.3006.603	C•CURE 9000 Client 2.60 SP3

Service Packs Improvements

This service pack includes the following updates and enhancements. SPAR numbers are included in Table 2: Enhancements, Table 3: Key Fixes.

Key Fixes

Key fixes are applicable to the majority of installed systems.

Table 3: Key fixes

Category	SPAR Number	SPAR Description
Administration and Monitoring Stations	455348	Export properties remain consistent when editing export report settings for multiple Run Report actions within the Event editor.
	535882	An issue which caused some Monitoring Stations to stop working unexpectedly has been resolved.
	534673	Events configured with the action “Play Sound Once” correctly play the required sound.
	562283	Image capture field in Personnel record displays correct information when Images and Badging fields are combined in one tab.
	571417	Audits on more than 2000 records are divided into object chunks of 2000 records to enable successful auditing of large records.
	444384	Event sounds and wav files do not play when Events are in maintenance mode.
	516891	Assigning a Clearance to a Personnel file which already contains that Clearance does not cause an error.
	537810	An issue which caused the Monitoring Station to close if you click on the “V” symbol on the Swipe and Show window has been resolved.

	520203	An issue which prevented data from being automatically refreshed in the Dynamic View has been resolved.
	575534	Doors shown in the Dynamic View correspond to the correct SAS.
	612128	Multiple clusters can be copied and pasted between Dynamic Views.
	602779	Drag and drop operations which encounter errors are cancelled and an error message is displayed.
	609511	SMTP email errors have been resolved.
	614966	Re-enabling a disabled credential after enabling Synchronization Operations using the checkbox facility does not cause a databased error.
	613431	Intrusion Zone mode status is updated correctly when IZ Arm event is downloaded to iSTAR Edge.
Anti-Passback	602015	Antipassback grace works as expected when using Swipe and Show within an overlay.
	555144	De-mustered cards are not rejected for tailgating.
Application Server	517458	C•CURE database backup errors on systems set to use French as the display language have been resolved.
	566106	The High Activity Monitor does not disrupt editing global objects from a SAS-connected client.
Credentials	614932	Access cards are disabled by inactivity after the card's activation date.
CrossFire Server	591091	Tracing when MAS clients generate errors after server reboot has been improved.
	542153	CrossFire server starts successfully when Tyco Web Bridge is in Start Pending mode.
	551398	Audit synchronization maintains speed during a large synchronization.
Cybersecurity	573171	Impersonation service only responds to local requests.
	561491	Security vulnerabilities have been addressed.
Import/Export	601738	Copy/Paste import includes Events linked to Existing Door objects.
	512328	Folder on Server path field displays the correct data import path.
iSTAR Driver	518560	C•CUREProToSEConvertUtility converts iSTAR Pro panels to iSTAR Ultra SE panels as expected.
	535719	Supervising Resistor Configuration is correctly transferred by the iSTAR Pro To Ultra Conversion Utility.
	561938	An issue which caused personnel downloads to fail on iSTAR controllers has been resolved.
	567837	An issue which caused the iSTAR driver to crash and not recover unless the OS was restarted has been resolved.
	587224	iSTAR Pro host name cannot be overwritten.

	587640	Changing cluster names using two different Operators does not affect communications state.
	591633	An issue which caused SQL compact database to crash has been resolved.
	593738	iSTAR driver does not cause CPU usage spikes.
	593753	Resetting a card for GAPB does not cause the iSTAR driver to enter a dead lock state.
	543519	Credentials added to a record using a client station in a different timezone to the panel are applied successfully.
Journal/Audit	513003	Crossfire memory usage remains stable during journal log sync.
	551532	All conditions which cause Journal or Audit sync to abort are logged.
	573362	Operators who cancel manual actions are including in the audit log.
Licensing	610517	License counts are correct after service restarts.
Operators/Privileges	507219	Service account Operator privileges cannot be modified while CrossFire is running.
	572288	Privilege behavior is consistent for different Operators.
	557863	Operators with privilege to assign or remove clearances can perform edit actions.
	603955	Context menu items are displayed as correctly as per Privilege.
Personnel	542618	The Credential tab and badge layouts work as expected when editing a Personnel record.
	554801	Credential status colors work as expected.
	523887	Modifications made to credentials are retained, as expected, when subsequent credentials are modified.
	613761	The Clearances column in the Personnel editor can be resized.
Queries/Reports	519070	The SWH06 Door Access Report and SWHrep0506 Query have been modified to ensure that they conform to the timeframe of report parameters.
Sync Conflicts	542679	Changing an audit synchronization block size no longer requires the Crossfire service to be restarted.
VideoEdge	524618	An issue which caused the VideoEdge Driver Service to stop unexpectedly has been resolved.
Visitor Management	538070	Visitor Management generates correct metadata for ICS files to be imported to Google Calendar.

Multi-version Support

C•CURE 9000 provides multi-version support. This is the ability for SAS systems not yet upgraded to the version the MAS is running to connect to the MAS, synchronize records, and identify conflicts, and attach clients to the MAS to configure and monitor the Enterprise. From the MAS perspective, a Global Operator has the ability to attach to both upgraded and non-upgraded SAS systems, with some limitations due to the version differences.

The multi-version process begins with an enterprise where the MAS and every SAS is currently at the same version, and the MAS is upgraded. Therefore, only two versions of C•CURE 9000 can be involved:

- The new version to which the MAS has been upgraded.
- The previous version at which all SAS systems were operating.

If an enterprise currently has a MAS at one version and SAS systems with differing versions, it is necessary to update all SAS systems to be at the same version as the MAS to establish a common baseline, prior to beginning to upgrade the MAS to take advantage of Multi-version support.

The intention still is to proceed with upgrading every SAS to match the new MAS version. The difference is that, until that point, all the SAS systems can participate in the enterprise, within version-specific limitations.
To enable upgraded clients to communicate with previous version SAS systems, during the upgrade a copy is made of the C•CURE 9000 client applications from the previous version so that these applications can be launched when needed if the upgraded client detects it is running in a multi-version enterprise.
For a complete list of Multi-version Support limitations, refer to the *C•CURE 9000 Enterprise Architecture Guide*.

Finding More Information

Technical Support Portal
The Technical Support Portal provides knowledge-based articles, technical documents, and tips to install and use Software House products.

Qualified Integrators can register to access the Technical Support Portal at http://www.swhouse.com. Click Support and select Support Portal to access the Support Portal log in page.

The email address you use to register for access to the portal must be the same one you used for the certification course.
If the request is approved, log in credentials are emailed 24 to 48 hours after received.

User Guides
The user guides are located in the Manuals folder included on the installation media.

End of Release Notes

Software House C•CURE 9000 Version 2.60 SP2 Critical Update 10 (Unified 3.52 SP2 CU10)

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 10 (Unified 3.52 SP2 CU10) Release Note
August 2019

This release note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 10 on C•CURE 9000 Server and Client machines. This release note also provides important information for uninstalling C•CURE AutoUpdate and C•CURE AutoUpdate services.

In case of discrepancy, the information in this document supersedes the information in any document referenced herein. Read this release note before installing the product.

Contents

Versions for C•CURE 9000 Software and Service Packs

Table 1: Version Matrix shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 10 includes all fixes released in the Critical Updates and Service Packs listed in Table 1: Version Matrix.

Table 1: Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1236.442	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2
2.60 SP2 CU01	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU01
2.60 SP2 CU02	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU02
2.60 SP2 CU03	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU03
2.60 SP2 CU04	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU04
2.60 SP2 CU05	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU05

2.60 SP2 CU06	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU06
2.60 SP2 CU07	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU07
2.60 SP2 CU08	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU08
2.60 SP2 CU09	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU09
2.60 SP2 CU10	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU10

Installing the Critical Update

Follow the steps below to install this critical update on both C•CURE 9000 servers and clients.

NOTE: Ensure to update victor Web Service before proceeding to install the Critical Update .exe file.

Updating victor Web Service:

1. Start the victor Web Service update by double clicking on **setup.exe** in the CrossFireWebService folder.
2. Follow the installation instructions on screen to complete victor Web Service update install.
3. Reboot your machine if prompted to do so.

On a C•CURE 9000 server:

1. Log out and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU10.exe**.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

Log off and exit the C•CURE 9000 Administration application on the client machine.

1. Log off and exit the C•CURE 9000 Monitoring Station application on the client machine.
2. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU10.exe**.
3. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
4. Reboot your machine if prompted to do so.

Uninstalling the Critical Update

NOTE: If you uninstall this Critical Update, the system reverts back to the previous C•CURE 9000 state.

To uninstall the Critical Update on the C•CURE 9000 server or client:

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station application.
3. In the Server Configuration application, click **Stop** in the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP2CU10.exe** from the C•CURE 9000 2.60 Service Pack 2 Critical Update 10 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station application.

3. In the Server Configuration application, click **Stop** in the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP2 CU10** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP2 CU10** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you must manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

Performing a Silent Uninstall:

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station application.
3. Hold the shift key and right-click the **2.60 SP2 CU10** update folder. Click **Open command window here**.
4. In the command window, type 2.60_SP2CU10.exe /q /x and press Enter.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

AutoUpdate

If you are not using the C•CURE Client AutoUpdate feature, Software House recommends that you uninstall the AutoUpdate Services included with C•CURE Client. You can uninstall this feature during the Critical Update installation or by running the AutoUpdateRemover.exe file without installing this Critical Update.

This critical update automatically disables the following C•CURE Client AutoUpdate Services:

- Software House AutoUpdate Service.
- Software House AutoUpdate Installer.

If C•CURE AutoUpdate is installed on your server, you can uninstall it during the critical update installation process. This will also delete the C•CURE Client AutoUpdate services listed above.

If C•CURE AutoUpdate is not installed, but the C•CURE Client AutoUpdate Services listed above are installed on your machine, you can delete these services during the critical update installation process.

Uninstalling C•CURE Client AutoUpdate or AutoUpdate Services during the Critical Update installation process:

C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled or deleted during the installation process of this critical update.

1. Start the C•CURE 9000 Critical Update by double clicking on **2.60_SP2CU10.exe**.
2. Click **Install**.
3. A dialog box displays one of the following queries:
   "C•CURE AutoUpdate is installed. Would you like to uninstall AutoUpdate?"
   OR
   "Would you like to delete the C•CURE Client AutoUpdate Services?"
4. Click **Yes** and continue with the installation process.

Uninstalling C•CURE Client AutoUpdate or AutoUpdate Services using AutoUpdateRemover.exe:

C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled using AutoUpdateRemover.exe without installing the Critical Update file or at any time after the installation of the Critical Update.

1. Start AutoUpdateRemover by double clicking on **AutoUpdateRemover.exe.**
2. A command window displays stating: `Uninstall CCure AutoUpdate(Y/N)?`
3. To uninstall, type `Y`, then press enter. AutoUpdate is uninstalled.

SPARs Fixed

This Critical Update includes a security update and SPAR fix as described in Table 2: SPAR Table.

Table 2: SPAR Table

SPAR Number	SPAR Description
602878	A warning is displayed on the iSTAR Ultra controller configuration screen reminding users that network configuration can only be completed via ICU or the iSTAR webpage for panels running firmware 6.6.5 or later.
603120	An issue which caused iSTAR drivers to enter a one-way communication state has been resolved.
626561	Host events are logged correctly to the journal, as expected.

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP2 Critical Update 09 (Unified 3.52 SP2 CU09)

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 09 (Unified 3.52 SP2 CU09) Release Note
June 2019

This release note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 09 on C•CURE 9000 Server and Client machines. This release note also provides important information for uninstalling C•CURE AutoUpdate and C•CURE AutoUpdate services.

In case of discrepancy, the information in this document supersedes the information in any document referenced herein. Read this release note before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

Table 1: Version Matrix shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 09 includes all fixes released in the critical updates and service packs listed in Table 1: Version Matrix.

Table 1: Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1236.442	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2
2.60 SP2 CU01	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU01
2.60 SP2 CU02	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU02
2.60 SP2 CU03	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU03
2.60 SP2 CU04	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU04
2.60 SP2 CU05	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU05
2.60 SP2 CU06	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU06

2.60 SP2 CU07	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU07
2.60 SP2 CU08	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU08
2.60 SP2 CU09	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU09

2. Installing the Critical Update

Follow the steps below to install this critical update on both C•CURE 9000 servers and clients.

NOTE: C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled during the Critical Update installation process. For more information see Section 4: AutoUpdate.

On a C•CURE 9000 server:

1. Log out and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU09.exe**.
   NOTE: You may be prompted to uninstall AutoUpdate during the installation process. For more information see Section 4: AutoUpdate.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log off and exit the C•CURE 9000 Administration application on the client machine.
2. Log off and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU09.exe**.
   NOTE: You may be prompted to uninstall AutoUpdate during the installation process. For more information see Section 4: AutoUpdate.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

Performing a Silent Install:

1. Log off and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log off and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. Hold the shift key and right-click the 2.60 SP2 CU09 update folder. Click **Open command window here**.
4. In the command window, type `2.60_SP2CU09.exe /q` and press **Enter.**
5. View installation progress in the **UnifiedPatch log**.

3. Uninstalling the Critical Update

NOTE: If you uninstall this Critical Update, the system reverts back to the previous C•CURE 9000 state. To uninstall the Critical Update on the C•CURE 9000 server or client:

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, click **Stop** in the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP2CU09.exe** from the C•CURE 9000 2.60 Service Pack 2 Critical Update 09 media.

5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, click **Stop** in the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP2 CU09** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP2 CU09** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you must manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

Performing a Silent Uninstall:

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. Hold the shift key and right-click the **2.60 SP2 CU09** update folder. Click **Open command window here**.
4. In the command window, type `2.60_SP2CU09.exe /q /x` and press Enter.

4. AutoUpdate

If you are not using the C•CURE Client AutoUpdate feature, Software House recommends that you uninstall the AutoUpdate Services included with C•CURE Client. You can uninstall this feature during the Critical Update installation or by running the AutoUpdateRemover.exe file without installing this Critical Update.

This critical update automatically disables the following C•CURE Client AutoUpdate Services:

- Software House AutoUpdate Service.
- Software House AutoUpdate Installer.

If C•CURE AutoUpdate is installed on your server, you can uninstall it during the critical update installation process. This will also delete the C•CURE Client AutoUpdate services listed above.

If C•CURE AutoUpdate is not installed, but the C•CURE Client AutoUpdate Services listed above are installed on your machine, you can delete these services during the critical update installation process.

Uninstalling C•CURE Client AutoUpdate or AutoUpdate Services during the Critical Update installation process:
C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled or deleted during the installation process of this critical update.

1. Start the C•CURE 9000 Critical Update by double clicking on **2.60_SP2CU09.exe**.
2. Click **Install**.
3. A dialog box displays one of the following queries:

"C•CURE AutoUpdate is installed. Would you like to uninstall AutoUpdate?"

OR

"Would you like to delete the C•CURE Client AutoUpdate Services?"

4. Click **Yes** and continue with the installation process.

Uninstalling C•CURE Client AutoUpdate or AutoUpdate Services using AutoUpdateRemover.exe:
C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled using AutoUpdateRemover.exe without installing the Critical Update file or at any time after the installation of the Critical Update.

1. Start AutoUpdateRemover by double clicking on **AutoUpdateRemover.exe.**
2. A command window displays stating: `Uninstall CCure AutoUpdate(Y/N)?`
3. To uninstall, type `Y`, then press enter. AutoUpdate is uninstalled.

5. SPARs Fixed

This Critical Update includes a security update and SPAR fixes as described in Security Update and Table 2: SPAR Table. This Critical Update also fixes a Microsoft Windows Update-related issue described in the section Microsoft Update-related SPAR fix.

Security Update

This Critical Update contains security updates related to the AutoUpdate service.

Table 2: SPAR Table

SPAR Number	SPAR Description
591441	Host Event activation messages match Input activation.
602878	A warning is displayed on the iSTAR Ultra controller configuration screen reminding users that network configuration can only be completed via ICU or the iSTAR webpage for panels running firmware 6.6.5 or later.
603120	An issue which caused iSTAR drivers to enter a one-way communication state has been resolved.
611571	This critical update includes TycoESS.

Microsoft Windows Update-related SPAR fix

Overview

Microsoft May 2018 Preview updates caused problems in C•CURE 9000 Client-Server and Server-Server communications. Installing Microsoft KBs at all client and server workstations solves this problem.

Microsoft August 2018 Preview updates cause similar problems in C•CURE 9000 Client-Server and Server-Server communications. Software House has worked with Microsoft to develop this Critical Update to provide a workaround to these Microsoft Windows Update defects.

Table 3: Solutions

Solution 1	Install Microsoft KBs at all client and server workstations simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.

Solution 2	Install this Critical Update on C•CURE 9000 servers. Microsoft Windows Updates can then be deployed on servers and clients as required and non-simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.

NOTE: The Microsoft Windows Update fix only requires installation of this Critical Update on C•CURE 9000 servers. To deploy this Critical Update's non-Microsoft client-side fixes, ensure to also install this Critical Update on C•CURE 9000 clients.

Microsoft Preview of Quality Rollup (KB) numbers are cross-referenced against their associated Windows operating systems in the Table 4: KB numbers. Install the relevant KBs for your operating system according to the solution you have chosen from Table 3: Solutions.

Table 4: KB Numbers

Operating System	Parent KB (Windows Update offering)	Child KB (displayed in *Installed Updates*)	
Windows Server 2008	4346083	2.0 =	4342308
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows 7 / Server 2008 R2	4346080	3.5.1 =	4342309
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows Server 2012	4346081	3.5 =	4342307
		4.5.2 =	4342318
		4.6.x/4.7.x =	4342314
Windows 8.1 / Server 2012 R2	4346082	3.5 =	4342310
		4.5.2 =	4342317
		4.6.x/4.7.x =	4342315
Windows 10 RS1 / Server 2016	4343884	Same as parent KB	
Windows 10 RS2	4343889	Same as parent KB	
Windows 10 RS3	4343893	Same as parent KB	
Windows 10 RS4	4346783	Same as parent KB	

NOTE: For full (updated) details, download Software House TAB SWH-TAB-000024206 from the Software House Support Portal (requires registration).

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP2 Critical Update 08 (Unified 3.52 SP2 CU08)

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 08 (Unified 3.52 SP2 CU08) Release Note
January 2019

This release note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 08 on C•CURE 9000 Server and Client machines. This release note also provides important information for uninstalling C•CURE AutoUpdate and C•CURE AutoUpdate services.

In case of discrepancy, the information in this document supersedes the information in any document referenced herein. Read this release note before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

Table 1: Version Matrix shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 08 includes all fixes released in the Critical Updates and Service Packs listed in *Table 1: Version Matrix*.

Table 1: Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1236.442	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2
2.60 SP2 CU01	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU01
2.60 SP2 CU02	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU02
2.60 SP2 CU03	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU03
2.60 SP2 CU04	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU04
2.60 SP2 CU05	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU05
2.60 SP2 CU06	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU06

2.60 SP2 CU07	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU07
2.60 SP2 CU08	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU08

2. Installing the Critical Update

Follow the steps below to install this critical update on both C•CURE 9000 servers and clients.

NOTE: C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled during the Critical Update installation process. For more information see *Section 4: AutoUpdate*.

On a C•CURE 9000 server:

1. Log out and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU08.exe**.
   NOTE: You may be prompted to uninstall AutoUpdate during the installation process. For more information see *Section 4: AutoUpdate*.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log off and exit the C•CURE 9000 Administration application on the client machine.
2. Log off and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU08.exe**.
   NOTE: You may be prompted to uninstall AutoUpdate during the installation process. For more information see *Section 4: AutoUpdate*.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

Performing a Silent Install:

1. Log off and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log off and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. Hold the shift key and right-click the 2.60 SP2 CU08 update folder. Click **Open command window here**.
4. In the command window, type `2.60_SP2CU08.exe /q` and press **Enter.**
5. View installation progress in the **UnifiedPatch log**.

3. Uninstalling the Critical Update

NOTE: If you uninstall this Critical Update, the system reverts back to the previous C•CURE 9000 state. To uninstall the Critical Update on the C•CURE 9000 server or client:

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, click **Stop** in the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP2CU08.exe** from the C•CURE 9000 2.60 Service Pack 2 Critical Update 08 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, click **Stop** in the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP2 CU08** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP2 CU08** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you must manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

Performing a Silent Uninstall:

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. Hold the shift key and right-click the **2.60 SP2 CU08** update folder. Click **Open command window here**.
4. In the command window, type `2.60_SP2CU08.exe /q /x` and press Enter.

