TycoAI suite Hardening guide

GPS0010-CE-20200805-EN
Rev B

Introduction

Our solution provides peace of mind to our customers with a holistic cyber mind set beginning at initial design concept, continuing through product development, and supported through deployment, including a rapid incident response to meet comprehensive and evolving cybersecurity environments.

The Hardening Guide intends to provide cybersecurity guidance used in planning, deployment and maintenance periods.

As cybersecurity threats affect all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution’s functional operation.

This guide provides hardening guidance for configuration and maintenance, including the operating system, user accounts, permissions and roles, backup and restore, redundancy, and patch management.

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Tyco cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Tyco makes no representation or warranty, express or implied, as to the efficacy of the cybersecurity practices or recommendations described in this guide. Tyco disclaims all liability for any damages that may occur as a result of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Table of Contents

1 Planning

Use this section to plan the TycoAI suite deployment. The contents within this section are useful in several planning stage functions:

- Assuring compliance with the cybersecurity criteria that govern the target environment.
- Designing the deployment architecture.
- Providing a reference for settings made during deployment.

1.1.0 Security feature set

This section describes TycoAI's many security features and how to configure them.

1.1.1 Human user account safeguards

No backdoor passwords.

User account password policy – TycoAI suite contains rules which govern password formation - restrictions including password length and complexity.

1.1.2 User authentication safeguards

Hidden password entry - password entries are hidden from view as the user enters them.

1.1.3 Camera authentication

As supported by camera – TycoAI suite authenticates with a connected camera using a username and password stored in the camera.

1.1.4 Secure communications

Remote login via secure shell (SSH) and remote desktop are disabled by default.

TycoAI suite uses Transport Layer Security (TLS) for encrypted communication including web-based HTTPS communications. Only TLS v1.2 is supported.

1.1.5 Audit logs

Audit logs - Activity and events from TycoAI suite are stored in audit log records that administrators can access to view evidence of the activities that have affected the system and indicate the timestamped operation, procedure or event. System, boot logs are recorded along with the logs from the tycoAI suite application.

- Enabled by default – TycoAI suite is preconfigured to record activity and events in an audit log.
- Time synchronized – TycoAI suite audit log timestamps can be synchronized to a common reference clock for the system, using NTP.
- Delete protected – TycoAI suite audit logs are protected from deletion.

1.1.6 Availability assurance

Backup and Restore – A backup copy of the TycoAI configuration and run-time data that can restore a TycoAI server.

1.1.7 Software updates

TycoAI suite software can be updated via the TycoAI Administrator web UI.

1.2.0 Intended environment

The TycoAI suite should be installed on premise within a data center equipment rack with restricted access.

Internet connectivity

This product does not require Internet access. It is recommended that TycoAI suite not be connected to the internet.

1.3.0 Hardening methodology

While TycoAI suite provides onboard security safeguards, including many secure-by-default settings, we recommend that the system is hardened according to the guidance outlined in section 2, deployment.

Generally a defense-in-depth strategy employing standard IT hardening methods and compensating controls as needed to compliment the base security features of each component.

1.1.8 User management best practices

Following best practices for managing user accounts, their credentials and authorizations (permissions) can greatly improve the security for the system. Some guidance is presented in this section. For additional guidance NIST standards such as SP 800-63 Digital Identity Guidelines may be consulted.

You should create unique user accounts for each administrator of TycoAI suite.

The proper configuration of individual user accounts assures that security best practices are followed and that all user actions cannot be repudiated. Best practices for account management include:

1.3.1.1 No shared accounts

Unique accounts should be used during all phases of operation for TycoAI suite. Installers, technicians, auditors and other deployment phase users should never share common user accounts.

1.3.1.2 Remove or rename default user accounts (as permitted)

By removing or renaming default user accounts, the ability to gain unauthorized access to the system will be reduced as those attempting to do so will need to enter an unpublished username which is much harder to gain knowledge of. During installation, the TycoAI suite mandates that most default user accounts are replaced.

1.3.1.3 Change default passwords

During installation, the TycoAI suite mandates that all default user accounts that have not been replaced must have their password changed.

1.3.1.4 Strong passwords

Strong passwords should be used to minimize the risk of password guessing. Automated forms of password guessing such as "dictionary attacks" and "rainbow tables" can run through commonly used passwords and can be successful if strong passwords are not used. You can strengthen a password with length and complexity. The length of a password has the biggest impact on making password guessing difficult.

1.3.1.5 Password policy

It is important to have a password policy. Customers often have password policies that all systems must support.

1.4.0 Communication ports table

Table 1: Communications ports table

Port	Transport	Protocol	Service
22	TCP	SSH	SSH
68	UDP	DHCP	wicked-dhcp4

80	TCP	HTTP	Apache
123	UDP	NTP	ntpd
554	TCP	RTP	TycoAI_api
8001	TCP	HTTPS	UI
4001	TCP	WSS	Event feed
8080	TCP	HTTPS	API
Port	Transport	Protocol	Service
22	TCP	SSH	SSH
68	UDP	DHCP	wicked-dhcp4
80	TCP	HTTP	Apache
123	UDP	NTP	ntpd
554	TCP	RTP	TycoAI_api
8001	TCP	HTTPS	UI
4001	TCP	WSS	Event feed
8080	TCP	HTTPS	API
Port	Transport	Protocol	Service
22	TCP	SSH	SSH
68	UDP	DHCP	wicked-dhcp4
80	TCP	HTTP	Apache
123	UDP	NTP	ntpd

1.5.0 Network planning

Video surveillance systems transmit, collect, process and, store sensitive data that will disclose sensitive information if accessed by unauthorized users. While several security controls are inherent to the TycoAI suite to limit access to authorized users, it is best practices for the network design to provide additional layers of defense.

With the full scope of components and functions in mind you can build the appropriate level of protection into the network design to protect both the network and end-points. Keep in mind that some of the system components, while compatible with TycoAI suite, may not support the same level of protection as TycoAI suite. In those cases, compensating controls may be utilized within the network design to reduce risk.

1.5.1 Trust boundaries overview

A trust boundary within a system is the boundary in which data is passed between components that do not share an equal level of trust. Products that are not part of the TycoAI suite or do not provide methods to sufficiently authenticate a component or user may be regarded as having a lower of level of trust. Networks may also have different levels of trust. For example, an isolated network with only video cameras, TycoAI Servers, and access control systems is usually trusted more than a shared use network such as the corporate IT network or a remote network.

When the trust deviation is beyond the risk tolerance, it is best to control the flow of data between trusted and untested network using a switch or router with data flow control capabilities, such as a firewall.

1.5.2 Network protection

Isolating TycoAI suite from networks of lower trust is recommended.

1.5.2.1 Demilitarized Zone (DMZ)

When communications to or from the TycoAI server is required from an untrusted network (from the perspective of TycoAI server), such as a corporate LAN, a demilitarized zone (DMZ) may be established to provide a high degree of data flow control and prevent direct access to resources on the TycoAI server network.

Use of a DMZ is strongly recommended with providing remote connectivity in conjunction with other safeguards such as a VPN and multi-factor authentication.

1.5.2.2 VLANs

A Virtual Local Area Network (VLAN) provides the ability to share the networking infrastructure while maintaining separation between trusted and untrusted networks. The use of VLANs reduce deployment costs by removing the need to run dedicated cabling and networking equipment for the TycoAI server.

If physical access to the cabling used for the VLAN is possible by authorized users, it is recommended that the VLAN switches are configured for to protect eavesdropping by employing encryption technology.

1.5.2.3 Firewalls

Routers and switches which are used to bridge trust boundaries should employ firewalls.

1.5.2.4 Remote access

Remote access points should be protected and always treated as access from an untrusted network.

1.5.2.5 VPN

A Virtual Private Network (VPN), should always be used to provide encrypted and authenticated communication for remote access connections. VPN technologies the enabled for multi-factor authentication are recommended.

1.6.0 Anti-virus

The TycoAI suite does not include pre-installed Anti-virus software. As specific Linux compatible anti-virus software is not pre-qualified for use with the TycoAI suite, it is recommended that the anti-virus software compatibility is tested in a controlled, non-production environment.

1.7.0 Hardware and software requirements

See the TycoAI suite installation guide.

1.7.1 Required services

Required services for TycoAI suite operations are set up by default with the correct settings. These services must stay enabled for continuous operations.

2 Deployment

This section is designed to help execute the deployment of TycoAI suite. The contents within this section address how to initiate secure deployment for new installations, how to harden TycoAI server and additional steps after commissioning required before the TycoAI suite is turned over to runtime operations.

2.1.0 Deployment overview

Security hardening of TycoAI suite begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review this section prior to deployment to fully understand the security feature set of TycoAI suite, its architecture, data flow and requirements before physically installing and making application specific configuration changes.

In this section more details are provided to help the installer prepare for deployment:

- Physical installation considerations
- Default security behavior
- Considerations for commissioning
- Recommended knowledge level

2.1.1 Physical installation considerations

Install the TycoAI suite hardware using the instructions provided in the user guide. Keep in mind that the physical access to the device and physical installation of the device can impact the cybersecurity.

Physical access to this device enables actions that cannot be authenticated and logged electronically through the capabilities of this product. To prevent unauthorized access, be sure to place the device in a room, cabinet or enclosure that can restrict access (for example, mechanical lock or physical access control). Consider using protective electric wire conduits when communication wires with paths through areas of lower trust.

2.1.2 Default security behavior

The TycoAI suite installation wizard will enforce replacement or password change for all default user accounts, as described in the user guide.

2.2.0 Hardening

While TycoAI suite has several secure-by-default safeguards, TycoAI server should be hardened to meet the security requirements of the target environment.

In this section configuration settings labelled as “minimum baseline protection” is provided as general guidance and may not be sufficient for the target application. It is important to apply to the correct level of protection as warranted by policies and regulations that may govern the application security settings for a deployment instance of TycoAI suite.

2.2.1 Hardening checklist

2.2.2 Administration

As TycoAI suite has been designed as an appliance, users do not need to log on to tyco operating system directly for most operations. You can conduct software access to TycoAI suite from a remote application or webpage. Some administrators may choose to log on to the operating system directly to deploy operating system level updates. In such cases, unique operating system level accounts are recommended.

2.2.2.1 BIOS administration

BIOS administrator requires direct access to the TycoAI server.

To enter the BIOS configuration complete the following steps:

1. Turn on the computer.
2. Within 10 seconds of startup press the F2 button on the keyboard.
3. Enter into **Advanced mode**.

Note: each hardware platform may have a slight deviation.

2.2.2.2 Operating System administration

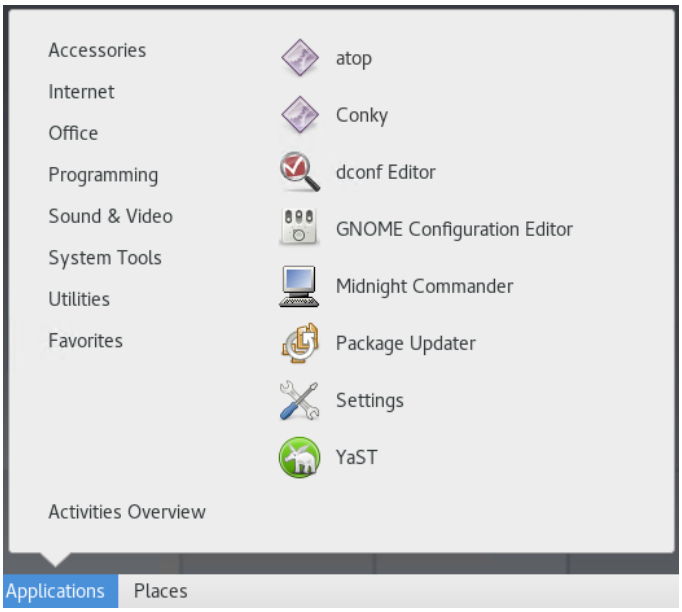
You can access Operating System administration locally.