4. AutoUpdate

If you are not using the C•CURE Client AutoUpdate feature, Software House recommends that you uninstall the AutoUpdate Services included with C•CURE Client. You can uninstall this feature during the Critical Update installation or by running the AutoUpdateRemover.exe file without installing this Critical Update.

This Critical Update automatically disables the following C•CURE Client AutoUpdate Services:

- Software House AutoUpdate Service.
- Software House AutoUpdate Installer.

If C•CURE AutoUpdate is installed on your server, you can uninstall it during the Critical Update installation process. This will also delete the C•CURE Client AutoUpdate services listed above.

If C•CURE AutoUpdate is not installed, but the C•CURE Client AutoUpdate Services listed above are installed on your machine, you can delete these services during the Critical Update installation process.

Uninstalling C•CURE Client AutoUpdate or AutoUpdate Services during the Critical Update installation process:
C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled or deleted during the installation process of this Critical Update.

1. Start the C•CURE 9000 Critical Update by double clicking on **2.60_SP2CU08.exe**.
2. Click **Install**.
3. A dialog box displays stating one of the following:
   "C•CURE AutoUpdate is installed. Would you like to uninstall AutoUpdate?"
   OR

"Would you like to delete the C•CURE Client AutoUpdate Services?"

4. Click **Yes** and continue with the installation process.

Uninstalling C•CURE Client AutoUpdate or AutoUpdate Services using AutoUpdateRemover.exe:
C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled using AutoUpdateRemover.exe without installing the Critical Update file or at any time after the installation of the Critical Update.

1. Start AutoUpdateRemover by double clicking on **AutoUpdateRemover.exe.**
2. A command window displays stating: `Uninstall CCure AutoUpdate(Y/N)?`
3. To uninstall, type `Y`, then press enter. AutoUpdate is uninstalled.

5. SPARs Fixed

This Critical Update includes a security update and SPAR fixes as described in *Security Update* and *Table 2: SPAR Table*. This Critical Update also fixes a Microsoft Windows Update-related issue described in the section *Microsoft Update-related SPAR fix*.

Security Update

This Critical Update contains security updates related to the AutoUpdate service.

Table 2: SPAR Table

SPAR Number	SPAR Description
595861	Resetting a card does not cause iSTAR driver to enter a dead lock state.
596618	IP Address text box can now contain 100 characters.

Microsoft Windows Update-related SPAR fix

Overview

Microsoft May Preview updates caused problems in C•CURE 9000 Client-Server and Server-Server communications. Installing Microsoft KBs at all client and server workstations solved this problem.

Microsoft August Preview updates cause similar problems in C•CURE 9000 Client-Server and Server-Server communications. Software House has worked with Microsoft to develop this Critical Update to provide a workaround to these Microsoft Windows Update defects.

Table 3: Solutions

Solution 1	Install Microsoft KBs at all client and server workstations simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.
Solution 2	Install this Critical Update on C•CURE 9000 servers. Microsoft Windows Updates can then be deployed on servers and clients as required and non-simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.

NOTE: The Microsoft Windows Update fix only requires installation of this Critical Update on C•CURE 9000 servers. To deploy this Critical Update's non-Microsoft client-side fixes, ensure to also install this Critical Update on C•CURE 9000 clients.

Microsoft Preview of Quality Rollup (KB) numbers are cross-referenced against their associated Windows operating systems in the *Table 4: KB numbers*. Install the relevant KBs for your operating system according to the solution you have chosen from *Table 3: Solutions*.

Table 4: KB Numbers

Operating System	**Parent KB (Windows Update offering)**	**Child KB (displayed in *Installed Updates*)**	
Windows Server 2008	4346083	2.0 =	4342308
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows 7 / Server 2008 R2	4346080	3.5.1 =	4342309
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows Server 2012	4346081	3.5 =	4342307
		4.5.2 =	4342318
		4.6.x/4.7.x =	4342314
Windows 8.1 / Server 2012 R2	4346082	3.5 =	4342310
		4.5.2 =	4342317
		4.6.x/4.7.x =	4342315
Windows 10 RS1 / Server 2016	4343884	Same as parent KB	
Windows 10 RS2	4343889	Same as parent KB	
Windows 10 RS3	4343893	Same as parent KB	
Windows 10 RS4	4346783	Same as parent KB	

NOTE: For full (updated) details, download Software House TAB SWH-TAB-000024206 from the Software House Support Portal (requires registration).

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP2 Critical Update 07 (Unified 3.52 SP2 CU07)

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 07 (Unified 3.52 SP2 CU07) Release Note
December 2018

This release note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 07 on C•CURE 9000 Server and Client machines. This release note also provides important information for uninstalling C•CURE AutoUpdate and C•CURE AutoUpdate services.

In case of discrepancy, the information in this document supersedes the information in any document referenced herein. Read this release note before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

Table 1: Version Matrix shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 07 includes all fixes released in the Critical Updates and Service Packs listed in *Table 1: Version Matrix*.

Table 1: Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1236.442	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2
2.60 SP2 CU01	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU01
2.60 SP2 CU02	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU02
2.60 SP2 CU03	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU03
2.60 SP2 CU04	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU04
2.60 SP2 CU05	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU05
2.60 SP2 CU06	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU06

2.60 SP2 CU07	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU07

2. Installing the Critical Update

Follow the steps below to install this critical update on both C•CURE 9000 servers and clients.

NOTE: C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled during the Critical Update installation process. For more information see *Section 4: AutoUpdate*.

On a C•CURE 9000 server:

1. Log out and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU07.exe**.
   NOTE: You may be prompted to uninstall AutoUpdate during the installation process. For more information see *Section 4: AutoUpdate*.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log off and exit the C•CURE 9000 Administration application on the client machine.
2. Log off and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU07.exe**.
   NOTE: You may be prompted to uninstall AutoUpdate during the installation process. For more information see *Section 4: AutoUpdate*.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

Performing a Silent Install:

1. Log off and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log off and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. Hold the shift key and right-click the 2.60 SP2 CU07 update folder. Click **Open command window here**.
4. In the command window, type `2.60_SP2CU07.exe /q` and press **Enter.**
5. View installation progress in the **UnifiedPatch log**.

3. Uninstalling the Critical Update

NOTE: If you uninstall this Critical Update, the system reverts back to the previous C•CURE 9000 state. To uninstall the Critical Update on the C•CURE 9000 server or client:

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, click **Stop** in the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP2CU07.exe** from the C•CURE 9000 2.60 Service Pack 2 Critical Update 07 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, click **Stop** in the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP2 CU07** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP2 CU07** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you must manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

Performing a Silent Uninstall:

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. Hold the shift key and right-click the **2.60 SP2 CU07** update folder. Click **Open command window here**.
4. In the command window, type `2.60_SP2CU07.exe /q /x` and press Enter.

4. AutoUpdate

If you are not using the C•CURE Client AutoUpdate feature, Software House recommends that you uninstall the AutoUpdate Services included with C•CURE Client. You can uninstall this feature during the Critical Update installation or by running the AutoUpdateRemover.exe file without installing this Critical Update.

This Critical Update automatically disables the following C•CURE Client AutoUpdate Services:

- Software House AutoUpdate Service.
- Software House AutoUpdate Installer.

If C•CURE AutoUpdate is installed on your server, you can uninstall it during the Critical Update installation process. This will also delete the C•CURE Client AutoUpdate services listed above.

If C•CURE AutoUpdate is not installed, but the C•CURE Client AutoUpdate Services listed above are installed on your machine, you can delete these services during the Critical Update installation process.

Uninstalling C•CURE Client AutoUpdate or AutoUpdate Services during the Critical Update installation process:
C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled or deleted during the installation process of this Critical Update.

1. Start the C•CURE 9000 Critical Update by double clicking on **2.60_SP2CU07.exe**.
2. Click **Install**.
3. A dialog box displays stating one of the following:
   "C•CURE AutoUpdate is installed. Would you like to uninstall AutoUpdate?"
   OR

"Would you like to delete the C•CURE Client AutoUpdate Services?"

4. Click **Yes** and continue with the installation process.

Uninstalling C•CURE Client AutoUpdate or AutoUpdate Services using AutoUpdateRemover.exe:
C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled using AutoUpdateRemover.exe without installing the Critical Update file or at any time after the installation of the Critical Update.

1. Start AutoUpdateRemover by double clicking on **AutoUpdateRemover.exe.**
2. A command window displays stating: `Uninstall CCure AutoUpdate (Y/N)?`
3. To uninstall, type `Y`, then press enter. AutoUpdate is uninstalled.

5. SPARs Fixed

This Critical Update includes a security update and SPAR fixes as described in *Security Update* and *Table 2: SPAR Table*. This Critical Update also fixes a Microsoft Windows Update-related issue described in the section *Microsoft Update-related SPAR fix*.

Security Update

This Critical Update contains security updates related to the AutoUpdate service.

Table 2: SPAR Table

SPAR Number	SPAR Description
572342	Multiple clusters can be copied and pasted between Dynamic Views.
587215	iSTAR Pro host name cannot be overwritten.
587361	iSTAR driver does not cause CPU usage spikes.
587639	Crossfire maintains updates to iSTARs when internal notification queue is full.
588011	Controller does not change state when cluster is disabled and modified.
587223	Changing cluster names using two different Operators does not affect communications state.
593295	iSTAR driver hang on panel download has been mitigated.
593296	A lock has been added to SQL compact database files.

Microsoft Windows Update-related SPAR fix

Overview

Microsoft May Preview updates caused problems in C•CURE 9000 Client-Server and Server-Server communications. Installing Microsoft KBs at all client and server workstations solved this problem.

Microsoft August Preview updates cause similar problems in C•CURE 9000 Client-Server and Server-Server communications. Software House has worked with Microsoft to develop this Critical Update to provide a workaround to these Microsoft Windows Update defects.

Table 3: Solutions

Solution 1	Install Microsoft KBs at all client and server workstations simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.
Solution 2	Install this Critical Update on C•CURE 9000 servers. Microsoft Windows Updates can then be deployed on servers and clients as required and non-simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.

NOTE: The Microsoft Windows Update fix only requires installation of this Critical Update on C•CURE 9000 servers. To deploy this Critical Update's non-Microsoft client-side fixes, ensure to also install this Critical Update on C•CURE 9000 clients.

Microsoft Preview of Quality Rollup (KB) numbers are cross-referenced against their associated Windows operating systems in the *Table 4: KB numbers*. Install the relevant KBs for your operating system according to the solution you have chosen from *Table 3: Solutions*.

Table 4: KB Numbers

Operating System	Parent KB (Windows Update offering)	Child KB (displayed in *Installed Updates*)	
Windows Server 2008	4346083	2.0 =	4342308
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows 7 / Server 2008 R2	4346080	3.5.1 =	4342309
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows Server 2012	4346081	3.5 =	4342307
		4.5.2 =	4342318
		4.6.x/4.7.x =	4342314
Windows 8.1 / Server 2012 R2	4346082	3.5 =	4342310
		4.5.2 =	4342317
		4.6.x/4.7.x =	4342315
Windows 10 RS1 / Server 2016	4343884	Same as parent KB	
Windows 10 RS2	4343889	Same as parent KB	
Windows 10 RS3	4343893	Same as parent KB	
Windows 10 RS4	4346783	Same as parent KB	

NOTE: For full (updated) details, download Software House TAB SWH-TAB-000024206 from the Software House Support Portal (requires registration).

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP2 Critical Update 06 (Unified 3.52 SP2 CU06)

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 06 (Unified 3.52 SP2 CU06) Release Note
November 2018

This release note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 06 on C•CURE 9000 Server and Client machines. This release note also provides important information for uninstalling C•CURE AutoUpdate and C•CURE AutoUpdate services.

In case of discrepancy, the information in this document supersedes the information in any document referenced herein. Read this release note before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

Table 1: Version Matrix shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 06 includes all fixes released in the Critical Updates and Service Packs listed in *Table 1: Version Matrix*.

Table 1: Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1236.442	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2
2.60 SP2 CU01	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU01
2.60 SP2 CU02	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU02
2.60 SP2 CU03	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU03
2.60 SP2 CU04	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU04
2.60 SP2 CU05	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU05
2.60 SP2 CU06	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU06

2. Installing the Critical Update

Follow the steps below to install this critical update on both C•CURE 9000 servers and clients.

NOTE: C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled during the Critical Update installation process. For more information see *Section 4: AutoUpdate*.

On a C•CURE 9000 server:

1. Log out and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU06.exe**.
   NOTE: You may be prompted to uninstall AutoUpdate during the installation process. For more information see *Section 4: AutoUpdate*.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log off and exit the C•CURE 9000 Administration application on the client machine.
2. Log off and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU06.exe**.
   NOTE: You may be prompted to uninstall AutoUpdate during the installation process. For more information see *Section 4: AutoUpdate*.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

Performing a Silent Install:

1. Log off and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log off and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. Hold the shift key and right-click the 2.60 SP2 CU06 update folder. Click **Open command window here**.
4. In the command window, type `2.60_SP2CU06.exe /q` and press **Enter.**
5. View installation progress in the **UnifiedPatch log**.

3. Uninstalling the Critical Update

NOTE: If you uninstall this Critical Update, the system reverts back to the previous C•CURE 9000 state. To uninstall the Critical Update on the C•CURE 9000 server or client:

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, click **Stop** in the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP2CU06.exe** from the C•CURE 9000 2.60 Service Pack 2 Critical Update 06 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, click **Stop** in the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP2 CU06** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP2 CU06** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you must manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

Performing a Silent Uninstall:

1. Log off and exit the C•CURE 9000 Administration application.
2. Log off and exit the C•CURE 9000 Monitoring Station.
3. Hold the shift key and right-click the **2.60 SP2 CU06** update folder. Click **Open command window here**.
4. In the command window, type `2.60_SP2CU06.exe /q /x` and press Enter.

4. AutoUpdate

If you are not using the C•CURE Client AutoUpdate feature, Software House recommends that you uninstall the AutoUpdate Services included with C•CURE Client. You can uninstall this feature during the Critical Update installation or by running the AutoUpdateRemover.exe file without installing this Critical Update.

This Critical Update automatically disables the following C•CURE Client AutoUpdate Services:

- Software House AutoUpdate Service.
- Software House AutoUpdate Installer.

If C•CURE AutoUpdate is installed on your server, you can uninstall it during the Critical Update installation process. This will also delete the C•CURE Client AutoUpdate services listed above.

If C•CURE AutoUpdate is not installed, but the C•CURE Client AutoUpdate Services listed above are installed on your machine, you can delete these services during the Critical Update installation process.

Uninstalling C•CURE Client AutoUpdate or AutoUpdate Services during the Critical Update installation process:
C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled or deleted during the installation process of this Critical Update.

1. Start the C•CURE 9000 Critical Update by double clicking on **2.60_SP2CU06.exe**.
2. Click **Install**.
3. A dialog box displays stating one of the following:
   "C•CURE AutoUpdate is installed. Would you like to uninstall AutoUpdate?"
   OR
   "Would you like to delete the C•CURE Client AutoUpdate Services?"
4. Click **Yes** and continue with the installation process.

Uninstalling C•CURE Client AutoUpdate or AutoUpdate Services using AutoUpdateRemover.exe:
C•CURE Client AutoUpdate and AutoUpdate Services can be uninstalled using AutoUpdateRemover.exe without installing the Critical Update file or at any time after the installation of the Critical Update.

1. Start AutoUpdateRemover by double clicking on **AutoUpdateRemover.exe.**
2. A command window displays stating: `Uninstall CCure AutoUpdate (Y/N)?`
3. To uninstall, type `Y`, then press enter. AutoUpdate is uninstalled.

5. SPARs Fixed

This Critical Update includes a security update and SPAR fixes as described in *Security Update* and *Table 2: SPAR Table*. This Critical Update also fixes a Microsoft Windows Update-related issue described in the section *Microsoft Update-related SPAR fix*.

Security Update

This Critical Update contains security updates related to the AutoUpdate service.

Table 2: SPAR Table

SPAR Number	SPAR Description
570307	DBManager runs as expected during installation.
572916	All Door Groups can be excluded from Doors selection for a Clearance.

Microsoft Windows Update-related SPAR fix

Overview

Microsoft May Preview updates caused problems in C•CURE 9000 Client-Server and Server-Server communications. Installing Microsoft KBs at all client and server workstations solved this problem.

Microsoft August Preview updates cause similar problems in C•CURE 9000 Client-Server and Server-Server communications. Software House has worked with Microsoft to develop this Critical Update to provide a workaround to these Microsoft Windows Update defects.

Table 3: Solutions

Solution 1	Install Microsoft KBs at all client and server workstations simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.
Solution 2	Install this Critical Update on C•CURE 9000 servers. Microsoft Windows Updates can then be deployed on servers and clients as required and non-simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.

NOTE: The Microsoft Windows Update fix only requires installation of this Critical Update on C•CURE 9000 servers. To deploy this Critical Update's non-Microsoft client-side fixes, ensure to also install this Critical Update on C•CURE 9000 clients.

Microsoft Preview of Quality Rollup (KB) numbers are cross-referenced against their associated Windows operating systems in the *Table 4: KB numbers*. Install the relevant KBs for your operating system according to the solution you have chosen from *Table 3: Solutions*.

Table 4: KB Numbers

Operating System	Parent KB (Windows Update offering)	Child KB (displayed in *Installed Updates*)	
Windows Server 2008	4346083	2.0 =	4342308
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows 7 / Server 2008 R2	4346080	3.5.1 =	4342309
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows Server 2012	4346081	3.5 =	4342307
		4.5.2 =	4342318
		4.6.x/4.7.x =	4342314
Windows 8.1 / Server 2012 R2	4346082	3.5 =	4342310
		4.5.2 =	4342317
		4.6.x/4.7.x =	4342315
Windows 10 RS1 / Server 2016	4343884	Same as parent KB	
Windows 10 RS2	4343889	Same as parent KB	
Windows 10 RS3	4343893	Same as parent KB	
Windows 10 RS4	4346783	Same as parent KB	

NOTE: For full (updated) details, download Software House TAB SWH-TAB-000024206 from the Software House Support Portal (requires registration).

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP2 Critical Update 05 (Unified 3.52 SP2 CU05)

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 05 (Unified 3.52 SP2 CU05) Release Notes
September 2018

This Release Note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 05 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read this release note before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 05 includes all fixes released in the Critical Updates and Service Packs listed in the Version Matrix table.

Table 1: Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1236.442	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2
2.60 SP2 CU01	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU01
2.60 SP2 CU02	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU02
2.60 SP2 CU03	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU03
2.60 SP2 CU04	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU04
2.60 SP2 CU05	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU05

2. Installing the Critical Update

Follow the steps below to install this critical update on both C•CURE 9000 servers and clients.

Updating victor Web Service:

1. Start the victor Web Service update by double clicking on **setup.exe** in the CrossFireWebService folder.
2. Follow the installation instructions on screen to complete victor Web Service update install.
3. Reboot your machine if prompted to do so.

On a C•CURE 9000 server:

1. Log out and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU05.exe**.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log out and exit the C•CURE 9000 Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU05.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

3. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state. To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit the C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP2CU05.exe** from the C•CURE 9000 2.60 Service Pack 2 Critical Update 05 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit the C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP2 CU05** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP2 CU05** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

4. SPARs Fixed

This critical update includes the SPAR fix described in the SPAR table below. This critical update also fixes a Microsoft Windows Update-related issue described under *Microsoft Update-related SPAR fix.*

Table 2: SPAR Table

SPAR Number	SPAR Description
567995	Clearances can be assigned or removed without having to edit Personnel.
568725	Tracelog exceptions related to events have been corrected.

Microsoft Windows Update-related SPAR fix

Overview

Microsoft May Preview updates caused problems in C•CURE 9000 Client-Server and Server-Server communications. Installing Microsoft KBs at all client and server workstations solved this problem.

Microsoft August Preview updates will cause similar problems in C•CURE 9000 Client-Server and Server-Server communications. Software House has worked with Microsoft to develop this Critical Update to provide a workaround to these Microsoft Windows Update defects.

Table 3: Solutions

Solution 1	Install Microsoft KBs at all client and server workstations simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.
Solution 2	Install this Critical Update on C•CURE 9000 servers. Microsoft Windows Updates can then be deployed on servers and clients as required and non-simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.