2.2.2.2.1 YaST Graphical User Interface

The tyco operating system comes with the Yet another Setup Tool (YaST) to aid with configuration.

You can find YaST from the operating system level under applications, system tools:

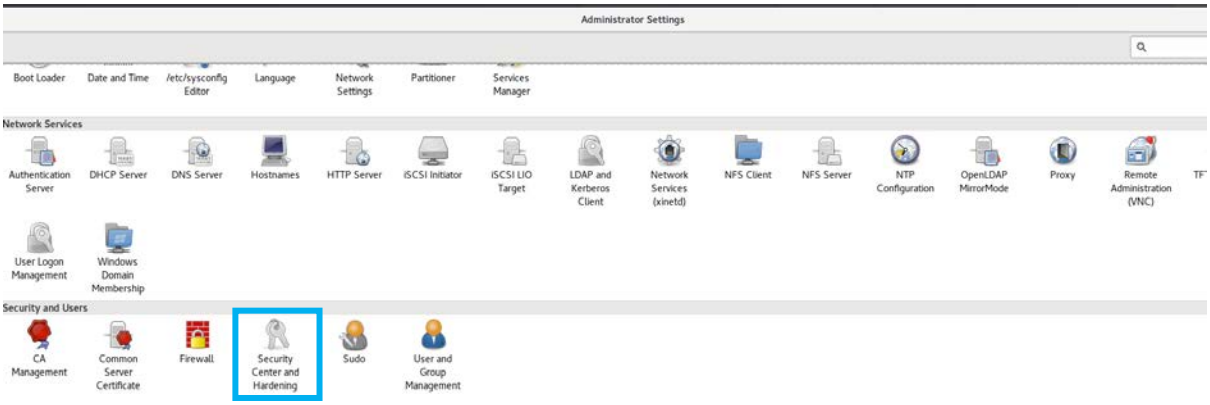
Figure 1



Once opened, YaST provides access to the operating system configuration settings. The Security Center and Hardening tool within YaST provides administrative functions to configure predefined security configurations, password settings, boot settings, and log on settings among other settings.

You can access the Security Center and Hardening tool from the YaST administrator settings, Security User section:

Figure 2



2.2.2.2.2 Command Line User Interface

Some administrators prefer to a command line user interface for configuring the operating system security settings.

To use the command line remotely, SSH must be enabled. (See 2.5 Communication hardening)

Locally the command line may be accessed as follows:

1. To open a terminal, click Application > Utilities.
2. In the terminal window type su – enter root password.

2.2.2.3 TycoAI suite administration

The following administration tools are available for the TycoAI suite application:

2.2.2.3.1 TycoAI Administrator

You can complete administration for TycoAI suite through the TycoAI administrator, a web-based application accessible on the TycoAI server desktop or by simply entering the IP address of the TycoAI server into any browser.

Local access - Locally launch the TycoAI Administrator by selecting the TycoAI Administrator desktop icon. This will launch Mozilla Firefox ESR with the TycoAI Administration Interface log on page loaded.

Remote access - From the web browser of a Windows PC with network connectivity to the TycoAI server, enter the IP address of the TycoAI server in the address bar of your web browser. Supported browsers are Microsoft Edge, Google Chrome, and Mozilla Firefox (latest version in all cases).

First-time access - TycoAI suite setup wizard - The first time accessing the Administration Interface after installation you will be automatically be directed to the Setup Wizard. This will guide you through the process of replacing or changing the password of all default user accounts, creating an API account, and creating a security certificate.

TycoAI Administrator - Users menu – Use the Users menu to administer TycoAI administrator user accounts. You can add and remove accounts and change passwords.

TycoAI Administrator - System menu – Use the System menu to backup and restore system settings and upgrade the TycoAI suite software.

2.2.3 BIOS configuration

Hardening step 1: Configure BIOS

It is important to protect the BIOS configuration from being modified by unauthorized users.

Note: BIOS menus can vary between servers used to host TycoAI suite. The following steps are based on the BIOS menus available when this guide was created.

Hardening step 1.1: Enable BIOS password

Enable password protection of the TycoAI suite BIOS and set the password. This password should only be known to administrators that have been authorized.

How to set a BIOS password:

1. Turn on the computer.
2. Within 10 seconds of startup press the F2 button on the keyboard.
3. Enter into **Advanced mode**.
4. Click the **Security** tab.
5. Set a new Administrator password and a user password. The password should be stored securely as there is no recovery mechanism

Note: You need the user password on start up. You need the administrator password when any BIOS changes are made

2.2.4 Set boot sequence

The boot sequence should prevent boot up by USB devices as it is a possible for USB devices to inject malicious code without warning.

Hardening step 1.2: Prevent USB boot

How to disable USB ports:

1. Turn on the computer.
2. Within 10 seconds of startup press the F2 button on the keyboard.
3. Enter into **Advanced mode**.
4. In the **Advanced** tab click **USB Configuration.**
5. Click on **USB Single Port Control.**
6. Notice all the USB ports are listed as “Enabled”.
7. Change all the ports that are not required to “Disabled”.
8. Save and restart the machine.

Note: Take note to know which ports are being used prior to disabling. This would be done by using the `lsusb -v` command in a terminal.

An end user should have the ability to restrict ability to interact with physical interfaces. The USB port is an important technical interface that would allow for a malicious user to upload corrupted files or download information.

2.2.5 User management

In this section you can find information on user management.

2.2.5.1 Operating system level user accounts (interactive)

You can access TycoAI operating system using the following account:

Table 2

<username>	The standard linux user that was created in the install wizard.

Hardening step 2: Configure operating system user accounts

Changing default system root and standard user account passwords and making them unique enhances the security of the product.

Hardening step 2.1: Change System user account passwords

Change user account passwords using the TycoAI Setup Wizard

The TycoAI Setup Wizard includes the ability to change the system standard user and system root passwords. These passwords must conform to the active password policy of the operating system. The User Accounts page will display within the Setup Wizard. Use this page to replace the WebUI administrator account and Linux admin account, create a new REST API user account, and change the password of the root system account.

Note: It is critical that the new passwords be recorded and kept secure as they cannot be recovered.

Hardening step 2.2: Set invalid attempt user lockout policy

Configure invalid attempt lockout policy to prevent the use of a user account when the lockout is engaged to protect against brute force attacks. The operating system supports invalid attempt lockout. When the invalid attempt lockout is engaged when a configurable number of invalid operating system log on attempts are attempted. This rule may be configured as a temporary lockout (automatically reset after a configurable time period).

Set invalid attempt user lockout policy using the YaST Graphical User Interface

In **Login settings** there is the capability to set the delay after incorrect log on attempts.

Figure 3

Set invalid attempt user lockout policy using the command Line User Interface

- Modify the /etc/pam.d/login file to the following:

```
auth required pam_tally2.so onerr=fail no_magic_root
account required pam_tally2.so per_user deny=5 no_magic_root reset
```

- The first line counts failed log on and failed su attempts for each user. The default location for attempted accesses is recorded in/var/log/faillog.
- The second line specifies to lock accounts automatically after 5 failed log on or su attempts (deny=5). The counter will be reset to 0 (reset) on successful entry if deny=*n* was not exceeded. But you don't want system or shared accounts to be locked after too many log on failures (denial of service attack).
- It is also possible to add the lock_time=*n* parameter, and then optionally the unlock_time=*n* parameter. For example, setting the lock_time=60 would deny access for 60 seconds after a failed attempt.

The unlock_time=*n* option would then allow access after n seconds after an account has been locked. If this option is used the user will be locked out for the specified amount of time after he exceeded his maximum allowed attempts. Otherwise the account is locked until the system administrator removes the lock manually. Refer to the pam_tally man page for more information.

- To exempt system and shared accounts from the deny=*n* parameter, the per_user parameter was added to the module. The per_user parameter instructs the module *not* to use the deny=*n* limit for accounts where the maximum number of log on failures is set explicitly. For example:

```
jupiter:~ # faillog -u oracle -m -1
Username   Failures  Maximum  Latest
oracle     0         -1       Fri Dec 10 23:57:55 -0600 2005 on unknown
```

- By default, the maximum number of log on failures for each account is set to zero (0) which instructs pam_tally to leverage the deny=*n*parameter. To see failed log on attempts, run:

```
faillog
```

- To unlock a locked account (after too many log on failures), use the -r option:

```
faillog -u user -r
```

- Make sure to test these changes (and *any* changes – for that matter) thoroughly on your system using ssh and su, and make sure the root id does not get locked! To lock/unlock accounts manually, you can run one of the following commands:

Locking

```
passwd -l user
         usermod -L user
```

Unlocking

```
passwd -u user
usermod -U user
```

Hardening Step 2.3: Set the password complexity policy

Configure the Operating Systems password length, number of passwords to remember, password encryption method, minimum and maximum password age, and number of days before to give a warning for when a password is about to expire.

Set the password complexity policy using the YaST Graphical User Interface

From Security Center and Hardening tool, select “Password Settings”:

Figure 4

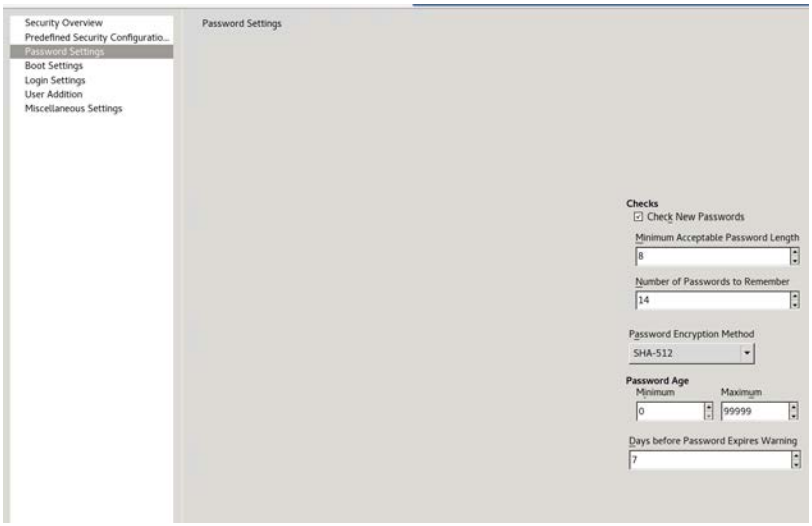


Table 3

	Minimum baseline protection	To strengthen protection
Check New Passwords	☑ (checked)	☑ (checked) is the strongest setting
Minimum Acceptable Password Length	14	increase length
Password Encryption Method	SHA-512	SHA-512 is the strongest setting
Password age minimum	no guidance - consult with local policy / preference	
Password age maximum	90	shorten length

2.2.5.1.1.1.1.1 Set the password complexity using the Command Line User Interface

Input the following commands into the command line interface:

```
pam-config -a --cracklib --cracklib-minlen=8 --cracklib-lcredit=-1 --cracklib-ucredit=-1
--cracklib-dcredit=-1 --cracklib-ocredit=-1
```

Once set using either method, the use of simple passwords will not be allowed. The system will only accept passwords which satisfy these parameters.