NOTE: The Microsoft Windows Update fix only requires installation of this Critical Update on C•CURE 9000 servers. To deploy this Critical Update's non-Microsoft client-side fixes ensure to also install this Critical Update on C•CURE 9000 clients.

Microsoft Preview of Quality Rollup (KB) numbers are cross-referenced against their associated Windows operating systems in the KB numbers table below. Install the relevant KBs for your operating system according to the solution you have chosen from the Solutions table above.

Table 4: KB Numbers

Operating System	Parent KB (Windows Update offering)	Child KB (displayed in *Installed Updates*)	
Windows Server 2008	4346083	2.0 =	4342308
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows 7 / Server 2008 R2	4346080	3.5.1 =	4342309
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows Server 2012	4346081	3.5 =	4342307
		4.5.2 =	4342318
		4.6.x/4.7.x =	4342314
Windows 8.1 / Server 2012 R2	4346082	3.5 =	4342310
		4.5.2 =	4342317
		4.6.x/4.7.x =	4342315
Windows 10 RS1 / Server 2016	4343884	Same as parent KB	
Windows 10 RS2	4343889	Same as parent KB	
Windows 10 RS3	4343893	Same as parent KB	
Windows 10 RS4	4346783	Same as parent KB	

NOTE: For full (updated) details, download Software House TAB SWH-TAB-000024206 from the Software House Support Portal (requires registration).

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP2 Critical Update 04 (Unified 3.52 SP2 CU04)

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 04 (Unified 3.52 SP2 CU04) Release Notes
September 2018

This Release Note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 04 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read this release note before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

Table 1: Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1236.442	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2
2.60 SP2 CU01	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU01
2.60 SP2 CU02	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU02
2.60 SP2 CU03	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU03
2.60 SP2 CU04	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU04

2. Installing the Critical Update

Follow the steps below to install this critical update on both C•CURE 9000 servers and clients.
NOTE: Ensure to update victor Web Service before proceeding to install the Critical Update .exe file.

1. Updating victor Web Service:

2. Start the victor Web Service update by double clicking on **setup.exe** in the CrossFireWebService folder.
3. Follow the installation instructions on screen to complete victor Web Service update install.
4. Reboot your machine if prompted to do so.

2. On a C•CURE 9000 server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU04.exe**.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

3. On a C•CURE 9000 client:

1. Log out and exit the Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU04.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

3. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state.
To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit the C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP2CU04.exe** from the C•CURE 9000 2.60 Service Pack 2 Critical Update 04 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit the C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.

5. Select **C•CURE 9000 2.60 Client SP2 CU04** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP2 CU04** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

4. SPARs Fixed

This critical update includes the SPAR fix described in the SPAR table below. This critical update also fixes a Microsoft Windows Update-related issue described under *Microsoft Update-related SPAR fix.*

Table 2: SPAR Table

SPAR Number	SPAR Description
567794	An issue which caused the iSTAR driver to crash and not recover unless the OS was restarted has been resolved.
566138	SAS clearances and Global clearances are displayed, as expected, on the SAS Personnel editor.

Microsoft Windows Update-related SPAR fix

Overview

Microsoft May Preview updates caused problems in C•CURE 9000 Client-Server and Server-Server communications. Installing Microsoft KBs at all client and server workstations solved this problem.

Microsoft August Preview updates will cause similar problems in C•CURE 9000 Client-Server and Server-Server communications. Software House has worked with Microsoft to develop this Critical Update to provide a workaround to these Microsoft Windows Update defects.

Table 3: Solutions

Solution 1	Install Microsoft KBs at all client and server workstations simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.
Solution 2	Install this Critical Update on C•CURE 9000 servers. Microsoft Windows Updates can then be deployed on servers and clients as required and non-simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.

NOTE: The Microsoft Windows Update fix only requires installation of this Critical Update on C•CURE 9000 servers. To deploy this Critical Update's non-Microsoft client-side fixes ensure to also install this Critical Update on C•CURE 9000 clients.

Microsoft Preview of Quality Rollup (KB) numbers are cross-referenced against their associated Windows operating systems in the KB numbers table below. Install the relevant KBs for your operating system according to the solution you have chosen from the Solutions table above.

Table 4: KB Numbers

Operating System	Parent KB (Windows Update offering)	Child KB (displayed in *Installed Updates*)	
Windows Server 2008	4346083	2.0 =	4342308
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows 7 / Server 2008 R2	4346080	3.5.1 =	4342309
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows Server 2012	4346081	3.5 =	4342307
		4.5.2 =	4342318
		4.6.x/4.7.x =	4342314
Windows 8.1 / Server 2012 R2	4346082	3.5 =	4342310
		4.5.2 =	4342317
		4.6.x/4.7.x =	4342315
Windows 10 RS1 / Server 2016	4343884	Same as parent KB	
Windows 10 RS2	4343889	Same as parent KB	
Windows 10 RS3	4343893	Same as parent KB	
Windows 10 RS4	4346783	Same as parent KB	

NOTE: For full (updated) details, download Software House TAB SWH-TAB-000024206 from the Software House Support Portal (requires registration).

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP2 Critical Update 03 (Unified 3.52 SP2 CU03)

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 03 (Unified 3.52 SP2 CU03) Release Notes
September 2018

This Release Note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 03 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read these release notes before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

Table 1: Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1236.442	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2
2.60 SP2 CU01	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU01
2.60 SP2 CU02	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU02
2.60 SP2 CU03	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU03

2. Installing the Critical Update

On a C•CURE 9000 server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.

4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU03.exe**.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log out and exit the Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU03.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

3. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state. To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP2CU03.exe** from the C•CURE 9000 2.60 Service Pack 2 Critical Update 03 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP2 CU03** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP2 CU03** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

4. SPARs Fixed

This critical update includes the SPAR fix described in the SPAR table below. This critical update also fixes a Microsoft Windows Update-related issue described under *Microsoft Update-related SPAR fix.*

Table 2: SPAR Table

SPAR Number	SPAR Description
564470	An issue which caused personnel downloads to fail on iSTAR controllers has been resolved.

564618	An issue which caused Monitoring Stations to freeze intermittently, pending a services restart, has been resolved.
566062	The High Activity Monitor no longer causes an error message to appear on screen when editing global data from a SAS-connected client.
564598	Microsoft Windows Update issue (detailed below).

Microsoft Windows Update-related SPAR fix

Overview

Microsoft May Preview updates caused problems in C•CURE 9000 Client-Server and Server-Server communications. Installing Microsoft KBs at all client and server workstations solved this problem.

Microsoft August Preview updates will cause similar problems in C•CURE 9000 Client-Server and Server-Server communications. Software House has worked with Microsoft to develop this Critical Update to provide a workaround to these Microsoft Windows Update defects.

Table 3: Solutions

Solution 1	Install Microsoft KBs at all client and server workstations simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.
Solution 2	Install this Critical Update on C•CURE 9000 servers. Microsoft Windows Updates can then be deployed on servers and clients as required and non-simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.

NOTE: The Microsoft Windows Update fix only requires installation of this Critical Update on C•CURE 9000 servers. To deploy this Critical Update's non-Microsoft client-side fixes ensure to also install this Critical Update on C•CURE 9000 clients.

Microsoft Preview of Quality Rollup (KB) numbers are cross-referenced against their associated Windows operating systems in the KB numbers table below. Install the relevant KBs for your operating system according to the solution you have chosen from the Solutions table above.

Table 4: KB Numbers

Operating System	**Parent KB (Windows Update offering)**	**Child KB (displayed in *Installed Updates*)**	
Windows Server 2008	4346083	2.0 =	4342308
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows 7 / Server 2008 R2	4346080	3.5.1 =	4342309
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows Server 2012	4346081	3.5 =	4342307
		4.5.2 =	4342318
		4.6.x/4.7.x =	4342314
Windows 8.1 / Server 2012 R2	4346082	3.5 =	4342310
		4.5.2 =	4342317
		4.6.x/4.7.x =	4342315

Windows 10 RS1 / Server 2016	4343884	Same as parent KB
Windows 10 RS2	4343889	Same as parent KB
Windows 10 RS3	4343893	Same as parent KB
Windows 10 RS4	4346783	Same as parent KB

NOTE: For full (updated) details, download Software House TAB SWH-TAB-000024206 from the Software House Support Portal (requires registration).

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP2 Critical Update 02 (Unified 3.52 SP2 CU02)

C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 02 (Unified 3.52 SP2 CU02) Release Notes
August 2018

This Release Note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 2 Critical Update 02 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read these release notes before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

Table 1: Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1236.442	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2
2.60 SP2 CU01	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU01
2.60 SP2 CU02	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2 CU02

2. Installing the Critical Update

On a C•CURE 9000 server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU02.exe**.

5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log out and exit the Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP2CU02.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

3. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state. To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP2CU02.exe** from the C•CURE 9000 2.60 Service Pack 2 Critical Update 02 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP2 CU02** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP2 CU02** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

4. SPARs Fixed

This critical update includes the SPAR fix described in the SPAR table below. This critical update also fixes a Microsoft Windows Update-related issue described under *Microsoft Update-related SPAR fix.*

Table 2: SPAR Table

SPAR Number	SPAR Description
562125	An issue which stopped CrossFire from starting as expected after upgrading from 2.60 SP1 to 2.60 SP2 has been resolved.

Microsoft Windows Update-related SPAR fix

Overview

Microsoft May Preview updates caused problems in C•CURE 9000 Client-Server and Server-Server communications. Installing Microsoft KBs at all client and server workstations solved this problem.

Microsoft August Preview updates will cause similar problems in C•CURE 9000 Client-Server and Server-Server communications. Software House has worked with Microsoft to develop this Critical Update to provide a workaround to these Microsoft Windows Update defects.

Table 3: Solutions

Solution 1	Install Microsoft KBs at all client and server workstations simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.
Solution 2	Install this Critical Update on C•CURE 9000 servers (not clients). Microsoft Windows Updates can then be deployed on servers and clients as required and non-simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.

Microsoft Preview of Quality Rollup (KB) numbers are cross-referenced against their associated Windows operating systems in the KB numbers table below. Install the relevant KBs for your operating system according to the solution you have chosen from the Solutions table above.

Table 4: KB Numbers

Operating System	**Parent KB (Windows Update offering)**	**Child KB (displayed in *Installed Updates*)**	
Windows Server 2008	4346083	2.0 =	4342308
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows 7 / Server 2008 R2	4346080	3.5.1 =	4342309
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows Server 2012	4346081	3.5 =	4342307
		4.5.2 =	4342318
		4.6.x/4.7.x =	4342314
Windows 8.1 / Server 2012 R2	4346082	3.5 =	4342310
		4.5.2 =	4342317
		4.6.x/4.7.x =	4342315
Windows 10 RS1 / Server 2016	4343884	Same as parent KB	
Windows 10 RS2	4343889	Same as parent KB	
Windows 10 RS3	4343893	Same as parent KB	
Windows 10 RS4	4346783	Same as parent KB	

NOTE: For full (updated) details, download Software House TAB SWH-TAB-000024206 from the Software House Support Portal (requires registration).

End of Release Notes

SOFTWARE HOUSE

From Tyco Security Products

Release Notes

C•CURE 9000 Version 2.60 Service Pack 2

Applicable Software	Product Data
C•CURE 9000 Version 2.60	Visit the C•CURE 9000 section of the Software House website – http://www.swhouse.com/Support/SoftwareDownloads.aspx – to download product critical updates, service packs, and release notes.

September 2018

NOTE: In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Contents

This Release Note provides important information for installing and uninstalling C•CURE 9000 Version 2.60 Service Pack 2, for both server and client machines.

Service Pack Overview

This Service Pack provides software improvements for C•CURE version 2.60, and can be applied as a minor version update, without the impact or effort required for major version upgrades. Service Packs contain no database changes or modifications that can break external integrations. For further information refer to the Service Pack Improvements section below.

This Service Pack contains one or more of the following categories of modifications:

- **Security Updates** – Modifications that address exposure to industry security vulnerabilities.
- **Enhancements** – Modifications which provide new functionality and/or optimizations that improve system performance.
- **Key Fixes** – Applicable to the majority of installed systems.
- **General Fixes** –May or may not be applicable to a specific system.

Service Pack content is driven by our Customer Support team and prioritized by severity, impact, and overall customer needs through our Software Problem Action Request (SPAR) process. Each modification contained in this Service Pack is identified with a SPAR number in the table.

NOTE: C•CURE GO for 2.60 Service Pack 2 is installed automatically as part of the installation package.

Requirements

This Service Pack for C•CURE version 2.60 requires the following software:

- C•CURE 9000 Security and Event Management System version 2.60.

Contents of the Service Pack

The Service Pack is installable from the downloaded media.
The media contains the following files:

- **2.60_SP2.exe** – the Service Pack software installer.
- **9000 2.60_sp2_rn_lt_en_8200-1367-51b0.pdf -** this release note file.

Installation

NOTE: C•CURE 9000 V2.60 must be properly installed for this service pack to install and run properly.

On the C•CURE 9000 Server:

1. Log out and exit the C•CURE 9000 Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.

3. On the server machine, use the Server Configuration application to stop the CrossFire Service and the Server Component Framework, and then exit the application.
4. Install the C•CURE 9000 service pack update by double clicking on **2.60_SP2.exe** on the root of the media.
5. Follow the installation instructions to complete the C•CURE 9000 service pack install.

On the C•CURE 9000 Client:

1. Log out and exit the C•CURE 9000 Administration application on the client.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client.
3. Install the C•CURE 9000 service pack update by double-clicking on **2.60_SP2.exe** on the root of the CD.
4. Follow the installation instructions to complete the C•CURE 9000 service pack install.

Uninstalling the Service Pack

NOTE: If you uninstall this service pack, both C•CURE 9000 installation reverts to its previous SP state. If Critical Updates were previously applied to this original SP state, you must reapply these.

1. Log out and exit the C•CURE 9000 Administration application.
2. Log out and exit the C•CURE 9000 Monitoring Station application.
3. Through the Server Management application, stop the CrossFire Service and the Server Component Framework, then exit the application.
4. Run **2.60_SP2.exe** from the original C•CURE 9000 2.60 Service Pack 2 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack.

NOTE: If you uninstall the client and server components separately you must remove the Service Pack from both the client and server components to ensure the versions correspond correctly.

1. Log out and exit the C•CURE 9000 Administration application.
2. Log out and exit the C•CURE 9000 Monitoring Station application.
3. Through the Server Configuration application, stop the CrossFire Framework Service and the Server Component Framework Service, then exit the application.
4. Navigate to **Control Panel>Programs and Features>View Installed Updates**.
5. Select C•CURE 9000 Client 2.60 SP2 and click **Uninstall**.
6. Select victor Application Server 3.52 SP2 and click **Uninstall.**

Rebooting may be required after uninstalling the Service Pack.

Updating victor Web Service

1. Start the victor Web Service update by double clicking on **setup.exe** in the CrossFireWebService folder.
2. Follow the installation instructions on screen to complete victor Web Service update install.
3. Reboot your machine if prompted to do so.

Versions for C•CURE 9000 Software and Service Packs

This table shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		C•CURE Client Version	victor Application Server	SP/CU
2.60	2.60.4947.0389	2.60.4947.0389	3.52.1158.403	N/A
2.60 SP1	2.60.5011.0453	2.60.5011.0453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP2	2.60.5544.572	2.60.5544.572	3.52.2044.572	C•CURE 9000 Client 2.60 SP2

Service Pack Improvements

This Service Pack includes the following features and enhancements. SPAR numbers are included in the SPAR table below.

Security Updates

Security updates are applicable to all installed systems.

Category	SPAR Number	SPAR Description
Licensing	524504	An extra HostID has been added to ensure C•CURE license integrity when run on a virtual machine in a cloud environment.

Enhancements

Enhancements are applicable to all installed systems.

Category	SPAR Number	SPAR Description
Import/Export	456975	Users can now select folders using the automatic data import function.

Key Fixes

Key fixes are applicable to the majority of installed systems.

Category	SPAR Number	SPAR Description
Administration and Monitoring Applications	436431	Monitoring station memory usage has been made more efficient by releasing memory to the system when tabs or app layouts are switched. This results in the system being more stable and prevents “out of memory” errors.

General Fixes

General fixes may or may not be applicable to a specific system.

Category	SPAR Number	SPAR Description
Administration and Monitoring Applications	538100	QR codes are inserted to calendar attachments as JPEG files.
	443029	Multiple application views configured within the monitoring application no longer cause instability upon application start-up. **NOTE:** C•CURE supports up to 50 layouts.
	460438	Right-click displays “Show Locked Causes” for Schlage wireless locks.
	512653 / 525403 / 474416	UDF label changes now update properly on dynamic views.
	474608	UI does not allow hardware to be saved without OwnerClassType data.
	533263	Message Date/Time and Message Local Date/Time reports correctly on 2.60 Enterprise systems.
	454683	Mandatory visit additional details are correctly validated when a visit is saved from the Administration workstation.
	512172	UDF label changes are not affected by application of critical updates.
	525073	The Name Field Quick Search for Personnel criteria field has been changed from “Starts with” to “Contains”.
Areas and Zones	464430	Records remain consistent between the Monitoring Station and Go Reader when Areas are used with Go Reader roll call function.
Aperio	540429	AS100 input can be wired as a Door Switch Monitor without generating a false Door Forced alarm.
APC Driver	453115	When communication is restored to an offline panel, or an apC is disabled and then re-enabled, a fresh full download occurs correctly.
	474414	Journal history shows correct time for door-forced events on apc panels.
Application Server	517410	An offline SAS can be successfully removed from a MAS.
	474680	The system variable Auto Credential Issue Code now increments correctly.
Card Formats	472066	A delay which occurred when opening a global card format for edit within the Admin application of an enterprise environment has been resolved.

	506646	Personnel records save correctly after modifying a credential or clearance without causing CHUID errors.
Credentials	521301	Assigning a temporary credential to a Personnel record does not reset the CHUID format of that credential.
CrossFire Server	537879	A memory leak in CrossFire caused by an Operator term with a trailing space has been resolved.
	543903	An error which caused CrossFire to crash when LogBackUp was attempted to a drive that was out of space has been resolved.
	552165	An issue which caused CrossFire memory spikes when sync DBqueue is backed up has been resolved.
Encryption	541490	RSA encryption problems related to Microsoft DLL process can no longer cause iSTAR drivers to crash.
Events	472144	Panel events which pulse an output are now cleared successfully from the Manual Actions list.
	444717	Events configured to export a Personnel Portrait now work correctly.
	464212	Saving an event with action “Secure Door” does not generate an error.
	538473	Sound on event stops playing, as expected, when an event is acknowledged.
Firmware	523895	Users can upgrade iSTAR Ultra SE firmware using C•CURE client.
Import/Export	442118	Data Import “Folder On Server” value displays and saves correctly.
	510970	Import configuration does not change on upgrading to 2.60.
	511106	Values are properly imported to the Label field in an existing UDF Enumerated List.
	506159	Reports can be exporting via email from C•CURE clients.
	455841	UDF XML files import correctly.
	474443	The Card Number (for matching only) field in Data Import supports numerical card values larger than 2147483647.
Installation and Upgrade	511862	An error which prevented Crossfire from starting after installing C•CURE 2.60 SP1 has been resolved.

	525375	Language pack installs successfully upon upgrade.
	518786	An error that caused C●CURE to display a message stating that "WebBridgeState" column was invalid or missing has been resolved.
iSTAR Driver	512005	Credential activation time values do not affect SQLite downloads.
	529630	Clearance Filter applies equally across Pro, Edge, and Ultra readers.
	453106	Panel names with special characters will not crash the CCureProToSEConvertUtility.
	511110	iSTAR panels which come back online simultaneously will download personnel records concurrently.
	463278	iSTAR Ultra panels do not lose configured readers when Schlage wireless locks are configured.
	537884	New memory status messages sent from updated iSTAR Edge firmware are logged and recorded within the C•CURE Journal. These messages can be enabled or disabled through a new System Variable.
	540776	RM Readers successfully come online with the iSTAR Ultra SE running firmware versions 6.5.2.20569, 6.5.2.20589, 6.6.0.20823.
Journal	532961	Journal sync calls have been made more efficient to prevent slowdowns over WAN links.
Licensing	475708	Licence verification of the HostID has been optimised to prevent system outages.
	557371	After upgrade to 2.60SP1 CU04, License Manager performance issues resolved.
Maps	511991	Editing and saving icons or maps will not cause the Administration centre to crash on Windows 10 and Windows Server 2012 clients.
	442025	When a map is loaded in the monitoring application it displays correctly in the center of the screen without leaving excessive white space on its borders.
Operators/Privileges	525066	Operator roles perform correctly when Unification is introduced to Enterprise.
	444151	An error which caused unwanted executors to be added to custom privileges has been resolved.
	440314	Door reports can be made from a personnel record by an Operator with read access to personnel.
	456976	Users cannot disable the service operator account running the C•CURE services.