2.2.5.2 User management overview

As TycoAI suite has been designed as an appliance, users do not need to log on to Tyco operating system directly. Software access to TycoAI suite is conducted from a remote application or webpage. Some administrators may choose to log on to the Operating system directly to deploy operating system level updates. In such cases, unique operating system level accounts are recommended.

You can create unique user accounts for each administrator of the TycoAI suite application.

2.3.0 Additional operating system hardening

You can perform additional operating system hardening using YaST.

When the Security Center and Hardening tool is opened, it displays a security overview by default showing the status of the security features as either enabled or disabled:

Figure 5

To refresh the status, the security center and hardening tool will need to be closed and re-launched.

Hardening step 3: Security center and hardening configuration

In this section you can find information on the security center and hardening configuration

Hardening step 3.1: Select a predefined or custom security configuration

There are four predefined security configurations to choose from: **Workstation, Roaming Device, Network Server** or **Custom Settings**.

1. From Security Center and Hardening tool, select **Predefined Security Configuration**.

Figure 6

2. Configure your workstation and network to the following settings:

Figure 7

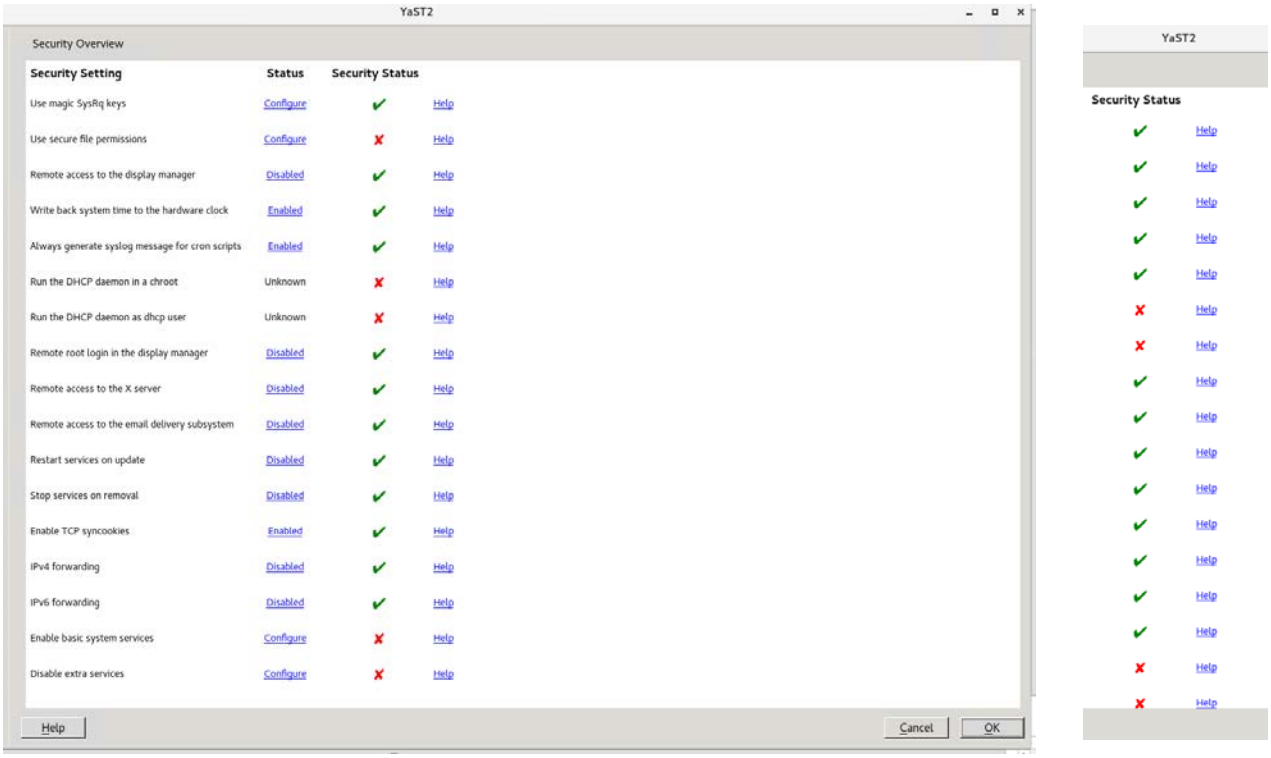


Table 4

	Minimum baseline protection	To strengthen protection	
Check New Passwords	☑ Network Server	☑ Custom Settings Select Network Server + additional protection	Check New Passwords

The network configuration adds in use of secure file permissions of the workstation profile. A custom profile provides the flexibility to configure specific settings tailored for the target environment. The **Roaming Device** profile is not suitable because the TycoAI suite hardware is stationary.

Hardening step 3.2: Set boot permissions

In the security center and hardening you can set boot permissions. The administrator is able to set what the system will do when a user executes Ctrl+Alt+Delete. You can restrict shutdown to root only and set the system to require authentication in order to hibernate the TycoAI Server.

Figure 8

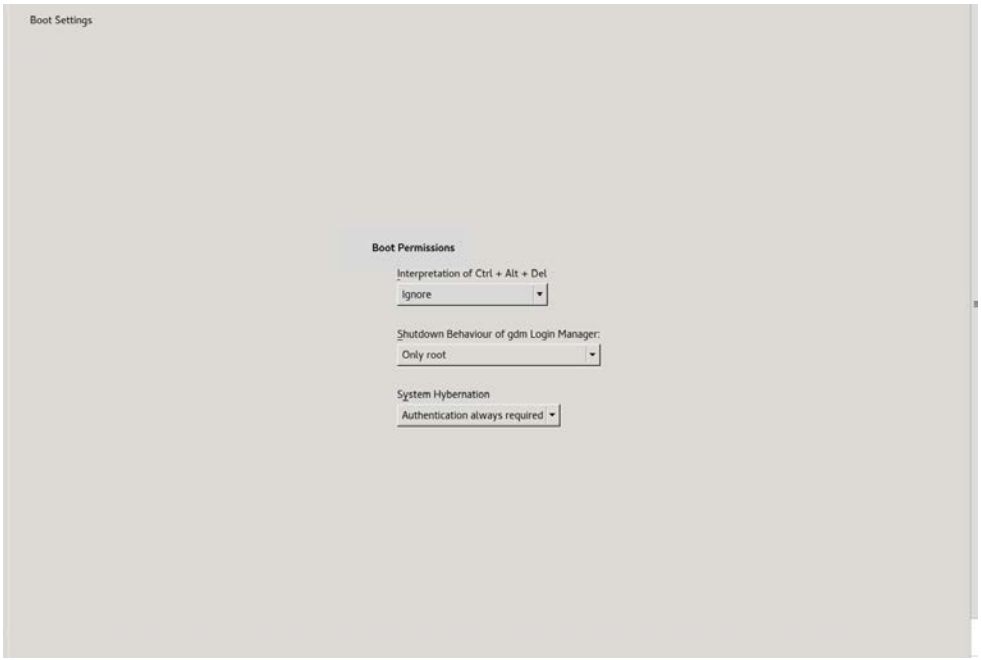


Table 5

	Minimum baseline protection	To strengthen protection
Interpretation of CTRL + ALT + DEL	REBOOT	IGNORE
Shutdown behavior of GDM	Only root	Only root is the strongest setting
System hibernation	User on console	Authentication always required
Interpretation of CTRL + ALT + DEL	REBOOT	IGNORE
Shutdown behavior of GDM	Only root	Only root is the strongest setting

2.4.0 Software updates

Here you can find information on software updates including operating system updates and TycoAI suite application updates.

2.4.1 TycoAI suite and Operating System updates

Hardening step 4: Update software

TycoAI suite should be updated to the current released version with all applicable patches applied during and after the commissioning process. Applying security patches assists in mitigating known vulnerabilities. It is important that any known issue is addressed, even during the commissioning process.

Hardening step 4.1: Update operating system software

Operating system updates are distributed with each release of TycoAI suite. To update the operating system, run the most current update of TycoAI suite.Refer to the TycoAI suite user guide for instructions for updating the TycoAI suite and operating system to the latest supported version.

2.5.0 Communication hardening

Communication hardening limits an attacker's ability to gain access to TycoAI suite. Attackers look for weakness in communication protocols, and communications that is left on encrypted and unauthenticated include the risk that the attacker will be successful in their efforts. Employ techniques to harden the communication interfaces and the transmission of data within this section.

2.5.1 Communication management best practices

Communication to and from the TycoAI server should be configured according to the principle of least functionality.

Least functionality is a security measure designed to limit functions only to those required for the target application and communication sessions used at a given time. In configuring components in this manner, the attack surface is reduced and with it the risk of a cybersecurity breach is minimized.

NTP – Is used to synchronize time throughout the network to an external NTP server. Its use is encouraged for system hardening because it assures that all logs are referencing the same time. When enabled NTP will use port 123.

Table 6

	Minimum baseline protection	To strengthen protection
NTP STATUS	⦿ (Enabled)	□⦿ (Enabled) is the strongest setting (ENABLED) IS THE STRONGEST SETTING

2.6.0 Configuring security monitoring features

In this section you can find information on configuring security monitoring features.

2.6.1 Audit logs

The TycoAI suite tracks important types of system events and system operation and stores the data in logs which are useful for troubleshooting and incident investigation. You can view logs data containing administrative changes, and system events.

The Linux operating system of the TycoAI Server generates a number of different log files specific to each function such as general system operation, web server operation, web server errors, and Network time Protocol (NTP) operation.

The TycoAI suite also generates a number of application-specific log files to aid in diagnosing areas such as camera communication and video playback events.

These audit trails keep track of system configuration operations including the configuration of information security controls. An audit log interrogation tool is provided as part of the TycoAI Administrator Interface. Using the audit log interrogation tool, you can view the system log files.

2.6.2 Backup/Restore

Making frequent backups of the TycoAI suite configuration during and after the commissioning phase can be beneficial if an error is made or settings are lost due to a hardware failure. Once the system is made operational, being able to restore from a good backup minimizes the downtime of the system.

2.6.2.1 TycoAI suite configuration

TycoAI suite has a built-in utility to backup and restore the TycoAI suite server configuration data. In the event of a system failure, the TycoAI suite may be restored to the saved configuration.

2.6.2.2 Operating system configuration

TycoAI suite backups contain

- Configured video inputs
- Face enrollment data
- System settings
- Users

2.6.2.3 Best practices for backup storage

Copies for the backup files should be stored externally from the server and ideally in a remote location to assure all the necessary backup files will still be available if there is a hardware failure or disaster at the site. Backup is protected from unauthorized access using encryption.

Note: Consult the TycoAI user guide for details of how to backup and restore the TycoAI configuration.

2.7.0 Security audits and documentation

A well-documented deployment of TycoAI suite will be useful in security audits, and a security audit can expose errors in the system documentation and identifying gaps in protection. Each task feeds the other and it may be necessary to repeat hardening step 5, after an audit is complete and the gaps are addressed.

2.7.1 Security documentation

Document deployment once hardening is sufficient for run-time operations. When updates are released or security advisories are published this documentation will be useful. The documentation will allow for quick assessment to determine if the deployment is impacted by the issues described in a security advisory and requires a configuration change, software update or patch.

Hardening step 7: Security documentation

Include the following details in creating as-built security documentation:

- As-built architecture drawing of system
- For all system components (TycoAI servers, clients, and cameras) record:
    - Component identification
        - Name
        - Description
        - Device Type
        - Location

    - Vendor
    - Model
    - IP address
    - MAC address
- Support details
    - Software version
    - Hardware version
    - Licenses
    - Installation date
- Communication configuration details
    - Enabled Ports and protocols
    - Encryption settings

2.7.2 Security audit checklist

An audit of the security configuration will help reveal any missed steps and will allow for further hardening of the system. This will be particularly important if a less secure configuration was utilized to facilitate efficient deployment before the full infrastructure was available. Use the security gaps identified with the audit to tighten security to the appropriate levels of protection for the target environment before turning over the system to run-time operations.