	536946	Passwords entered to the Basic Authentication Dialog are not kept within memory.
Personnel	536357	Switching between tabs in Personnel view does not cause badge layout errors.
	458413	Personnel editor views remain consistent between different Personnel records.
Query/Reports	474332	The SWH06 Door Access Report and SWHrep0506 Query have been modified to ensure that they conform to the timeframe of report parameters.
	460347	Audit queries return list of modified System Variables when queried on Object-type System Variables.
	505981	Report queries which use the Journal Default Query do not generate a syntax error.
	514497	SWH41 report can handle NULL date fields.
Server Configuration Application	557371	After upgrade to 2.60SP1 CU04, Server Configuration performance issues resolved.
Swipe and Show	525004	A functionality issue with the Momentary Unlock function has been resolved.
Sync Conflicts	527557	Upgrades in MAS multi-version mode supports 2.40 SAS.
	426389	Resolved a sync error that sometimes occurred when Personnel were deleted.
	458958	A sync conflict caused by lack of partition ID between the victor MAS and SAS has been resolved.
	474706	Data is safeguarded when an Enterprise sync is performed with database restore.
victor Web Service	514085	Users can log in to Visitor Management when group policy prevents interactive login for non-administrative users.
victorWebClient	556229	Door activity shown in the Journal is accurately reflected within the Previous Doors tab of the Personnel Record.
	556246	A search reset button has been added to allow a search to be cancelled if an error is encountered.
	556247	Journal Search can match text-string as entered in an Exact Match or Like Comparison search.

	556248/556249	A checkbox has been added to select Exact Match or Like Comparison searches within Journal Search.
	456173	Unwanted portrait images can be deleted.
VideoEdge	450362	VideoEdge units do not trigger messages in the C•CURE monitoring station when the VideoEdge unit is disabled.

Service Pack Limitations

Multiversion Support

C•CURE 9000 provides Multi-version support. This is the ability for SAS systems not yet upgraded to the version the MAS is running to connect to the MAS, synchronize records, and identify conflicts, and attach clients to the MAS to configure and monitor the Enterprise. From the MAS perspective, a Global Operator has the ability to attach to both upgraded and non-upgraded SAS systems, with some limitations due to the version differences.

The Multi-version process begins with an Enterprise where the MAS and every SAS is currently at the same version, and the MAS is upgraded. Therefore, only two versions of C•CURE 9000 can be involved:

- The new version to which the MAS has been upgraded.
- The previous version at which all SAS systems were operating.

If an Enterprise currently has a MAS at one version and SAS systems with differing versions, it is necessary to update all SAS systems to be at the same version as the MAS to establish a common baseline, prior to beginning to upgrade the MAS to take advantage of Multi-version support.

The intention still is to proceed with upgrading every SAS to match the new MAS version. The difference is that until that point, all the SAS systems can participate in the Enterprise, within version-specific limitations.

To enable upgraded clients to communicate with previous version SAS systems, during the upgrade a copy is made of the C•CURE 9000 client applications from the previous version so that these applications can be launched when needed if the upgraded client detects it is running in a Multi-version Enterprise.

For a complete list of Multi-Version Support limitations, refer to the *C•CURE 9000 Enterprise Architecture Guide* included with this service pack.

Finding More Information

The user guides are included on the installation image and are automatically installed.

You can find further information in the user guides located here: Program Files (x86)\Tyco\CCURE Client.

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP1 Critical Update 07 (Unified 3.52 SP1 CU07)

C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 07 (Unified 3.52 SP1 CU07) Release Notes
August 2018

This Release Note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 07 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read this release note before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

Table 1: Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features		
		Client Version	victor Application Server	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	3.52.1158.403	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU06	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU06
2.60 SP1 CU07	2.60.5011.453	2.60.5011.453	3.52.1236.442	C•CURE 9000 Client 2.60 SP1 CU07

2. Installing the Critical Update

On a C•CURE 9000 server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU07.exe**.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.

6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log out and exit the Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU07.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

3. Updating victor Web Service

On a C•CURE 9000 server or client:

1. Start the victor Web Service update by double clicking on **setup.exe** in the CrossFireWebService folder.
2. Follow the installation instructions on screen to complete victor Web Service update install.
3. Reboot your machine if prompted to do so.

4. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state. To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP1CU07.exe** from the C•CURE 9000 2.60 Service Pack 1 Critical Update 07 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP1 CU07** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP1 CU07** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media > ISOImage > Bin**.

5. SPARs Fixed

This critical update includes the SPAR fixes described in the SPAR table below. This critical update also fixes a Microsoft Windows Update-related issue described under *Microsoft Update-related SPAR fix.*

Table 2: SPAR Table

SPAR Number	SPAR Description
561435	An issue which caused personnel downloads to fail on iSTAR controllers has been resolved.
535311	An issue which caused some Monitoring Stations to stop working unexpectedly has been resolved.
539115	Users can log in to Visitor Management when group policy prevents interactive login for non-administrative users.
535458	Badge layout remains as expected when switching between tabs in personnel view.

Microsoft Windows Update-related SPAR fix

Overview

Microsoft May Preview updates caused problems in C•CURE 9000 Client-Server and Server-Server communications. Installing Microsoft KBs at all client and server workstations solved this problem.

Microsoft August Preview updates will cause similar problems in C•CURE 9000 Client-Server and Server-Server communications. Software House has worked with Microsoft to develop this Critical Update to provide a workaround to these Microsoft Windows Update defects.

Table 3: Solutions

Solution 1	Install Microsoft KBs at all client and server workstations simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.
Solution 2	Install this Critical Update on C•CURE 9000 servers (not clients). Microsoft Windows Updates can then be deployed on servers and clients as required and non-simultaneously. See Table 4 for cross-references of operating systems with parent and child KB numbers.

Microsoft Preview of Quality Rollup (KB) numbers are cross-referenced against their associated Windows operating systems in the KB numbers table below. Install the relevant KBs for your operating system according to the solution you have chosen from the Solutions table above.

Table 4: KB Numbers

Operating System	Parent KB (Windows Update offering)	Child KB (displayed in *Installed Updates*)	
Windows Server 2008	4346083	2.0 =	4342308
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows 7 / Server 2008 R2	4346080	3.5.1 =	4342309
		4.5.2 =	4342319
		4.6.x/4.7.x =	4342316
Windows Server 2012	4346081	3.5 =	4342307
		4.5.2 =	4342318

		4.6.x/4.7.x =	4342314
Windows 8.1 / Server 2012 R2	4346082	3.5 =	4342310
		4.5.2 =	4342317
		4.6.x/4.7.x =	4342315
Windows 10 RS1 / Server 2016	4343884	Same as parent KB	
Windows 10 RS2	4343889	Same as parent KB	
Windows 10 RS3	4343893	Same as parent KB	
Windows 10 RS4	4346783	Same as parent KB	

NOTE: For full (updated) details, download Software House TAB SWH-TAB-000024206 from the Software House Support Portal (requires registration).

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP1 Critical Update 06 (Unified 3.52 SP1 CU06)

C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 06 (Unified 3.52 SP1 CU06) Release Notes
July 2018

These Release Notes provide important information for installing the C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 06 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read these release notes before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features	
		Client Version	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1 CU05
2.60 SP1 CU06	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1 CU06

2. Installing the Critical Update

On a C•CURE 9000 server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU06.exe**.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.

6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log out and exit the Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU06.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

3. Updating victor Web Service

On a C•CURE 9000 server or client:

1. Start the victor Web Service update by double clicking on **setup.exe** in the CrossFireWebService folder.
2. Follow the installation instructions on screen to complete victor Web Service update install.
3. Reboot your machine if prompted to do so.

4. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state. To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP1CU06.exe** from the C•CURE 9000 2.60 Service Pack 1 Critical Update 06 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP1 CU06** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP1 CU06** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.50 Media > ISOImage > Bin**.

5. SPARs Fixed

This critical update includes the following SPAR fixes:

SPAR Number	SPAR Description
535311	A memory issue which caused Monitoring Stations to be unresponsive has been resolved.

535458	Switching between tabs in Personnel view does not cause badge layout errors.
537290	The “Display Record Video” button for an event functions correctly.
539114	victor Web Service application requires a valid Windows principal and valid password to function.
539115	Users can log in to Visitor Management when group policy prevents interactive login for non-administrative users.

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP1 Critical Update 05 (Unified 3.52 SP1 CU05)

C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 05 (Unified 3.52 SP1 CU05) Release Notes
May 2018

These Release Notes provide important information for installing the C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 05 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read these release notes before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features	
		Client Version	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1 CU04
2.60 SP1 CU05	2.60.5011.453	2.60.5011.453	C•CURE 9000 Client 2.60 SP1 CU05

2. Installing the Critical Update

On a C•CURE 9000 server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Configuration application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU05.exe**.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log out and exit the Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU05.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

3. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state. To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP1CU05.exe** from the C•CURE 9000 2.60 Service Pack 1 Critical Update 05 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP1 CU05** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP1 CU05** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.50 Media > ISOImage > Bin**.

4. SPARs Fixed

This critical update includes the following SPAR fixes:

SPAR Number	SPAR Description
512644	RSA encryption problems related to Microsoft DLL process can no longer cause iSTAR drivers to crash.

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP1 Critical Update 04 (Unified 3.52 SP1 CU04)

C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 04 (Unified 3.52 SP1 CU04) Release Notes
February 2018

These Release Notes provide important information for installing the C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 04 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read these release notes before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features	
		Client Version	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	C-CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	C-CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	C-CURE 9000 Client 2.60 SP1 CU03
2.60 SP1 CU04	2.60.5011.453	2.60.5011.453	C-CURE 9000 Client 2.60 SP1 CU04

2. Installing the Critical Update

On a C•CURE 9000 server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Management application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU04.exe**.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
6. Reboot your machine if prompted to do so.

On a C•CURE 9000 client:

1. Log out and exit the Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.

3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU04.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.
5. Reboot your machine if prompted to do so.

3. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state. To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP1CU04.exe** from the C•CURE 9000 2.60 Service Pack 1 Critical Update 04 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP1 CU04** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP1 CU04** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.50 Media > ISOImage > Bin**.

4. SPARs Fixed

This critical update includes the following SPAR fixes:

SPAR Number	SPAR Description
524490	A functionality issue with the Momentary Unlock function has been resolved.
525494	An error which caused ISTAR Panels to disconnect readers configured with Schlage locks has been resolved.
526328	Users can now select a folder within the Data Source Configuration section of the Data Import window to select a folder instead of a file or manually typing a folder path.
527542	Upgrades in MAS multi-version mode supports 2.40 SAS.

End of Release Notes

pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco are the property of their respective owners, and are used with permission or allowed under applicable laws.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP1 Critical Update 03 (Unified 3.52 SP1 CU03)

C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 03 (Unified 3.52 SP1 CU03) Release Notes
January 2018

These Release Notes provide important information for installing the C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 03 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read these release notes before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features	
		Client Version	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	C-CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	C-CURE 9000 Client 2.60 SP1 CU02
2.60 SP1 CU03	2.60.5011.453	2.60.5011.453	C-CURE 9000 Client 2.60 SP1 CU03

2. Installing the Critical Update

On a C•CURE 9000 server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Management application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU03.exe**.
5. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.

On a C•CURE 9000 client:

1. Log out and exit the Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU03.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.

3. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state. To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP1CU03.exe** from the C•CURE 9000 2.60 Service Pack 1 Critical Update 03 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP1 CU03** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP1 CU03** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.50 Media > ISOImage > Bin**.

4. SPARs Fixed

This critical update includes the following SPAR fixes:

514185
An error which prevented fast card downloads on iSTAR panels with over 20 IP-ACMs configured has been resolved.

516935
An offline SAS can be successfully removed from a MAS.

517579
SQLite fast download works correctly when activation and deactivation times for a credential are the same.

517580
Data is safeguarded when an Enterprise sync is performed with database restore.

520189
Panel events which pulse an output do not remain on the Manual Actions list when cancelled.

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP1 Critical Update 02 (Unified 3.52 SP1 CU02)

C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 02 (Unified 3.52 SP1 CU02) Release Notes
October 2017

These Release Notes provide important information for installing the C•CURE 9000 Version 2.60 Service Pack 1 Critical Update 02 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read these release notes before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features	
		Client Version	SP/CU Version
2.60	2.60.4947.389	2.60.4947.389	N/A
2.60 SP1	2.60.5011.453	2.60.5011.453	C-CURE 9000 Client 2.60 SP1
2.60 SP1 CU02	2.60.5011.453	2.60.5011.453	C-CURE 9000 Client 2.60 SP1 CU02

2. Installing the Critical Update

On a C•CURE 9000 server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Management application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Select the **CrossFireWebService.msi** and double click it.
5. Follow the on screen installation instructions to complete the victor Web Service critical update install.
6. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU02.exe**.
7. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.

On a C•CURE 9000 client:

1. Log out and exit the Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.

3. Start the C•CURE 9000 critical update by double clicking on **2.60_SP1CU02.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.

3. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state.
To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_SP1CU02.exe** from the C•CURE 9000 2.60 Service Pack 1 Critical Update 02 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel > Programs and Features > View Installed updates**.
5. Select **C•CURE 9000 2.60 Client SP1 CU02** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP1 CU02** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You then need to reinstall the previous version of CrossFireWebService which can be found in **2.50 Media > ISOImage > Bin**.

4. SPARs Fixed

This critical update includes the following SPAR fixes:

464702
The Action “Secure Door” will now save successfully when added to an Event.

End of Release Notes

SOFTWARE HOUSE

From Tyco Security Products

Release Notes

C•CURE 9000 Version 2.60 Service Pack 1

Applicable Software	Product Data
C•CURE 9000 Version 2.60	Visit the C•CURE 9000 section of the Software House website – http://www.swhouse.com/Support/SoftwareDownloads.aspx – to download product critical updates, service packs, and release notes.

July 2018

Note
In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Contents

This Release Note file provides important information for installing and uninstalling C•CURE 9000 Version 2.60 Service Pack 1, for both server and client machines.

Service Pack Overview

This Service Pack provides software improvements for C•CURE version 2.60, and can be applied as a minor version update, without the impact or effort required for major version upgrades.

Service Packs contain no database changes or modifications that can break external integrations, and may contain one or more of the following categories of modifications:

- **Security Updates** – Modifications that address exposure to industry security vulnerabilities.
- **Enhancements** – Modifications which provide new functionality and/or optimizations that improve system performance.
- **Key Fixes** – applicable to the majority of installed systems.
- **General Fixes** –May or may not be applicable to a specific system.

Service Pack content is driven by our Customer Support team and prioritized by severity, impact, and overall customer needs through our Software Problem Action Request (SPAR) process. Each modification contained in this Service Pack is identified with a SPAR number in parentheses "( )".

Requirements

This Service Pack for C•CURE version 2.60 requires the following software:

- C•CURE 9000 Security and Event Management System version 2.60.

The Service Pack for C•CURE version 2.60 supports the following operating systems:

Supported Operating Systems, DBMS, and SQL Collations

For support information for Operating Systems, DBMS's, and SQL Server Collations, see Table 1, Table 2, and Table 3 respectively.
NOTE: There are limitations on full client support for 64-bit.

Table 1: Microsoft Operating Systems for Server and Client

Server Series L/M/N/SAS	Supported Version
Windows 7 Professional SP1 or later	64-bit
Windows 7 Enterprise SP1 or later	64-bit
Windows 8.1 Professional SP1 or later	64-bit
Windows 8.1 Enterprise SP1 or later	64-bit
Windows Server 2008 R2 Standard SP1 or later	64-bit
Windows Server 2012 R2 Standard SP1 or later	64-bit

Windows Server 2016 Standard	64-bit
Windows Server 2016 Enterprise	64-bit
Windows 10 Professional	64-bit
Windows 10 Enterprise	64-bit
Server Series P/Q/R/R+/S/S+/T/SAS	**Supported Version**
Windows 10 Professional	64-bit
Windows 10 Enterprise	64-bit
Windows Server 2012 R2 Standard	64-bit
Windows Server 2016 Standard	64-bit
Windows Server 2016 Enterprise	64-bit
MAS Server	**Supported Version**
Windows Server 2012 R2 SP1 or later Standard	64-bit
Windows Server 2016 Standard	64-bit
Windows Server 2016 Enterprise	64-bit
Client	**Supported Version**
Windows 7 Professional SP1 or later	64-bit
Windows 7 Enterprise SP1 or later	64-bit
Windows 8.1 Professional SP1 or later	64-bit
Windows 8.1 Enterprise SP1 or later	64-bit
Windows 10 Professional	64-bit
Windows 10 Enterprise	64-bit
Windows Server 2012 R2 SP1 or later Standard	64-bit
Windows Server 2016 Standard	64-bit
Windows Server 2016 Enterprise	64-bit

Table 2: Microsoft DBMS

Server Series L/M/N/SAS	**Supported Version**
SQL Server 2008 R2 Standard	SP3 or later (64-bit)
SQL Server 2012 Express	SP2 or later (64-bit)
SQL Server 2012 Standard	SP2 or later (64-bit)
SQL Server 2012 Enterprise	SP2 or later (64-bit)
SQL Server 2014 Express	SP1 or later (64-bit)
SQL Server 2014 Standard	SP1 or later (64-bit)
SQL Server 2014 Enterprise	SP1 or later (64-bit)
SQL Server 2016 Express	All Service Packs (64-bit)
SQL Server 2016 Standard	All Service Packs (64-bit)
SQL Server 2016 Enterprise	All Service Packs (64-bit)
Server Series Standalone P/Q/R/R+/S/S+/T	**Supported Version**
SQL Server 2012 Standard	SP2 or later (64-bit)
SQL Server 2012 Enterprise	SP2 or later (64-bit)
SQL Server 2014 Standard	SP1 or later (64-bit)
SQL Server 2014 Enterprise	SP1 or later (64-bit)
SQL Server 2016 Standard	All Service Packs (64-bit)
SQL Server 2016 Enterprise	All Service Packs (64-bit)
SAS Server Series P/Q/R/R+/S/S+/T	**Supported Version**
SQL Server 2012 Standard	SP2 or later (64-bit)

SQL Server 2012 Enterprise	SP2 or later (64-bit)
SQL Server 2014 Standard	All Service Packs (64-bit)
SQL Server 2014 Enterprise	SP1 or later (64-bit)
SQL Server 2016 Standard	SP1 or later (64-bit)
SQL Server 2016 Enterprise	All Service Packs (64-bit)
MAS Server	**Supported Version**
SQL Server 2012 Standard	SP2 or later (64-bit)
SQL Server 2012 Enterprise	SP2 or later (64-bit)
SQL Server 2014 Standard	SP1 or later (64-bit)
SQL Server 2014 Enterprise	SP1 or later (64-bit)
SQL Server 2016 Standard	All Service Packs (64-bit)
SQL Server 2016 Enterprise	All Service Packs (64-bit)

Table 3: SQL Server Collations Supported

Windows Locale	Default Collation
Arabic (Saudi Arabia)	Arabic_CI_AS
Chinese (PRC)	Chinese_PRC_CI_AS
Chinese (Taiwan)	Chinese_Taiwan_Stroke_CI_AS
Czech (Czech Republic)	Czech_CI_AS
Danish (Denmark)	Danish_Norwegian_CI_AS
Dutch (Netherlands)	Latin1_General_CI_AS
English (United Kingdom)	Latin1_General_CI_AS
English (United States)	SQL_Latin1_General_CP1_CI_AS
French (France)	French_CI_AS
German (Germany)	Latin1_General_CI_AS
Hungarian (Hungary)	Hungarian_CI_AS
Italian (Italy)	Latin1_General_CI_AS
Japanese (Japan)	Latin1_General_CI_AI
Korean (Korea Dictionary Sort)	Korean_Wansung_CI_AS
Polish (Poland)	Polish_CI_AS
Portuguese (Brazil)	Latin1_General_CI_AS
Russian (Russia)	Cyrillic_General_CI_AS
Spanish (Spain)	Modern_Spanish_CI_AS
Swedish (Sweden)	Finnish_Swedish_CI_AS
Turkish (Turkey)	Turkish_CI_AS

Contents of the Service Pack

The Service Pack is installable from the downloaded media.