Hardening step 8: Perform a security configuration audit

The security audit must be conducted by someone who was not involved with the initial hardening of the system. An independent reviewer is more likely to find the security gaps the audit is intended to reveal.

The Hardening checklist outlined in this section must be used as the basis for the security audit checklist. (Section 2.2.1 Hardening checklist).

3 Maintain

The contents within this section address how to monitor for potential cybersecurity issues and maintain protection levels because conditions change.

An audit that produces a report indicating low cybersecurity risk is a very positive result and suggests that the deployment was conducted with a high degree of care and consideration. However, new attack vectors combined with enhanced hacking tools and more advanced testing techniques may, in the future, disclose vulnerabilities with the technologies used.

The impacted technologies and their implementation may have been previously well regarded by cybersecurity experts. The discovery of vulnerabilities post the final deployment audit may not reflect the quality of that audit.

You may require a higher degree of protection for the environment that TycoAI suite is serving because policies, regulations and guidance may change over time.

3.1.0 Cybersecurity maintenance checklist

Continuously or periodically practice the following cybersecurity maintenance items. The frequency of their execution will depend on the policies and regulations which govern the site. The typical maintenance periods provided are a starting point and adjusted to best suit the target conditions of the deployed environment:

1	*Backup configuration data*	*Weekly*
2	*Test backup data*	*Quarterly*
3	*Lock user accounts of terminated employees*	*Immediately*
4	*Remove inactive user accounts*	*Monthly*
5	*Update user account roles*	*Quarterly*
6	*Disable unused features, ports and services*	*Quarterly*
7	*Check for and prioritize advisories*	*Weekly*
8	*Plan and execute advisory recommendations*	*Based on priority*
9	*Check and prioritize software patches and updates*	*Weekly*
10	*Plan and execute software patches and updates*	*Based on priority*
11	*Review updates to organizational policies*	*Annually*
12	*Review updates to regulations*	*Annually*
13	*Update as build documentation*	*As changes are made or annually*
14	*Conduct security audits*	*Annually*

15	*Update password policies*	*Annually*
16	*Update standard operating procedures*	*Annually*
17	*Renew licensing agreements*	*Annually (or as required)*
18	*Renew support contracts*	*Annually*
19	*Check for end-of-life announcements and plan for replacements*	*quarterly*
20	*Periodically delete sensitive data in accordance to policies or regulations*	*As required*
21	*Monitor for cyber attacks*	*Continuously*

3.1.1 Backup configuration data

If you need to restore or replace a component it is important to have a backup of its configuration data to minimize the time required to restore its functions. If you need to restore or replace a component it is important to have a backup of its configuration data to minimize the time required to restore its functions. Please not that a manual record of the encryption configuration will help assure that the system can be reconstituted should a self-encrypting drive need to be restored.

Table 8

Action	Details	Suggested frequency
Backup configuration data	See 2.6.6 Backup/Restore	Daily

3.1.2 Test backup data

Test backups to provide assurance that the data backups contain the expected data and integrity.

Table 9

Action	Details	Suggested frequency
Test backup data	Load data from backup media into a non-production TycoAI server	Quarterly

3.1.3 Lock accounts on termination of employment

Disable user accounts of personnel who voluntarily or non-voluntarily are terminated from employment immediately.

Table 10

Action	Details	Suggested frequency
Lock accounts	Lock Linux user accounts	Immediately

3.1.4 Remove inactive user accounts

While an employee may still be employed by an organization in which the system is owned, managed, serviced or used by, they may not have utilized it for a long period. This suggests that independent of being authorized to use the system, they do not have a need to use the system and you should remove their user account. This is sometimes referred to as a use it, or lose it policy. This best practice reduced the amount of active user accounts in the system and therefore lowers the potential attack footprint.

Table 11

Action	Details	Suggested frequency
Lock accounts	Remove inactive Linux accounts and TycoAI admin GUI accounts.	Immediately

3.1.5 Disable unused features, ports and services

Reassess the need for optional features, ports, and services that are not required, and disable them. This practice will lower the attack surface of TycoAI suite resulting in a higher level of protection.

Table 12

Action	Details	Suggested frequency
Disabled unused features	See 2.2.4 Set boot sequence, 1.4 Communication ports table.	Quarterly

3.1.6 Check for and prioritize advisories

You can find security advisories for TycoAI suite on the Cyber Protection website. Access is provided once you have registered a user account with that site. User account registration is open to Tyco customers and authorized representatives. Determine if TycoAI suite is impacted by the conditions outlined in the advisories. Based on how the TycoAI suite system is deployed, configured and used, the advisory may not be of concern. Referring to as-built documentation of the TycoAI suite system will help with this assessment. A good set of as-built documentation will help you identify the number of components impacted and where they are located. While advisories call attention to a cybersecurity issue, it is not always possible to take immediate action or execute the full recommendation described in the advisories. If so, prioritization will aid in your planning to ensure that any issue impacting your system is fully and appropriately addressed in order of priority. Check for advisories from third party components such as networking equipment and operating systems by consulting with the respective vendor.

Table 13

Action	Details	Suggested frequency
Check for and prioritize advisories	Refer to https://tycosecurityproducts.com/CyberProtection/SecurityAdvisories.aspx	Weekly

3.1.7 Plan and execute advisory recommendations

Follow the plan determined in maintenance step 8.