The media contains the following files:

- **2.60_SP1.exe** – the Service Pack software installer.
- 9000 2.60_SP1_RN_8200-1367-46_B0.pdf - this release note file.

Installation

NOTE: You should have the original C•CURE 9000 V2.60 media available during installation, in case Windows prompts you to insert it to continue.

NOTE: C•CURE 9000 Web Client requires 7Zip to be installed on the machine. For further information, see the *C•CURE 9000 Version 2.60 Service Pack 1 Web Client release notes*.

IMPORTANT: Updating C•CURE GO to V2.60 Service Pack 1.

V2.60 Service Pack 1 updates have to be applied manually to the C•CURE GO application.

1. Navigate to Windows Programs and Features and uninstall the **C•CURE GO Web Service.**
2. Navigate to the C•CURE GO folder on the installation CD.
3. Execute the C•CURE GO update by double-clicking on **CCureGoWebService.msi** within the C•CURE GO folder.

C•CURE 9000 V2.60 must be properly installed for this service pack to install and run properly.

On the C•CURE 9000 Server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Management application to stop the CrossFire Service and the Server Component Framework, and then exit the application.
4. Execute the C•CURE 9000 service pack update by double clicking on **2.60_SP1.exe** on the root of the CD.
5. Follow the installation instructions to complete the C•CURE 9000 service pack install.

On the C•CURE 9000 Client:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. Execute C•CURE 9000 service pack update by double-clicking on **2.60_SP1.exe** on the root of the CD.
4. Follow the installation instructions to complete C•CURE 9000 service pack install.

Uninstalling the Service Pack

NOTE: If you uninstall this service pack, the C•CURE 9000 installation reverts to its previous state.

1. Log out and exit the C•CURE 9000 Administration application.
2. Log out and exit the C•CURE 9000 Monitoring Station application.
3. Through the Server Management application, stop the CrossFire Service and the Server Component Framework, then exit the application.
4. Run **2.60_SP1.exe** from the original CCURE 9000 2.60 Service Pack 1 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack.

1. Log out and exit the C•CURE 9000 Administration application.
2. Log out and exit the C•CURE 9000 Monitoring Station application.
3. Through the Server Management application, stop the CrossFire Framework Service and the Server Component Framework Service, then exit the application.
4. Navigate to **Control Panel>Programs and Features>View Installed Updates**.
5. Select **C•CURE 9000 Client 2.6 SP1** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP1** and click **Uninstall.**

Rebooting may be required after uninstalling the Service Pack.

Updating victor Web Service

On a C•CURE 9000 server or client:

1. Start the victor Web Service update by double clicking on **setup.exe** in the CrossFireWebService folder.
2. Follow the installation instructions on screen to complete victor Web Service update install.
3. Reboot your machine if prompted to do so.

Versions for C•CURE 9000 Software and Service Packs

This table shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features	
		Client Version	SP/CU Version
2.60	2.60.4947.0389	2.60.4947.0389	N/A
2.60 SP1	2.60.5011.0453	2.60.5011.0453	C-CURE 9000 Client 2.60 SP1

New Features

iSTAR Ultra LT – a new compact network controller that supports up to 8 readers and can be powered over Ethernet and supports the following features:

- One network Gigabit Ethernet port.
- Connection to the IP-ACM Ethernet door module.
- One RS-485 port for Aperio™ readers (HUB) or Schlage® readers (PIMs). The total number of readers cannot exceed eight and cannot be combined.
- A LED bar that displays information for the booting process and firmware installation.
- Onboard unsupervised inputs: Tamper, Power Fail, and External Battery Low.
- Rechargeable coin cell battery to maintain the Ultra LT system clock up to 30 days.

TST-100 Touchscreen Terminal Reader – a new dynamic and interactive card reader with connectivity through a RS-485 interface. Smart mode protocol supports AES-256 encrypted communication between

the TST-100 Touchscreen Terminal and the IP-ACM. The TST-100 Touchscreen Terminal supports the following features:

- An interactive LCD touchscreen.
- A built-in passive infrared sensor (PIR) to detect motion in front of the reader. The LCD display dims when motion is not detected for a period of 2 minutes.
- RM mode protocol supports: iSTAR Classic, Pro, eX, Edge, Ultra, Ultra SE, Ultra Video, and Ultra controllers.
- Smart mode protocol supports: iSTAR Ultra, Ultra SE (in Ultra mode), and Ultra LT connected to an IP-ACM.
- Indoor and outdoor installation.
- Two supervised inputs, dual tamper, and two solid state outputs.
- Access validation by PIN and card.
- Keypad Commands.

For more information, see the *C•CURE 9000 Hardware Configuration Guide.*

Visitor Management Phase III – a countable license feature for the C•CURE Kiosk iOS application. This application provides a self-check-in facility for scheduled and unscheduled visitors. The C•CURE Kiosk iOS application has been enhanced in this release with the following features:

- QR code identification for visitors registering for a visit.
- Multiple language support.

The C•CURE Kiosk application only supports iOS devices and does not support Android. For more information, see the *C•CURE 9000 Visitor and Access Management Guide.*

Visitor Management – QR codes are now included in emails sent to visitors for visitor identification during visitor registration.

NOTE: Web Client Language Pack support included in this release (C•CURE 9000 Classic Web Client).

Users must refresh their web browser (using the F5 key or refresh button) to correctly display translated Web Client Help files.

EV1 encoding support for C•CURE ID badge – a standard feature that extends smart card programming and enrollment capabilities to support MIFARE DESFIRE EV1 Encoding. For more information see the *C•CURE 9000 C•CURE ID Guide.*

C•CURE ID Windows Image Acquisition and DirectShow support for USB Cameras – a standard feature that has been enhanced to support use of non-twain cameras to capture portraits. You can choose to use a local device with DirectShow capabilities, which most modern web cams have, to capture portraits for the C•CURE ID application. For more information see the *C•CURE 9000 C•CURE ID Guide.*

IPv4 and IPv6 support – C•CURE 9000 now supports configuration of the server to communicate with mixed IPv4 and IPv6 controllers and clients. For more information, see the *C•CURE 9000 Hardware Configuration Guide*.

License Update without CrossFire Restart – the License Manager has been enhanced so that the CrossFire Service does not restart when a new license is applied to C•CURE 9000.

Unified Installer – the Unified installer has been upgraded with the following enhancements:

- Installers write all log files to the following location, C:\ProgramData\Tyco\InstallerTemp
- Installation of ID Scanning is a silent install.

Service Pack Improvements

Security Updates

C•CURE GO

CCURE GO application now verifies TLS certificates for server authentication. (303976)

Personnel records imported through import watcher or automatically imported can now be viewed and edited correctly within CCURE GO. (441593)

Acknowledging an event in the Activity Monitor will no longer generate an object reference error. (441697)

Temporary Credentials

An issue which caused disabled/expired credentials to become active when clicked after removing a temporary credential has been resolved. (435428)

Enhancements

This Service Pack includes the following features and enhancements. SPAR numbers are included in parentheses “( )”.

Key Fixes

Key fixes are applicable to the majority of installed systems.

General Fixes

General fixes may or may not be applicable to a specific system.

Administration and Monitoring Application

An issue which prevented the application layouts from being saved when using multiple partitions has been fixed. (426647)

Monitoring station memory usage has been made more efficient by releasing memory to the system when tabs or app layouts are switched. This results in the system being more stable and prevents “out of memory” crashes. (436431)

Predefined log messages can now be added to events in bulk. (300726)

Activity Viewer messages for Manual Actions are now configurable to be shown based upon the operator's privilege to see the target object. (441671)

An administrator-level filter now allows messages in the **Activity Viewer** to be filtered for Manual Action, Log Message, and Object Changed State. This allows an administrator to determine what messages an operator can view. (444393)

An issue which prevented English (United Kingdom) from displaying when a UDF configuration was set to English (United States) has been resolved. (444700)

Operations which an operator has the correct privilege to perform will now load without a permissions error. (446228)

APC Driver

Action notices related to critical events will not remain on screen after an event shows as inactive. (339342)

Application Server

The import processor has been modified to ensure that when personnel are imported into the local SAS partition, their credential and image are also placed into the local SAS partition. (424812)

Custom Clearances

All door types are now supported for custom clearances. (435535)

Events

Opening the Action Tab after upgrading from CCURE 9000 2.20 to CCURE 9000 2.40 no longer causes an unexpected error to occur. Events previously configured in CCURE 9000 2.20 will now be available to view in CCURE 9000 2.40 under the Action Tab. (431629)

When printing badges, the following errors "*The handle is invalid", "System.ComponentModel.Win32Exception (0x80004005): The handle is invalid…."* and *"Print aborted. The configured printer is not valid"* can be resolved. Create a new operator using the Windows principal specified in the error message and login to CCURE 9000 Administration Application as that operator. The error no longer occurs when printing badges. (352413)

GPI

Large numbers of GPi message protocols will no longer cause the CCURE 9000 Administration application to become non-responsive. (430513)

Holidays/Schedules

An issue which caused information messages to appear in the event viewer after adding a global holiday to a local SAS database holiday group has been resolved. (417813)

Licensing

An issue which caused crashes associated with the file *ADResource2.dll* has been resolved. (432057)

Import/Export

The configuration field Card Number (for matching only), when used as one of the Personnel Match Fields, now allows personnel records to be imported without error. (441574)

iSTAR Driver

A new Communication state status is now available: *Waiting for Fast Card Download*. This indicates the controller has been entered into the fast download queue. (428664)

It is now possible to choose a panel to be the next *fast download* candidate. (428665)

The field, *Controller Boot Time*, is now available as an option within the dynamic view of an iStar Controller. (428667)

Personnel

Assigning a personnel photo from a server or client pc will not shut down the Administration Station when it is running Turkish as the primary OS language. (430733)

An error will no longer occur when a badge is sent to printer immediately after having been saved and closed. (416555)

Existing badge layout templates can be used to create a new badge layout without producing duplicate fields. (439717)

Reports

Personnel queries that use *PersonnelClearancePair* as a criteria now operate within CCURE 9000 v2.60. (441684)

Limitations

1. The use of custom clearances with inherited doors depends on whether the door's firmware supports custom clearances. The end-user must verify this.

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 Critical Update 07 (Unified 3.52 CU07)

C•CURE 9000 Version 2.60 Critical Update 07 (Unified 3.52 SP1 CU07) Release Notes
June 2017

These Release Notes provide important information for installing the C•CURE 9000 Version 2.60 Critical Update 07 on C•CURE 9000 Server and Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read these release notes before installing the product.

Contents

1. Installing the Critical Update

On a C•CURE 9000 server:

1. Log out and exit the Administration application on the server and all clients.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the server and all clients.
3. On the server machine, use the Server Management application to stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Select the **CrossFireWebService.msi** and double click it.
5. Follow the on screen installation instructions to complete victor Web Service critical update install.
6. Start the C•CURE 9000 critical update by double clicking on **2.60_CU07.exe**.
7. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.

On a C•CURE 9000 client:

1. Log out and exit the Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 critical update by double clicking on **2.60_CU07.exe**.
4. Follow the installation instructions on screen to complete C•CURE 9000 critical update install.

2. Uninstalling the Critical Update

NOTE: If you uninstall this critical update, the system reverts back to the previous C•CURE 9000 state.
To uninstall the critical update on the C•CURE 9000 server or client:

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Run **2.60_CU07.exe** from the C•CURE 9000 2.60 Critical Update 07 media.
5. Click **Remove**.

Alternatively, you can manually uninstall both the client and server components of this Service Pack Critical Update.

1. Logout and exit C•CURE 9000 Administration application.
2. Logout and exit the C•CURE 9000 Monitoring Station.
3. In the Server Configuration application, stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**, and then exit the application.
4. Navigate to **Control Panel>Programs and Features>View Installed updates**.
5. Select **C•CURE 9000 Client 2.60 CU07** and click **Uninstall**.
6. Select **victor Application Server 3.52 SP1 CU09** and click **Uninstall**.

NOTE: To uninstall the CrossFireWebService you need to manually uninstall it via **Programs and Features.** You would then need to reinstall the previous version of CrossFireWebService which can be found in **2.60 Media>ISOImage>Bin**.

3. SPARs Fixed

This critical update includes the following SPAR fixes:

441214
The configuration field **Card Number (for matching only)**, when used as one of the **Personnel Match Fields**, now allows personnel records to be imported without error.

444114
Wireless IP locks and readers are no longer counted as regular readers against license counts.

444117
Custom Clearance can now be configured for third-party doors.

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Security System

Version 2.60 Release Notes – January 2017
Contents

For a list of supported operating systems, see **Section 4**.

IMPORTANT:
Read before upgrading and installing C•CURE 9000 version 2.60
Firmware v 6.5.0 is not included with C•CURE 9000 v 2.60 installer software.
Firmware v 6.5.0 is required for certain C•CURE 9000 v 2.60 features. Navigate to the Software House website to download firmware v 6.5.0.

IMPORTANT:
Read before upgrading and installing C•CURE 9000 version 2.60 on Windows Server 2012R2
Windows Update KB2919355 is required for installation of .Net 4.6.1. If your system does not have KB2919355, installation of .Net 4.6.1 stops and an error message appears with a link to download the Windows Update from Microsoft Support. After clicking the link, you must complete the following:

1. Follow the instructions on the Microsoft Support page and install the **Clearcompressionflag.exe** tool for your specific Windows OS.
2. Install KB2919355.
   This will complete installation of .NET 4.6.1.

IMPORTANT: Read before upgrading to C•CURE 9000 Version 2.60 from 2.40 and 2.41
C•CURE 9000 v2.60 requires a new HostID generated license, unless the system is already at 2.50, and you must do the following on your existing system before starting the upgrade process:

1. Run the **HostIDUtil.exe** to get the new HostID of your existing system – this utility resides at the root level of the new 2.60 installation package or DVD media.
2. Make an upgrade license request, using the new HostID - http://www.swhouse.com/Support/upgrade_center.aspx
3. Receive a new license file (.tlic) from the licensing team.
4. Run the C•CURE 9000 v2.60 Installer (**Setup.exe**) to start the upgrade process and apply the new license file (.tlic)

If you are upgrading to C•CURE version 2.60 from 2.50 you do NOT need a new HostID.

IMPORTANT: Read before upgrading to C•CURE 9000 Version 2.60 from 2.40 and 2.41
Upgrading from 2.40 to 2.60 may result in the deletion of journal backup files. Before upgrading, you must save the contents of the Tyco\CrossFire to a location outside of the folder where C•CURE 9000 is installed. After upgrading, the saved files must be copied back to the original location.

IMPORTANT: C•CURE 9000 SiteServer Upgrade Information
Go to http://www.swhouse.com/Support/upgrade_center.aspx to download and read the C•CURE 9000 v2.60 SiteServer Upgrade Release Notes before you upgrade your SiteServer.

1. DVD Contents

This dual-layer DVD includes the C•CURE 9000 from Software House and the victor product in support of American Dynamics and Unified deployments. The DVD also includes the supporting Services, Integration drivers, and latest firmware for both products.

NOTE: The C•CURE 9000 Server component is now named the "victor Application Server".

- C•CURE 9000 Install components ("*victor Application Server"* and *"C•CURE 9000 Client*")
- EULA.rtf – End User License Agreement.
- HostIDUtil.exe – HostID Application.
- 2.60_Relnote_8200-1367-27_B0.pdf – the C•CURE 9000 v2.60 Release Notes file.
- The following Quick Start Guides:
    - UNIFIED Quick Start Guide.pdf - the Unified Installer Quick Start Guide.
    - CCURE Quick Start Guide.pdf –the CCURE Quick Start Guide.
    - victor Quick Start Guide.pdf – the victor Quick Start Guide.
- Setup.exe – Executable to launch the installation dashboard.
- Certificates folder containing security certificate files.
- Bin folder containing supporting installers and support files for C•CURE 9000 and victor products. Installers should be installed via the installation dashboard, **not** through individual install files.
- A Manuals folder containing folders with PDF (Portable Document Format) manual files in the following languages:
    - English
    - German
    - Spanish
    - French
    - Italian
    - Portuguese
- Integrations folder containing installers and support files for DSC and Galaxy Intrusion integration software.
- Prerequisites folder containing prerequisite software requirements for C•CURE 9000 and victor.
- ThirdParty folder containing support files for C•CURE Mobile handheld reader.

NOTE: The Intellex, Video Edge, and HDVR/Exacq video drivers are included with this 2.60 release.

2. New Features and Enhancements

Access Management Portal – a licensed feature for designated personnel to directly manage formal access requests in the C•CURE Portal. Personnel are designated as requesters or approvers in C•CURE 9000 and use the C•CURE Portal to manage access requests in the following ways:

- **Requesters** create and submit access requests directly to approvers who are authorized to grant clearance.

- **Approvers** are Personnel who are ultimately responsible for access to a location. An Approver can approve or reject access requests. More importantly, even without requests, an Approver can simply audit a location in order to revoke clearance assignments from personnel.
- **Clearances** can additionally be configured so that they are approved before Personnel assignment. Selected clearances requiring approval will not be assignable through the standard C•CURE interfaces, but through the C•CURE Portal.
- **Access Request Site** objects are used to establish locations for clearance management in the C•CURE Portal. Separate sites used by requesters and approvers to create and manage access requests in the Access Management application in C•CURE Portal.
- **Doors** can also be configured to automatically initiate an Access Request when a known card is rejected for clearance at the door.

For more information, see the *C•CURE 9000 Visitor and Access Management Guide*.

Expiring Clearances per Person – a standard feature for configuration of Clearances for iSTAR Ultra series Doors and Elevators that support individual activation and expiration date and time per person. When an expiring clearance is assigned to a person, the start date and end date of that clearance displays in their personnel record. The new Access Management Portal can use expiring clearances so that requesters and approvers can set the Start Date and Time, and the End Date and Time, of the clearance assignment. Support for up to a maximum of 1,000 combined clearances per person (standard/custom/expiring) is supported in iSTAR Ultra series controllers. For more information, see the *C•CURE 9000 Personnel Configuration Guide.*

Visitor Management Phase III – a countable license feature for the new C•CURE Kiosk iOS application. This application provides a self-check-in facility for scheduled and unscheduled visitors. Check-in Site objects are configured to specify C•CURE Kiosk options:

- Taking a visitor portrait with the device's camera.
- Automatic visitor check-in.
- Accepting unregistered visitors.
- Acknowledgement of documents, such as NDAs.
- Customizing messages displayed to visitors during visitor registration.

The C•CURE Kiosk application only supports iOS devices and does not support Android. For more information, see the *C•CURE 9000 Visitor and Access Management Guide.*

Privileges – Visitor Management Kiosk has been added to the list of Application Clients that can be assigned to an Operator Privilege. This provides Operators with permission to login and set up the C•CURE Kiosk iOS application for visitor self-check-in. For more information, see the *C•CURE 900 Software Configuration Guide*.

Personnel Quick Search – a standard feature that has been enhanced in 2.60 to provide C•CURE 9000 administrators with additional criteria when searching Personnel records:

- In addition to the existing check boxes in the Personnel Quick Search view, two check boxes have been added:
  - Can Approve Requests
  - Can Submit Requests
- In addition to the existing search fields in the Personnel Quick Search view, two default search fields have been added:
  - Personnel Quick Search Field1
  - Personnel Quick Search Field2

  These default search fields can be customized with a User-Defined Field (UDF) so that an administrator can search Personnel Records based on a text, integer, or date value. For example, an administrator can

create a Visit Purpose UDF, and assign it to one of the two new fields so that this criteria displays in the search results of a Personnel quick search.

For more information, see the *C•CURE 9000 System Maintenance Guide*.

ID Scanner and EV1 encoding support for C•CURE ID badge – an enhanced feature that now supports Scanshell and Snapshell scanners for personnel data enrollment. The ID Scanner utility can be configured to map data from driver's licenses or passports to fields in the Personnel editor when creating or editing a Personnel record. You can also use the ID Scanner to detect information in a driver's license or passport and initiate a quick search of Personnel and Visits in C•CURE 9000 database. Current smart card programming and enrollment capabilities have been extended to support MIFARE DESFIRE EV1 Encoding, which will be implemented in 2.60 SP1.

C•CURE Web– the next generation version of C•CURE Web Client. This new licensed feature provides independent browser support and improved user experience with the following features:

- Dockview management
- Site Explorer for doors, inputs, outputs and controllers.
- Manual actions for access control devices:
    - Door actions – Locking and unlocking
    - Input actions – arming and disarming
    - Event actions
- Swipe and Show
- Personnel Monitoring
- Basic Reporting:
    - Access Reports
    - Audit Logs
    - Activity Journals

For more information, see the *C•CURE Web Installation and User Guide.*

Enterprise Multiple Global Partitions – an enhanced feature that supports multiple global partitions in an Enterprise environment. You can configure multiple Global partitions in addition to the MAS system default **Global** partition. By configuring multiple partitions, C•CURE Administrators have more organization options for the objects within the Enterprise system. This feature is a convenient way to divide the system in a way that makes sense for operators and administrators, giving them permissions to see certain objects and not others. For instance, a business with global personnel can use multiple global partitions to regionally divide personnel and clearances. SAS administrators and operators only see Global groups and objects relevant to their region. The Administrators in the MAS can see all the Global partitions as well as the partitions of each SAS. There is no limit on the amount of global partitions you can have on a MAS. For more information, see the *C•CURE 9000 Enterprise Architecture Guide*.

Local time zone awareness for monitoring and reporting – a standard feature that uses the **Toggle Event Local Display** button in the Event Viewer in the Monitoring Station to display the local time and date of an event if the event occurs outside of the Monitoring Station Operator's time zone. For more information, see the *C•CURE 9000 Monitoring Station User Guide*.

Email Configuration – email configuration options have been enhanced to increase the reliability of the application's email. The upgraded Email Configuration editor now provides the option to:

- Poll an email server to make sure that it is communicating and functioning.
- Configure settings for re-sending emails.
- Add a journal message when an email is unsent and deleted.

For more information, see the *C•CURE 9000 Software Configuration Guide*.

Random Screening – a standard feature that randomly screen personnel as they swipe their card to gain access in or out of a facilities perimeter, or a sensitive area. You can configure a random access percentage frequency per door, which creates an unpredictable pattern of card rejection. When an access request is rejected, an event is activated. This event can be associated with an output such as a light or buzzer that notifies the guard or operator for further action. After screening is completed, the event can be acknowledged and cleared, and access can be granted. You can configure door(s) to operate in Random Screening mode permanently or under schedule, or enabled/disabled by an event. Random screening is supported in iSTAR Ultra doors only. For more information, see the *C•CURE 9000 Hardware Configuration Guide.*

Double Swipe Operation Mode - a standard feature that now supports two different double card-swipe modes to unlock an iSTAR Door:

- **Toggle Mode** – unlocking an iSTAR Door requires double swipe of a single card at a reader.
- **Two Person Mode** - unlocking an iSTAR Door requires two separate personnel card swipes at a reader.

Clearance permission to card-holders options have been enhanced to support team rules requiring personnel from different personnel groups. Double swipe operation mode is supported only in iSTAR Ultra controllers in Ultra mode. For more information, see the *C•CURE 9000 Hardware Configuration Guide.*

iSTAR Ultra DB sync monitoring and notification – a new utility intended for Technical Support for diagnostic purposes only. This feature retrieves credential data from an iSTAR Ultra panel and then compares the data between the panel and the victor Application Server. After the comparison is complete, any inconsistencies appear as a list.

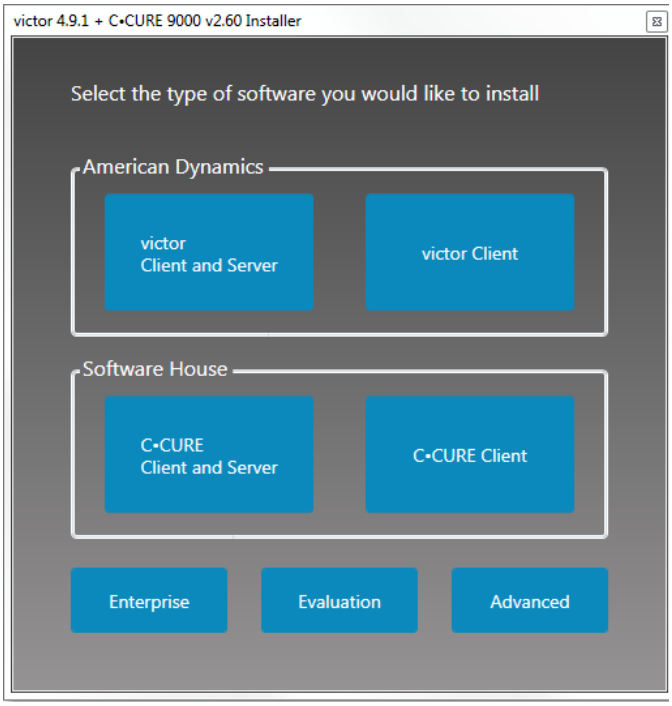
After-Hours Enabling Reader Group – a standard feature that administartors use to identify a Group of readers that are disabled during a defined After-Hours period. Readers can be configured as Enabling Readers, so that cardholders with clearance can gain access to a Door that is normally restricted after business hours. After a card has been presented and accepted at an Enabling Reader, the reader has access to any reader objects in an After-Hours group who have valid clearance for the remainder of the schedule. For more information see the *C•CURE 9000 Hardware Configuration Guide*.

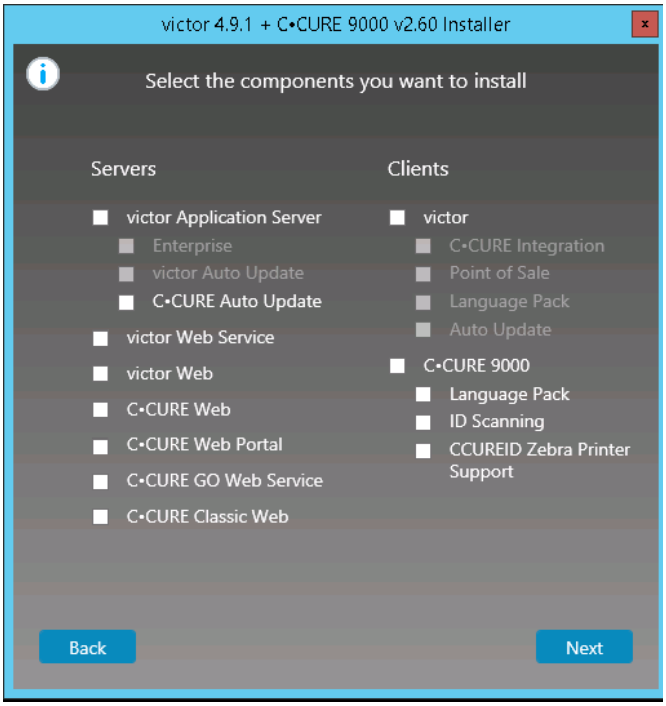
IPv6 Support – In addition to IPv4 protocol, C•CURE 9000 now supports IPv6 communication to clusters with IPv6 iSTAR Ultra controllers in a standalone environment. IPv6 support allows for a significant increase in available IP addresses, so that you can allocate individual IP addresses to controllers or WiFi enabled devices. For more information, see the *C•CURE 9000 Hardware Configuration Guide*.

Event activation after consecutive rejections – a standard feature that administrators use to configure the number of consecutive rejections, and the time period during which consecutive rejects are counted. These consecutive rejects can include card rejections, incorrect PIN number entries, incorrect keypad commands, or incorrect keypad entry of card numbers. If the number of consecutive rejects occurs before the timer expires, a pre-defined event message displays in the Monitoring Station. For more information, see the *C•CURE 9000 Hardware Configuration Guide.*

3. Upgraded Unified Installer

The Unified Installer has been technically enhanced to reduce the complexity of C•CURE 9000 and victor software installation screen flows, and the interface has been re-designed to improve usability. You can select victor Application Server and associated services and applications, and also select victor Client and C•CURE Client and associated options. The upgraded Unified Installer replaces the traditional InstallShield Wizard to perform a silent install after installation components have been selected.





4. Supported Operating Systems, DBMS, and SQL Collations

For support information for Operating Systems, DBMS's, and SQL Server Collations, see Table 1, Table 2, and Table 3 respectively.

NOTE: There are limitations on full client support for 64-bit.

Table 1: Microsoft Operating Systems for Server and Client

Server Series L/M/N/SAS	**Supported Version**
Windows 7 Professional SP1 or later	64-bit
Windows 7 Enterprise SP1 or later	64-bit
Windows 8.1 Professional SP1 or later	64-bit
Windows 8.1 Enterprise SP1 or later	64-bit
Windows Server 2008 R2 Standard SP1 or later	64-bit
Windows Server 2008 R2 Enterprise SP1 or later	64-bit
Windows Server 2012 R2 Standard SP1 or later	64-bit
Windows 10 Professional	64-bit
Windows 10 Enterprise	64-bit
Server Series P/Q/R/R+/S/S+/T/SAS	**Supported Version**
Windows Server 2008 R2 Standard SP1 or later	64-bit
Windows Server 2008 R2 Enterprise SP1 or later	64-bit
Windows Server 2012 R2 Standard	64-bit
MAS Server	**Supported Version**
Windows Server 2008 R2 Standard SP1 or later	64-bit
Windows Server 2008 R2 Enterprise SP1 or later	64-bit
Windows Server 2012 R2 SP1 or later Standard	64-bit

Client	Supported Version
Windows 7 Professional SP1 or later	64-bit
Windows 7 Enterprise SP1 or later	64-bit
Windows 8.1 Professional SP1 or later	64-bit
Windows 8.1 Enterprise SP1 or later	64-bit
Windows 10 Professional	64-bit
Windows 10 Enterprise	64-bit
Windows Server 2008 R2 Standard SP1 or later	64-bit
Windows Server 2008 R2 Enterprise SP1 or later	64-bit
Windows Server 2012 R2 SP1 or later Standard	64-bit

Table 2: Microsoft DBMS

Server Series L/M/N/SAS	Supported Version
SQL Server 2008 R2 Standard	SP2 or later (64-bit)
SQL Server 2008 R2 Enterprise	SP2 or later (64-bit)
SQL Server 2012 Express	SP2 or later (64-bit)
SQL Server 2012 Standard	SP2 or later (64-bit)
SQL Server 2012 Enterprise	SP2 or later (64-bit)
SQL Server 2014 Express	SP1 or later (64-bit)
SQL Server 2014 Standard	SP1 or later (64-bit)
SQL Server 2014 Enterprise	SP1 or later (64-bit)
SQL Server 2016 Express	(64-bit)
SQL Server 2016 Standard	(64-bit)
SQL Server 2016 Enterprise	(64-bit)
Server Series Standalone P/Q/R/R+/S/S+/T	**Supported Version**
SQL Server 2008 R2 Standard	SP2 or later (64-bit)
SQL Server 2008 R2 Enterprise	SP2 or later (64-bit)
SQL Server 2012 Standard	SP2 or later (64-bit)
SQL Server 2012 Enterprise	SP2 or later (64-bit)
SQL Server 2014 Standard	SP1 or later (64-bit)
SQL Server 2014 Enterprise	SP1 or later (64-bit)
SQL Server 2016 Standard	(64-bit)
SQL Server 2016 Enterprise	(64-bit)
SAS Server Series P/Q/R/R+/S/S+/T	**Supported Version**
SQL Server 2008 R2 Standard	SP2 or later (64-bit)
SQL Server 2008 R2 Enterprise	SP2 or later (64-bit)
SQL Server 2012 Standard	SP2 or later (64-bit)
SQL Server 2012 Enterprise	SP2 or later (64-bit)
SQL Server 2014 Standard	(64-bit)
SQL Server 2014 Enterprise	SP1 or later (64-bit)
SQL Server 2016 Standard	SP1 or later (64-bit)
SQL Server 2016 Enterprise	(64-bit)
MAS Server	**Supported Version**
SQL Server 2008 R2 Standard	SP2 or later (64-bit)
SQL Server 2008 R2 Enterprise	SP2 or later (64-bit)
SQL Server 2012 Standard	SP2 or later (64-bit)
SQL Server 2012 Enterprise	SP2 or later (64-bit)

SQL Server 2014 Standard	SP1 or later (64-bit)
SQL Server 2014 Enterprise	SP1 or later (64-bit)
SQL Server 2016 Standard	(64-bit)
SQL Server 2016 Enterprise	(64-bit)

Table 3: SQL Server Collations Supported

Windows Locale	Default Collation
Arabic (Saudi Arabia)	Arabic_CI_AS
Chinese (PRC)	Chinese_PRC_CI_AS
Chinese (Taiwan)	Chinese_Taiwan_Stroke_CI_AS
Czech (Czech Republic)	Czech_CI_AS
Danish (Denmark)	Danish_Norwegian_CI_AS
Dutch (Netherlands)	Latin1_General_CI_AS
English (United Kingdom)	Latin1_General_CI_AS
English (United States)	SQL_Latin1_General_CP1_CI_AS
French (France)	French_CI_AS
German (Germany)	Latin1_General_CI_AS
Hungarian (Hungary)	Hungarian_CI_AS
Italian (Italy)	Latin1_General_CI_AS
Japanese (Japan)	Latin1_General_CI_AI
Korean (Korea Dictionary Sort)	Korean_Wansung_CI_AS
Polish (Poland)	Polish_CI_AS
Portuguese (Brazil)	Latin1_General_CI_AS
Russian (Russia)	Cyrillic_General_CI_AS
Spanish (Spain)	Modern_Spanish_CI_AS
Swedish (Sweden)	Finnish_Swedish_CI_AS
Turkish (Turkey)	Turkish_CI_AS

5. Supported Browser and Mobile Operating Systems

IIS Versions	**2.60**
IIS Web Server	v8 or higher
C•CURE Go	
Android	Supported
iOS	Supported
C•CURE 9000 Web Client Classic	
Internet Explorer (Silverlight required)	Supported
C•CURE Web	
Internet Explorer	Supported
Edge	Not Supported
Chrome	Supported
Firefox	Supported
Safari	Supported
C•CURE Portal	**Visitor and Access Management**
Internet Explorer	Supported
Edge	Not Supported
Chrome	Supported

Firefox	Supported
Safari	Supported
C•CURE Kiosk	
Android	Not Supported
iOS	iPad device only. Phones and other iOS devices are not supported.

6. Redundancy and Disaster Recovery

Versions	v2.40	v2.50	v2.60
Stratus everRun MX	6.2	6.2	X
Stratus everRun Enterprise	7.2.1.339	7.2.1.339	7.3
C•CURE 9000 Warm Standby	Supported	Supported	Supported

7. Enterprise Architecture Considerations and Known Limitations

5.1 Installation and Upgrade Issues

5.1.1 Using SQL Server Express with SAS Server L/M/N Upgrades

The use of SQL Server Express is supported for upgrades of SAS Servers Series L/M/N. However, for the best performance, Software House recommends using full SQL Server Standard/Enterprise with C•CURE 9000 v2.60. Please refer to the datasheet for applicable SQL Server versions compatible with C•CURE 9000 v2.60.

5.1.2 SAS and Licensing

Once a SAS is successfully licensed and installed, simply changing the license to standalone will not convert the SAS, rather it will prevent it from starting at all.

5.1.3 Relation between SAS and its MAS

There is no way to point an existing SAS at a different MAS. **Consequently, it is critical to perform a system backup of the MAS before each new SAS is added**, in case it becomes necessary to revert the enterprise back to before a given SAS was added. In the same vein, you cannot remove a SAS from a MAS once it has been installed into the Enterprise Architecture System.

5.1.5 Upgrading MAS before its SAS

It is required that when you upgrade your MAS and SAS systems, you first upgrade the MAS and then upgrade the SAS systems to the same version. Otherwise—if you upgrade your SAS systems first, those SASes will require another full restart once you've upgraded the MAS.

5.1.6 Synchronizing Journal before Upgrading from v2.30/2.30 R2/2.50 to v2.60

Prior to upgrading your MAS and SAS systems from v2.30/2.30 R2/2.50 to v2.60, you should verify that any scheduled Journal Synchronization from SAS to MAS has been completed.

Caution: You should close the 'CrossFire Server Component Framework Service' prior to performing this last synchronization. If you do **not** synchronize before upgrading to v2.60, unsynchronized journal messages from v2.20/2.30/2.30 R2 will never sync to the MAS. (For more information about the Application Server Synchronization tab, see Chapters 4 and 10 in the *C•CURE 9000 Enterprise Architecture Guide*.)

5.1.7 Upgrading SAS While Server Not Configured/Running Correctly May Fail

If you try to upgrade a SAS when the server is non-functional (drivers stuck in loading state, for example), the upgrade may fail. Subsequent attempts to run a repair may also fail.

Workaround:

1. Do **not** attempt to upgrade such a system.
2. Run a repair first.
3. Make sure the repair was successful.
4. Re-start the upgrade.

5.1.8 Converting a Standalone C•CURE 9000 System with UDFs to a v2.60 SAS

You **cannot automatically convert** a C•CURE 9000 v2.30/2.30 R2/2.50 system with User Defined Fields (UDFs) to a v2.60 SAS. For detailed instructions, see Chapter 2 of the *C•CURE 9000 Standalone to SAS Migration Utility User Guide*—located in the Manuals subdirectory on the application DVD or in the Technical Library on www.swhouse.com.

5.1.9 Upgrading Enterprise System with SAS Once Standalone C•CURE 9000 to v2.60

If you are upgrading an Enterprise System with a SAS that was once a Standalone system to v2.60, you may need to do the following after the SAS is upgraded and fully running: stop and then re-start any running Administration/Monitoring Station applications connected to the MAS. This allows the application to access certain Enterprise functions, such as Synchronization Conflict Views.

5.1.10 Uninstalling MAS with Server Management Application Open Causes Error

If you try to uninstall a MAS without closing the Server Management Application, the following message displays: "Server Management Application must be closed to proceed. Do you want to close the Server Management Application now?" If you click **No**, the uninstall seems to proceed and complete. However, at the end when you click **Finish**, a fatal error message displays and the uninstall was **not** successful.

5.2 Application Layouts on MAS

You may **use** the three pre-defined Application Layouts (Default View 1/Default View 2/ Default Application Layout) on the MAS, but should **never edit** them. Software House recommends you create at least one new MAS Application Layout that you assign to all Operators—to avoid the need to edit the pre-defined Layouts.

5.3 Editing Global Operators

You should **not** edit Global Operators if you are logged into the system as a Local Operator because you will not be able to save Application Layouts correctly.

5.4 Importing Considerations

- For performance reasons, imports should be done on the server that owns that Object's partition.
  Example:
  Global data should be imported on the MAS, and Local data should be imported on the SAS that owns it.
- Very large imports can cause the MAS performance to significantly degrade when synching with the SAS. Importing personnel records with attached documents and/or images can use significant amounts of memory during replication. Software House recommends you keep imports down to a total of 400MB, including both Image and Document data.
  Example:
  3000 personnel with 500KB Documents for each personnel record = 1.5GB of memory to process.

5.5 Replication of Images

The Enterprise architecture only supports replication of personnel and badge images if the images are 3.75 MB or smaller. Therefore, be sure all your images are smaller than 3.75 MB. If an image larger than 3.75 MB is encountered, no further images will be replicated until that image is removed or resized.

8. General Considerations and Known Limitations

6.1 Windows 7, Windows 8.1, and Windows 10 Operating System Support

C•CURE 9000 supports client and server installation on:

- Windows 7 Professional (SP 1) and Enterprise (SP 1).
- Windows 8.1 Professional and Enterprise.
- Windows 10 Professional and Enterprise.

The following limitations exist when running a C•CURE 9000 Client on these operating systems:

- Digi International WatchPort/V2 USB Camera - Not supported.
- Penware 100 signature tablet - Not supported.
- Bioscrypt - The VeriAdmin application used to configure Bioscrypt readers does not support Windows 7, 8.1, or 10. You can configure the readers using a separate workaround.
- Edge browser – the Windows 10 Edge browser is not supported.
- Third party integrations – check with the vendor for Windows 10 client support.

6.2 Windows Server 2008 R2 and Windows 2012 R2, Windows 2014, Operating System Support

C•CURE 9000 supports client and server installation on:

- Windows Server 2008 R2 Standard and Enterprise SP2 or later.
- Windows Server 2012 R2 Standard SP1 or later.

The following limitations exist when running a victor Application Server on these operating systems:

- Digi International WatchPort/V2 USB Camera - Not supported.
- Penware 100 signature tablet - Not supported.
- Bioscrypt - The VeriAdmin application used to configure Bioscrypt readers does not support Windows Server 2008 R2 or Windows 2012 R2. You can configure the readers using a workaround, if one is provided by the manufacturer.

6.3 64-Bit Operating System Support with C•CURE 9000 Client

The Tango Magiccard 32-bit setup **cannot** be run on a C•CURE 9000 Client on a 64-bit operating system.

6.4 SQL Database and Backup

The hard drive partition you install the C•CURE 9000 database on requires a minimum of 80 GB free space.

6.5 ISC Controllers

C•CURE 9000 v2.60 does **not** support ISC Controllers. (This includes Classic Web Client and C•CURE Web Client).

6.6 Maximum Time for iSTAR Controller Certificate Signature Timeout

iSTAR eX/Edge/Pro controllers use five minutes as the maximum time for “Controller Certificate Signature Timeout.” Thus, if you do not approve certificate requests when changing to controller-based encryption mode, the iSTAR reboots at five minutes—even if you configure a timeout period greater than five minutes.

6.7 Editing iSTAR Input Trigger Causes Output To Stay Active

If you configure and save a trigger for an iSTAR Input that uses the Armed status value to activate an Output and you edit the trigger to change the Armed status value after the Output has been activated, the Output stays active. To change the trigger so the Armed status value for the trigger updates properly, you need to delete the trigger and re-create it with the new value for Armed status.

6.8 apC Panels

6.8.1 apC Panel Limitations with Timed Actions

Under certain circumstances, apCs do **not** behave the same as iSTARs when they lose communication with the host. The host to apC connection supports a limited timed Action capability that works well for locking/ unlocking

Doors, activating/deactivating Outputs, etc. If, however, there are overlapping or conflicting timed Actions at the apC when power or communication is lost, the results are indeterminate.
Example: If there is a manual Door lock timed Action for an hour and a scheduled host-based Event to unlock the Door during that time, the host will sort it out. On the other hand, if the host is not communicating, the apC may or may not restore everything correctly. Software House recommends that you keep apC timed Actions simple—to avoid overlapping conflicting Actions.

6.8.2 Scheduled Events on apC Door, Input, and Output Groups
Events configured to unlock an apC Door Group, arm an apC input Group, or activate a group of apC outputs according to a Schedule do **not** work if the apC panel is offline.

6.8.3 Event Activation Delay Time and/or Minimum Activation Time Ignored if apC is Offline
In offline mode the apC does **not** support Activation Delay Time and Minimum Activation Time. Consequently, if an Event configured with Activation Delay Time and/or Minimum Activation Time activates while the apC is offline, the action will be performed immediately when the apC comes back online.

6.8.4 apC Event Action Activation Message Not Reported under Certain Circumstances
Timed Actions that occur when the apC is offline may not report (display on Monitoring Station) when the apC comes back online.

6.8.5 apC Connected to a different server needs to be reset before Clearance download.
If an apC is connected to a new C•CURE 9000 Server, the panel must be reset in order to correctly download Clearances.

6.9 Restrictions for Cross Panel Events between apC Panels and iSTAR Controllers
You can configure an apC Door or Input Trigger to activate an iSTAR Event, but if the Event is configured with the **Download to compatible controller** option, it will **not** activate. Either of the following will work:

- Configure the apC Door/Input Trigger to activate a host-based Event that in turn activates the iSTAR Event.
- Do not select the **Download to compatible controller** option for the iSTAR Event.

6.10 Requirement for Adding PIN-only Card from Personnel View
If you want the capability to add a PIN-only Card from a Personnel View, you must ensure that the Auto Generate button in the PIN Credential box on the Personnel View is **not** hidden.

6.11 Fingerprint Capture Attempt Causes Exception Violation and Locks Administration Client
If you are using Bioscrypt, before trying to capture a fingerprint follow the workaround directions.
Workaround: Copy the BII_V1100.dll file from the Bioscrypt install directory to the Client \Badging directory.

6.12 Areas
6.12.1 Using Escorted Access with Muster/De-muster
If you are using the Escorted Access feature with Muster/De-muster, make sure that the De-muster Area does **not** have the “An Escort must always be present in Area with Escorted Visitors” check box selected.

6.12.2 Offline Transactions Cause Host Occupancy Counts to be Unreliable on iSTARs
A Cluster member iSTAR that goes into communications failure may still try to make occupancy decisions. When communications are restored, delivery of the delayed transactions invalidates the area counts at the host. This situation is made even worse if the “Always Track Personnel” system variable is set to ‘True’.

6.12.3 Remove All Personnel from Area Command Does Not Remove Personnel from Area
The ‘Remove All Personnel from Area’ command from the iSTAR Area Context Menu changes the Personnel records in the host, setting their ‘Area’ to a zero value. In addition, a Dynamic View of Personnel who were in the Area no longer shows a value in the Area column, and the ‘Show Personnel in Area’ command for the Area

displays an empty Dynamic View. However, the iSTAR controllers do **not** change the location of Personnel in that Area, so an Operator may have to grace Personnel for them to be granted access when swiping their cards. This is true if Antipassback is configured. In addition, the Personnel count for the Area is **not** reset in the iSTAR controllers, requiring an operator to use the 'Clear Area Counts' command on the Area to update the counts.

6.13 Aperio Doors

6.13.1 Aperio Doors Do Not Re-lock on Access Completion

Aperio Doors do **not** re-lock, as other iSTAR doors do, after being opened and then closed. They re-lock at the expiration of the unlock time.
Workaround: Configure the Doors to shunt for the full shunt time regardless of the Door lock/relock status.

6.13.2 Aperio Doors Become Disabled by the All Doors Group Unlock Manual Action

If you perform an Unlock Manual Action on the All Doors Group, Aperio Doors in the Group will be disabled—reading presented Cards, but **not** unlocking the Door. Software House recommends that you **not** perform manual actions on the 'All Doors Group'.

6.13.3 Aperio Doors Do Not Support Lock/Unlock/Momentary Unlock Manual Actions

Aperio Doors do **not** support Lock/Unlock/Momentary Unlock Manual Actions on the Monitoring Station or the Web Client.

6.14 Redundancy: EMC AutoStart and RepliStor

C•CURE 9000 v2.60 does not support EMC AutoStart or RepliStor products due to their End-Of-Life status.

- C•CURE 9000 v2.30 R2 is the last qualified version of C•CURE 9000 to provide support for EMC Autostart v5.5, which will reach End-Of-Life in July 2015.
- C•CURE 9000 v2.20 is the last qualified version of C•CURE 9000 to provide support for EMC RepliStor, which reached End-Of-Life in June 2013.

NOTE: If you have questions about redundancy support or planning new redundancy deployments, please contact your local Software House Sales Representative.

6.15 Intellex Comm Loss Alarm Does Not Respect Configured Poll Period/Comm Fail Delay

It takes up to three minutes to report state changes for the Intellex when communications are lost whether you configured a specific Poll Period or Comm Fail Delay time or not.

6.16 Language Pack Upgrade and Repair Requirements

If you are upgrading your C•CURE 9000 to v2.60 and currently have the C•CURE 9000 Language Pack installed, you must also upgrade the Language Pack. Make sure that during the upgrade process the Language Pack option on the Dashboard Integration and Services Screen remains selected (checked).
In addition, if you are repairing a C•CURE 9000 with an installed Language Pack, you also must repair the Language Pack.

6.17 Legacy Maps

Privileges assigned to Legacy Maps prior to 2.30R2 are not included in the conversion to new Map formats. It is recommended that you create a new Privilege, or update current Privileges to use this new Maps type.

6.18 ID Scanner

6.18.1 OS support

The Accuant IDScanners Snapshell R2 and Snapshell Passport are only supported in Windows 7.8, 8.1 and 10. Windows Server does not support these ID Scanners.

6.18.2 Hologram logos on the front side of driver's licenses and passports may interfere with scanning

Due to the variation in layouts of driver's licenses and passports, the hologram logo on the front side of the ID may interfere with the ability of the ID scanner to scan information. It is recommended that you configure the ID scanner settings to scan on both sides.

6.18.3 Delay of 5-10 seconds when performing ID Scanner

There is a 5-10 second delay between performing an ID Scan and receiving data from the ID Scanner.

6.18.4 Performing ID scan on two Administration Stations simultaneously may result in a failed scan

If users perform an ID scan simultaneously on two Administration Stations on the same machine, a failed scan may occur because the ID Scanner SDK can only be used on one Administration Station at a same time.

6.19 C•CURE Kiosk

6.19.1 C•CURE Kiosk generates license error during login despite using correct credentials

If a C•CURE Kiosk session is terminated without performing the correct log-out procedure, the C•CURE 9000 server does not assign the C•CURE Kiosk license the next time an operator attempts to login. Either of following can be used as a workaround:

- Wait for approximately two minutes for C•CURE 9000 to re-assign the license.
- To release all the licenses back to the C•CURE 9000 server, restart the Internet Information Services (IIS) server that hosts the victor Web Service.

6.19.2 Visitor registration fails in C•CURE Kiosk if Email settings are not configured in C•CURE 9000

If Email settings have not been configured in C•CURE 9000, or if the Email server has been shut down, C•CURE Kiosk displays an error message at the end of the registration process to indicate that visitor registration has failed. For more information about configuring Email settings in C•CURE 9000, see the *C•CURE 9000 System Maintenance Guide*.

6.19.3 C•CURE Kiosk does not login after initial install

After initial install of the C•CURE Kiosk, there may be login issues where login credentials are recognized but no Check-in Sites display, and the C•CURE Kiosk reverts to the login screen. To work-around this issue, you must delete the C•CURE Kiosk application cache in the iPad and login again.

6.19.4 Multi-line User defined fields (UDFs) are not supported in the C•CURE Kiosk

If you assign a Multi-line UDF to a Visit Site, the UDF that displays in the C•CURE Kiosk is a regular text field that does not have the attributes of the Multi-Line UDF.

9. Compatibility of Third Party Hardware

The following list includes some of the third-party products compatible with C•CURE 9000 Version 2.60.

Table 4: Third-Party Hardware

Equipment Type	Vendor	Model	Latest Supported Version
Digital Video Management System	American Dynamics	Intellex	5.0
Digital Video Management System	American Dynamics	NVR	4.9
Digital Video Management System	American Dynamics	HDVR	1.7 2.1 2.2
Digital Video Management System	Exacq	Exacq	7.8.2.98464
Biometric Readers	Bioscrypt	V-SMART I CLASS V-STATION I CLASS	7.5K Soft. 5.50 7.30 Soft. 5.51
Wireless Reader/ Locks	Schlage	AD-400/401 AD-300/301	AD.A.60 AD.A.60
Wireless Reader/ Locks	Assa Abloy	Aperio	Hub: 6.2.28176
Signature Capture	Topaz Topaz USB PenWare 100	T-S261-B T-S261-HSB PW100	3.0.3 4.4.0 4.5.0
USB Badging Cameras	Video Associates Videology	Val Cam VA – 3 USB Camera 2X USB TWAIN	6.1.76.00 7.7 9.0 2.1.18
ID Scanners	Acuant Acuant	ScanShell R2 SnapShell Passport	SDK 10.11.04.00 SDK 10.11.04.00
IP Cameras	AXIS	2400/2401	2.33
Badging Printers	Fargo Fargo Magicard Magicard Magicard NISCA DYMO	HDP 5000 DTC 4500E Prima 4 Pronto Rio Pro P5350 450 Series	3.3.3.0 2.1.0.3.2 8.01 2.0.13.0 2.0.13.0 5.12 N/A
Smart Card Device	SCM Microsystems	SDI010	5.21
C•CURE Mobile	Datastrip	DSV 11SG	1.0.63.46

10. Compatibility of Third Party Software

The following list includes some of the third-party software compatible with C•CURE 9000 Version 2.60.

Table 5: Third-Party Software

Company	Product	Latest Supported Version
Data Dynamics	Active Reports	6.2.3681
American Dynamics	Intellex API	5.00.74.189
Flexera	FLEXNet Publisher	11.10.1
LEAD Technologies	LEADTOOLS	14.5.0.68
Infragistics	Infragistics	14.2
Microsoft	.NET	4.6.1 3.5 required if installing SQL Server
	Windows Installer	4.5
	MFC Runtime	9.0 SP1,10.0 SP1, 11.0, and 12.0
	Silverlight	5.0.61118.0
WIX		3.9R2
Sequiter Inc	CodeBase	6.5
Stratus	everRun MX	6.2
	everRun Enterprise	7.2.1.339
Stunnel	Stunnel	5.00
The OpenSSL Project	OpenSSL	1.0.1h
Apache	CouchDB	1.6.1
Joyent, Inc	Node.js	0.12.7

11. Firmware Versions for Tyco Security Products Controllers

The following list includes the firmware versions for the controllers for C•CURE 9000 Version 2.60.

Table 6: Firmware for Tyco Security Products Controllers

Controller	Latest Supported Version
iSTAR Classic	4.4.C
iSTAR Pro,ex	5.2.C
iSTAR Edge, eX	6.2.3
iSTAR Ultra	6.5.X
iSTAR Ultra SE	6.5.X
iSTAR Ultra LT	6.5.X
iSTAR Ultra Video	6.5.X
IP-ACM	6.5.X
apC, apC/8x, apC/L	x.72F

12. SPARs Fixed

44960 – The search functionality has been enhanced to allow a customizable quick search of objects.

162038 – The **Acknowledge** button correctly states and records single manual actions into the journal.

166060 – The SAS migration utility can now be launched manually by navigating to **SAtoSASmigrationUtility .exe**

174141 – It is possible to cancel multiple manual actions through the manual action dynamic view.

175299 - A rare problem that caused corruption of LDAP temporary .bin files and improper LDAP behavior has been fixed

189531 – A single entry now appears when performing a manual unlock or lock on an apC door configured with inbound and outbound readers.

192615 – The **New Personnel** template in the Administration application correctly saves pre-defined values.

197037 – Deleting a stop in a guard tour no longer re-sequences the remaining stops.

199352 – New functionality has been added to the **C•CURE9000License.exe** and the **License Manager** which allows the status of the license to be displayed with greater detail.

199725 – When setting up an Aperio Reader the customer can now assign any name to the reader and save.

202092 – The same schedule can now be assigned to multiple custom clearance items in the Personnel Clearances tab.

202110 – It is now possible to perform a successful license validation with a series D license on a SS2 unit.

203365- It is not possible to select an iSTAR Input group as a controlled input for an intrusion zone. This stops an error occurring when trying to save an iSTAR Intrusion Zone Configuration.

203887 – Naming a server “CCURE9000” does not affect license validation or the re-booting of the system.

205102 – When refreshing or closing the Assa Reader Dynamic View, the battery status and last contact now show correct values.

205772 – The response time for starting the administration application and other functions has been enhanced for larger systems.

205838 – C•CURE GO can now establish a connection with a server through a custom port.

206812 – The Swipe and Show feature screen displays all information on all screen resolution settings.

206846 – The Auto Increment feature when assigning card numbers now works correctly.

206979 – An error (“one or more values is not an object property name in the expression”) no longer occurs when running a Personnel Query for cardholders admitted/rejected at a door during a specified Time/Date range.

207159 – The loading time of Unified maps has been significantly reduced.

207672 - For a particular object; if you select the Maintenance Mode check box in the object editor and then configure the View Preference for an Application Layout to show Maintenance Mode objects only; the Monitoring Station (Activity Viewer) will display all the activities of that particular object that is in Maintenance Mode

207859 – Duplicate visit names can now be created in the Visitor Management application.

208443 – Personnel that have been disabled from the system can no longer access the Visitor Management application.

209647 – It is now possible to disable the basic authentication prompt using the System Variable **Single Sign On**. This system variable can be accessed under the category **System Operations.**

209933 – The **View Preferences** interface correctly acknowledges specified partition fields marked by the user.

210587 – For enterprise systems, Operators who do not have privileges in the MAS default partition are no longer prevented from editing personnel.

210700 - Upgrading from previous versions of C•CURE 9000 no longer causes map errors with operators that have limited privileges.

210731 - The amount of time it takes for the **Event Viewer** to load when there are a large number of active events have been reduced.

210748 – On C•CURE GO the **Door Names** are now listed clearly under the **Door List** on mobile devices.

210838 – When an input trigger is activated, the event is correctly activated and recorded in the **Monitoring Application**.

211357 – When selecting **Clearance** as the type within a new **Query** the correct order of items is now displayed.

212426 – Synchronization of changes to User Defined Fields is more reliable.

213314 - Using the LogBackup.exe no longer creates an error when restoring a journal log volume, during back up of a journal log using Log Volume Management.

213333 – When importing an image into a personnel record, Image Capture Date appears in the Images Dynamic View with the correct date displayed.

285870 – Synchronization of Clearances and their User Defined Fields has been fixed.

289245 – The security issue has been corrected.

290750 – When moving an iSTAR Cluster and Controller to a new Partition in a partitioned standalone or Enterprise system, all configured Elevators and Intrusion Zones in the iSTAR Cluster and Controller are included in the respective iSTAR Cluster and Controller parent folder.

292103 – The C•CURE 9000 Videoedge NVR unit has been enhanced to accept recorders by DNS when adding recorders to C•CURE 9000.

294985 – There is no minimum amount of iSTAR door exceptions that you can add to the Privilege exceptions tab.

294987 – Synchronization conflicts do not occur after adding a personnel type Visitor to a global personnel record in an Enterprise system.

295479 – Assess Application layout has been enhanced to support partition filtering for event assessment.

296847- The system has been optimized to add credentials to Personnel records faster.

298560- Operators with privilege exceptions for specific iSTAR Doors and iSTAR Door Groups are accessible to Operators so that they can view and edit them.

299085 – Manual actions no longer generate journal log error messages.

299087 – The system has been optimized to display images faster in Swipe and Show on remote clients.

299504 – When configuring an event to pulse an **Output**, clicking in the Details field before selecting an output no longer generates an error, and the event can be configured and saved.

300350 – The system has been enhanced so that an administrator can disable the SAS from copying ACVS journal messages to the MAS, so that messages do not overload the ACVSJournalStage database.

300414 – SAS servers and partitions are displayed in alphabetical order when viewing them in the Server dropdown and the **Read Data From** lists in the MAS.

300726 – The new **Assign Predefined Log Message** command from the Event context menu can be used to assign predefined log messages to multiple Events from the Events Dynamic View.

301719 – Enabling the iSTAR Message Encryption system does not affect iSTAR controller configuration download.

302362 – The C•CURE Portal (consisting of the Visitor and Access Management applications) has been configured so that it recognizes trailing spaces as authentic characters in users' passwords.

304943 – Upgrading from v2.30R2 to v2.50 and v2.60 no longer generates a database error.

308570 – The database schema has been enhanced so that the ICU now registers iSTAR run time information.

310605 – Query parameters have been enhanced to include the filter type **In span from now**. Customers can use this filter type to configure a date/time query parameter by entering a custom value in seconds, minutes, hours, or days, and select whether to search this range **in the past** or **in the future**.

311466 – Using a criteria filter for the ODBC Import configuration no longer generates database errors.

314478 – Using the **Galaxy Area** icon to arming and disarming a Galaxy Area no longer generates an error.
315649 – In the event of system latency during an inactivity scanning, the scan time remains unchanged.
318565 – Panel events that require acknowledgement are now in the correct state after Crossfire restart.
318860 – The system has been optimized so that system performance is not affected by successive clicks for the same **Grace Personnel** action.
319114 – The rare case where the CrossFire Server crashes due to problems with the inactivity process has been corrected.
324484 - Firmware download code has been amended so that the iSTAR driver no longer crashes during download.
415952 - No sync conflicts occur if you add an Application Server to a Global Operator on a SAS.

13. Upgrading to Version 2.60

The *C•CURE 9000 Installation and Upgrade Guide* includes step-by-step instructions for upgrading your C•CURE 9000 system. The upgrade chapter explains the steps you need to take prior to upgrading, the database updates that are performed when you upgrade, and the tasks you need to perform after the upgrade is completed. Please refer to this guide for information. You can upgrade to C•CURE 9000 v2.60 directly from the following earlier versions:

Table 7: Software Version Upgrades

SiteServers
2.4x to 2.60
2.5x to 2.60
Standalone
2.4x to 2.60
2.5x to 2.60
Enterprise
2.4x to 2.60
2.5x to 2.60

CAUTION: Before upgrading to C•CURE 9000 v2.60, see **Important Notes** in these Release Notes.
In addition, if you currently have the C•CURE 9000 Language Pack installed, see **Item 5.16**.
Be aware that upgrading **removes** the existing firmware files (<INSTALLDIR>Tyco\CrossFire\ServerComponents\ apC and istar) while adding the new firmware versions. If you need to keep your existing firmware, save the files elsewhere before you upgrade to v2.60. Otherwise, you will have to re-download these files from the Software House web site.

11.1 C•CURE + victor Server Databases May Expand During Upgrade

During an upgrade, the C•CURE + victor Server application databases may grow in size due to index re-creation and upgrade of the database tables. Depending on the size of the databases beforehand, the size may expand by up to 10GB. Thus, you should ensure that ample disk space is available before you begin.

11.2 Upgrade May Freeze with Out-of-Disk Space Error

During an upgrade, a message may inform you that there is **not** enough disk space available.
Workaround: Add more disk space on an existing/new drive and run the upgrade again.

11.3 Post-Upgrade Steps for C•CURE 9000 v2.60 System on Custom (Non-default) Path

If you are upgrading a system in a custom (non-default) location, once the upgrade to v2.60 is completed, you must verify that the System Variable paths for Import, Export, and Database Backup are correct.

11.4 Exported Objects into External XML Documents

If you have exported objects into external XML documents from previous versions of C•CURE 9000, you may not be able to re-import them directly into C•CURE 9000 v2.60. Object definitions in the database can change from version to version, so the import may fail or the imported object may **not** work correctly in C•CURE 9000 v2.60.
Workaround: If you have any valuable XML documents generated by Data Export in a prior version of C•CURE 9000, you should do the following prior to upgrading C•CURE 9000 to v2.60:

1. Re-Import the XML documents.
2. Upgrade to v2.60.
3. Export the Objects again.

11.5 SDK Connected Program Drivers

11.5.1 SDK Connected Program Drivers and C•CURE 9000 Upgrade

BEFORE UPGRADING C•CURE 9000: If you licensed any of the SDK Connected Program drivers with a previous release, check the Software House web site (**Home**>**Support**>**"Software House Connected"**> **Compatibility Matrix** http://www.swhouse.com/support/SWH_Connected_Compatibility_Matrix.aspx) to confirm that your integration is compatible with v2.50 **BEFORE YOU UPGRADE**.
Contact the distributor of the Connected Program driver to get your C•CURE 9000 v2.60 compatible driver.
NOTE: Client Auto-Update does **not** update clients with new versions of a Connected Program Driver product; you must perform Client updates for these products manually at each client.

11.5.2 Uninstalling SDK Connected Program Drivers

If you have a Connected Program Integration from a previous release that you do **not** intend to upgrade and wish to uninstall, you **must uninstall it before** you upgrade your C•CURE 9000 to v2.60. If you upgrade to v2.60 and then try to uninstall, the uninstall may fail.

11.5.3 Error message during C•CURE Client auto upgrade

If you run a C•CURE Client auto upgrade from v2.40 to v2.60 on a machine that does not have .Net 4.6.1 installed, the following error message can be ignored and does not indicate an auto upgrade failure.

Error: Method not found: 'System.String.System.String.Format(System.IFormatProvider, System. String, System.Object)'

14. Installation of Version 2.60

12.1 SQL Privileges for Local System Account in a Workgroup

If you are installing C•CURE 9000 on a Workgroup system that already has SQL Server 2008 R2/2012 Express/Full installed, you must assign the SQL Sysadmin privilege to the Windows account local system. If you do **not** do this, the CrossFire Services do **not** start.

12.2 Server Requirements Failure Message during Installation on Windows Servers

If IIS Extension files are **not** installed on your server system, the Installer reports that IIS is **not** installed. You can safely continue installing and install the IIS Extension Files **after** the C•CURE 9000 install is complete.

12.3 Installation Completes on Longer-than-15-Character Name Computer but Clients Do Not Connect

If you install C•CURE 9000 on a computer with a name longer than 15 characters, the following error message displays: "The NetBIOS name is limited to 15 characters". You can continue the install, but the system name will be truncated. Consequently, Clients will be unable to log in to C•CURE 9000.

Workaround: Change the computer name to match the 15-character truncated version.

12.4 Installation Completes on Windows 7 system without SP 1 Prerequisite Installed

If you are installing C•CURE 9000 on a Windows 7 system without the SP 1 prerequisite installed, the process still continues and completes. However, before you use C•CURE 9000, you should install SP1.

12.6 Services/Server Components Manual Start

After installing C•CURE 9000 v2.60, you must run the Server Configuration Application (**Start**>**All Programs**> **Tyco**>**Server Configuration Application**) one time to start the CrossFire Framework and CrossFire Server Component Framework Services. (You cannot access C•CURE 9000 functions until you start these services.) You also need to enable and start the Extension Service (Hardware Driver) for each type of controller, video, or network component to be used on the server. (The Extension Services [Drivers] are not automatically started by default because enabling drivers for devices that are not used can affect system performance. In addition, starting them automatically would trigger a download for apC and iSTAR controllers.) See the *C•CURE 9000 Installation and Upgrade Guide* on the product DVD for specific instructions. You can view the status of these drivers from Windows Services, but should not configure them to start automatically from there; startup is managed by the CrossFire Server Component Framework Service.

12.7 victor Temporary License Expiration May Cause C•CURE 9000 Licensed Video Drivers to Not Work

If you install a C•CURE 9000 + victor Unified system **but do not** obtain a permanent license for victor, C•CURE 9000 Video drivers may stop working when the victor temporary license expires.

Workaround:

1. Either obtain a permanent victor license or remove the victor temporary license.
2. Edit, disable, and then save each Video Server on the C•CURE 9000 Administration Station.
3. Edit, enable, and save each Video Server to restore the connection with each server.

12.8 Installing C•CURE Go Web Service and C•CURE 9000 Web Client

12.8.1 IP Address Requirements for C•CURE Go Install

You should install the C•CURE Go Web Service application either on a system with a fixed IP address or on a system that cannot switch from one IP address to another by a simple reboot. Since C•CURE Go has no way of knowing that the IP address has changed, it cannot distinguish a server IP address change from the service on the server stopping or the server being shut down.

12.8.2 IIS Version Prerequisite for C•CURE Go Install

If the required IIS version for the C•CURE GO Web Service is **not** installed as a prerequisite, an error message appears when the C•CURE Go Web Service installation actually begins, rather than on the final prerequisite review screen earlier in the process.

12.8.3 Installing Language Pack for C•CURE Go and C•CURE 9000 Web Client

If you install either the C•CURE Go Web Service or the C•CURE 9000 Web Client on a computer that does **not** have the C•CURE 9000 client on it, you will **not** be able to install the language pack. Consequently, you will **not** have a fully translated product.

Workaround:

1. Install the C•CURE 9000 client.
2. Install the language pack on the computer with the C•CURE Go Web Service/ C•CURE 9000 Web Client.

12.8.4 C•CURE Go Web Service Installation Not Supported on MAS

You are **not prevented** from installing the C•CURE Go Web Service on a MAS system that is an IIS server. However, you should be aware that this configuration is **not supported** and the C•CURE 9000 MAS license does **not** allow it.

12.9 Uninstalling C•CURE 9000 Fails on Window Server 2012 with Remote SQL if .NET 3.5 Not Enabled

If you try to uninstall C•CURE 9000 from a Windows Server 2012 system that uses a remote SQL database and does **not** have .NET 3.5 installed locally, the following error message displays: “There is a problem with this Windows installer package. A program did not finish, … etc."

Workaround:

1. Click **OK** to terminate the uninstall process.
2. Enable the .NET 3.5 feature.
3. Re-start the uninstall process.

End of Release Notes

Software House C•CURE 9000 C•CURE Web

Version 2.60 SP3 Release Note
August 2019

This release note provides important information about the release of C•CURE 9000 C•CURE Web for version 2.60 SP3. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Contents

Features

C•CURE Web is an application that runs in a web browser. You can use it to manage your C•CURE 9000 system from multiple devices through any supported web browser.

C•CURE Web contains the following features:

- Dockview management
- Site Explorer for doors, inputs, outputs and controllers.
- Manual actions for access control devices:
  - Door actions – Locking and unlocking
  - Input actions – arming and disarming
- Basic Reporting:
  - Audit Logs
  - Activity Journals

Requirements

C•CURE Web requires the following software:

Client PC

- Supported web browsers:
  - Internet Explorer (v10 and up)
  - Chrome (v35 and up)
  - Firefox (v30 and up)

PDF Reader

- Adobe PDF Reader must be installed on the client PC where the browser will be run. To get Adobe Reader, the URL is https://get.adobe.com/reader/.

Microsoft Application Request Routing (ARR)

- C•CURE Web requires ARR to be installed on any system that is using IIS. To get ARR, the URL is https://www.iis.net/downloads/microsoft/application-request-routing.
- If you are unable to download ARR, you can use an offline ARR installer from the following URL https://www.microsoft.com/en-us/download/details.aspx?id=47332.

Web Server (IIS)

- C•CURE Web runs on node.js server. If C•CURE Web is installed on the web server where IIS is enabled and port 80 or 443 is in use, then Internet Information Services (IIS) Web Server v8 is required.

C•CURE 9000 Server

- C•CURE 9000 Security and Event Management System version 2.60.

victor Web Service API

Installation

For more information about installing C•CURE Web, see the *C•CURE Web Quick Start Guide.*

SPARs Fixed

This Web Client Update includes the SPAR fixes described in Table 2: SPAR Table.

Table 2: SPAR Table

SPAR Number	SPAR Description
456158	A search reset button has been added so you can cancel searches if an error is encountered.
617760	Operator accounts with privilege groups can log in to C•CURE Web as expected.

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Web Client

C•CURE 9000 Version 2.60 Service Pack 2 Web Client Release Notes
August 2018

This Release Note provides important information about the C•CURE 9000 Web Client for C•CURE 9000 v2.60 Service Pack 2. In case of discrepancy, the information in this document supersedes the information in any document referenced herein. Read this file before installing the product.

Contents

1. Features

The C•CURE 9000 Web Client provides a web-based administration client for C•CURE 9000.

The following features are available on the C•CURE 9000 Web Client:

- Personnel viewing and editing
- Dynamic Views of security objects
- Activity Monitoring
- Lock/Unlock Doors
- Activate Events
- Reporting
- Manual Action Challenge
- Auto Logoff
- Web Client Language Pack is supported in this release.

NOTE: You need to refresh your web browser by using the F5 key or refresh button to correctly display translated Web Client Help files.

2. Requirements

The C•CURE 9000 Web Client for v2.60 Service Pack 2 requires the following software:

Client PC

- Windows 7 (32- and 64-bit), Windows Server 2008, Windows Server 2008 R2.
- Silverlight 4.0 and 5.0 (can be downloaded from Microsoft when you start the Web Client).
- Web Browser software:
    - MS Internet Explorer 10 and higher (32- or 64-bit) – under **Tools>Compatibility View Settings**, uncheck **Display intranet sites in Compatibility View**.

- Mozilla Firefox 38.0.5 (32- or 64-bit)

Google Chrome no longer supports NAPI, which is required for use with Silverlight, so Google Chrome no longer supports the CCURE 9000 Web Client. See https://support.google.com/chrome/answer/6213033?hl=en for more information.

- For Internet Explorer, the client PC's system name must be added to the Trusted Sites list in the browser's **Internet Options>Trusted Sites** section as http://<systemname>.

Web Server

- Microsoft Internet Information Services (IIS) Web Server.

C•CURE 9000 Server (this server can be the same server as the IIS Web Server)

- C•CURE 9000 Security and Event Management System version 2.60 Service Pack 2.

3. Contents

You can install the Web Client from the C•CURE 9000 Version 2.60 Service Pack 2 media.
The Web Client installation contains the following files:

- **WebClientLauncher.exe** - C•CURE 9000 Web Client software.
- **7z938.msi** – 7-Zip Installer software.
- **9000-2-60-sp2_webclnt_rn_lt_ev_8200-1367-52a0.pdf** - this release note file.

4. Installation

You must install the Web Client software on your IIS Web Server system.
Perform the following steps to install the C•CURE 9000 Web Client:

1. Navigate to the C•CURE 9000 2.60 Service Pack 2 WebClient folder.
2. Double-click **7z938.msi**.
3. Follow the steps in the 7-Zip Install Wizard to install 7-Zip.
4. Double-click **WebClientLauncher.exe** to install the Web Client. For more details see the C•CURE 9000 Web Client User Guide PDF on the DVD.
5. Upon completion, click Exit.

To access the Web client, open your browser and navigate to http://<machinename>/CCure9000WebClient/WebStar.html. Where <machinename> is the name of your Web server.

5. Limitations

There are no known limitations for this release.

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Version 2.60 SP1 victorWebClient Update (Unified 3.52 SP1 CU01)

C•CURE 9000 Version 2.60 SP1 victorWebClient Update (Unified 3.52 SP1 CU01) Release Note
May 2018

This Release Note provides important information for installing the C•CURE 9000 Version 2.60 Service Pack 1 victorWebClient on C•CURE 9000 Client machines. In case of discrepancy, the information in this document supersedes the information in any document referenced herein.

Please read this release notes before installing the product.

Contents

1. Versions for C•CURE 9000 Software and Service Packs

The Version Matrix table below shows the version numbers for each release of version 2.60 of C•CURE 9000, the version number displayed in **Help> About** for the Administration Client and Monitoring Station Applications, and the way each version number is displayed in **Programs and Features** on the Windows system.

Version Matrix

C•CURE 9000 Version	C•CURE Client Help/About	Programs and Features SP/CU Version
2.60	3.3.1350.0	3.3.1350.0
2.60 SP1	3.3.1350.0	3.3.1350.0

2. Installing the Critical Update

This Critical Update installs victor Web or C•CURE Web to your system.

NOTE: If you have Internet Information Service installed, you must install Application Request Routing. A prompt displays to install if required. You do not have to exit the install process to install it.

Installing on a C•CURE 9000 client:

1. Log out and exit the C•CURE 9000 Administration application on the client machine.
2. Log out and exit the C•CURE 9000 Monitoring Station application on the client machine.
3. Start the C•CURE 9000 victor Web / C•CURE Web install by double clicking on **Setup.exe**.
4. Select either **victor Web** or **C•CURE Web.**
5. Review your selection in the next window, click **Next.**
6. Agree to the EULA and installation begins.

3. Uninstalling the Critical Update

NOTE: This uninstall will completely remove C•CURE Web or Victor Web from your system, depending on which you had installed.

Uninstalling on a C•CURE 9000 client:

1. Navigate to **Control Panel > Programs and Features.**
2. Select **C•CURE 9000 2.60 Client SP1 victorWebClient** and click **Uninstall.**

4. SPARs Fixed and Enhancements

This critical update includes the following SPAR fixes and enhancements:

SPAR Number	SPAR Description
453349	Door activity shown in the Journal is accurately reflected within the Previous Doors tab of the Personnel Record.
456148	C•CURE Web: A search reset button has been added to allow a search to be cancelled if an error is encountered.
456162	C•CURE Web: Journal Search can match text-string as entered in an Exact Match or Like Comparison search.
456163 / 456170	C•CURE Web: A checkbox has been added to select Exact Match or Like Comparison searches within Journal Search.
456173	C•CURE Web: Unwanted portrait images can be deleted.

End of Release Notes

SOFTWARE HOUSE
From Tyco Security Products

C•CURE 9000 Web Client

C•CURE 9000 Version 2.60 Service Pack 1 Release Notes
August 2017

This Release Note file provides important information about the release of the C•CURE 9000 Web Client for C•CURE 9000 Version 2.60 Service Pack 1. (In case of discrepancy, the information in this document supersedes the information in any document referenced herein.)

Please read this file before installing the product.

Contents

1. Features

The C•CURE 9000 Web Client provides a web-based administration client for C•CURE 9000.

The following features are available on the C•CURE 9000 Web Client:

- Personnel viewing and editing
- Dynamic Views of security objects
- Activity Monitoring
- Lock/Unlock Doors
- Activate Events
- Reporting
- Manual Action Challenge
- Auto Logoff
- Web Client Language Pack is supported in this release.

NOTE: Users must refresh their web browser (using the F5 key or refresh button) to correctly display translated Web Client Help files.

2. Requirements

The C•CURE 9000 Web Client for version 2.60 Service Pack 1 requires the following software:

Client PC

- Windows 7 (32- and 64-bit), Windows Server 2008, Windows Server 2008 R2
- Silverlight v4.0 and 5.0 (can be downloaded from Microsoft when you start the Web Client).

- Web Browser software:
    - MS Internet Explorer 10 and higher (32- or 64-bit) – under **Tools>Compatibility View Settings**, uncheck **Display intranet sites in Compatibility View**.
    - Mozilla Firefox 38.0.5 (32- or 64-bit)

  Google Chrome no longer supports NAPI, which is required for use with Silverlight, so Google Chrome no longer supports the CCURE 9000 Web Client. See https://support.google.com/chrome/answer/6213033?hl=en for more information.
- For Internet Explorer, the client PC's system name must be added to the Trusted Sites list in the browser's **Internet Options>Trusted Sites** section as http://<systemname>.

Web Server

- Microsoft Internet Information Services (IIS) Web Server

C•CURE 9000 Server (can be the same server as the IIS Web Server)

- C•CURE 9000 Security and Event Management System version 2.60, Service Pack 1.

3. Contents of the DVD

The Web Client is installable from the C•CURE 9000 Version 2.60 Service Pack 1 media.
The Web Client Install contains the following files:

- **WebClientLauncher.exe** - C•CURE 9000 Web Client software
- **7z938.msi** – 7Zip Installer software
- 9000_WebClient_Gd_UM227_rev0.pdf - User Guide for the Web Client software
- 9000_2_60_SP1_WEBCLNT_RN_8200-1367-47_A0.pdf - this release note file

4. Installation

You must install the Web Client software on your IIS Web Server system.
Perform the following steps to install the C•CURE 9000 Web Client:

1. Navigate to the C•CURE 9000 2.60 Service Pack 1 WebClient folder.
2. Double-click **7z938.msi**.
3. Follow the steps in the 7Zip Install Wizard to install 7Zip.
4. Double-click **WebClientLauncher.exe** to install the Web Client. For more details see the C•CURE 9000 Web Client User Guide PDF on the DVD.
5. Upon completion, click Exit.

To access the Web client, open your browser and navigate to
http://<machinename>/CCure9000WebClient/WebStar.html
Where <machinename> is the name of your Web server.

5. SPARs Fixed

CCURE Web Client now displays the leading 0s of a PIN number in the Personnel Record to accurately reflect the display of PIN numbers in CCURE Administration. (367664)

The Web Client now allows the Operator to properly access personnel records. (415456)

An issue which prevented CCURE Web from displaying all personnel records in a partition other than the default partition has been resolved. (418114)

The Web Client platform has been enhanced to allow greater amounts of data. For example, a dynamic view of available doors. New buttons allow the user to scroll through and view a larger record set than had been possible previously. (425793)

6. Limitations

1. If you configure 22 or more Dynamic Views on the CCURE 9000 Server, the Web Client Dynamic View toolbar cannot scroll horizontally to display all available Views.
2. Timeout and unhandled exception are encountered when running Journal query in a dynamic view. This is due to the query taking too long to execute within the HTTP Web request parameters. You must modify the query associated with the dynamic view to return smaller set of records.
3. The Web Client loses communication with the C•CURE 9000 server due to the C•CURE 9000 server stopping (for various reasons). The Web Client does not automatically re-establish a connection with the C•CURE 9000 server; you must manually re-establish the connection.
4. Because the Web Client treats the entire Personnel record (including Credentials, Clearances, Customer fields, Images, etc.) as a unit when editing, if an Operator with limited Privileges tries to save a Personnel record from the Web Client, the save is rejected if the Operator does not have correct permissions to modify any one of the objects in the Personnel record. The workaround is to ensure that the Operator has the correct Privileges to all Personnel-related objects.

End of Release Notes