Table 14

Action	Details	Suggested frequency
Plan and execute advisory recommendations	As determined in maintenance step 8	Based on priority

3.1.8 Check and prioritize patches and updates

While a TycoAI suite patch or update may or may not relate to a security advisory, it is always best practice to apply the most current patches and updates. These patches and updates can include cybersecurity enhancements also fixes to known issues. Review the release notes and prioritize the benefits of the patch or update. The overall benefit should include the improved protection that will aid in lowering the cybersecurity risk. Be sure also to check for updates and patches of third party components such as networking equipment and operating systems by consulting with the respective vendor.

Table 15

Action	Details	Suggested frequency
Check for and prioritize advisories	Refer to American Dynamics website	Weekly

3.1.9 Plan and execute software patches and updates

Follow the plan determined in maintenance step 10.

Table 16

Action	Details	Suggested frequency
Plan and execute advisory recommendations	As determined in maintenance step 10. Follow update process as outlined in Section 2.4.1 TycoAI suite and Operating System updates	Based on priority

3.1.10 Review organizational policy updates

Organizations may update their policies which include cybersecurity requirements. Changes to these policies can impact systems which were in compliance prior to the change. Periodically check to see if policy changes were made and re-assess compliance with those policies.

Table 17

Action	Details	Suggested frequency
Review organizational policy updates	Collect most recent security policies for your organization	Annually

3.1.11 Review updates to regulations

If TycoAI suite is deployed in a location that is governed by regulation, it is important to check to see if there are any updates to those regulations. In some cases, new regulations are introduced. Whether it is a review of an updated regulation to maintain compliance and a new regulation, an assessment of the changes should be conducted periodically.

Table 18

Action	Details	Suggested frequency
Review updates to regulations	Collect most recent copies of regulations as applicable. Perform a gap analysis against the deployed configuration.	Annually

3.1.12 Update as-build documentation

Update as-built documentation if the deployment architecture or component configuration changes. Some configuration changes happen without a formal project or plan and if such cases it may be common to negate updating the as-built documentation. Schedule a full update of the as-built documentation on a regular basis to ensure that all changes are documented.

Table 19

Action	Details	Suggested frequency
Update as-build documentation	See section 2.7.1 security documentation	Update as-build documentation

3.1.13 Conduct security audits

Periodic security audits are necessary as cybersecurity guidance, organizational policies, regulations, auditing processes, system use and configuration and threats have likely changed since the last audit. By conducting periodic security audits, the latest knowledge and conditions can be applied revealing gaps in protection previously undetected or created by changes in system use of configuration.

Table 20

Action	Details	Suggested frequency
Conduct security audits	See section 2.7.2 security audit checklist	Conduct security audits

3.1.14 Update password policies

Guidance on password policies has been evolving. Password policies should be re-assessed periodically to make sure the right policy in place for the target environment based on current organizational policies, regulations and guidance from standards organizations such as NIST.

Table 21

Action	Details	Suggested frequency
Update password policies	See section 2.2.5.1 operating system level user accounts (interactive)	Update password policies

3.1.15 Update standard operating procedures

Including best practices for cybersecurity within standard operating procedures can complement the protection that the system can deliver on its own. Depending on the procedures an operator uses, a gap in protection can be created, prevented or closed. Therefore, it is important to update standard operating procedures periodically.

Table 22

Action	Details	Suggested frequency
Update standard operating procedures	Collect standard operating procedures for use of tycoai suite within the organization	Annually

3.1.16 Renew licensing agreements

Assure that your TycoAI suite software license supports the necessary functions

Table 23

Action	Details	Suggested frequency
Renew licensing agreements	Collect active licensing details.	Annually

3.1.17 Renew support contracts

Assure that your TycoAI suite software support agreement (SSA) is up to date.

Table 24

Action	Details	Suggested frequency
Renew support contracts	Collect ssa details	Annually

3.1.18 Check for end-of-life announcements and plan for replacements

Review product announcements to determine if any of the components of TycoAI suite have a planned end-of-life announcement, including cameras.

Table 25

Action	Details	Suggested frequency
Check for end-of-life announcements and plan for replacements	Collect end-of-life details	Quarterly

3.1.19 Periodically delete sensitive data in accordance to policies or regulations

Table 26

Action	Details	Suggested frequency
Periodically delete sensitive data in accordance to policies or regulations	Collect details on policies and regulations that apply to your tycoai suite location	As required

3.1.20 Monitor for cyber attacks

Monitoring site perimeters, networks and end-points for cyber-attacks is a part of good cybersecurity operation. Many tools are available to assist with real-time analytics-based detection.

Table 27

Action	Details	Suggested frequency
Monitor for cyber attacks	Determine which security monitoring tools and services to implement	Run continuously once implemented

3.2.0 Patch policy

The policy documented here sets forth the current internal operating guidelines and process in regards to TycoAI suite, which may change from time to time at the sole discretion of Tyco. Tyco employs commercially reasonable efforts to pursue the operating guidelines and process described herein. However, other mitigating factors may prevent complete adherence to this policy, as determined by Tyco at its discretion. Regardless, Tyco endeavors to address issues that arise within TycoAI suite with the severity that they warrant.

When CRITICAL security vulnerabilities are discovered within TycoAI suite, Tyco will use commercially reasonable efforts to issue a Critical Service Pack for the current version of TycoAI suite as soon as is reasonably practicable.

When non-CRITICAL vulnerabilities are discovered within TycoAI suite, Tyco will use commercially reasonable efforts to:

- Apply fixes for HIGH severity vulnerabilities in the next immediate release of TycoAI suite
- Apply fixes for LOW and MEDIUM vulnerabilities within one of the next two available releases of TycoAI suite

Note: The TycoAI suite does not have a back port policy. Updates are only applied to latest version of the released product.

3.3.0 Release schedule

An update to TycoAI suite including new features and security fixes is released approximately every 6-8 months.

An interim update that will include only updates for the operating system will be released approximately three months after each release, unless there is a TycoAI suite release within this timeframe.

No TycoAI suite update will be released without undergoing extensive quality assurance testing.

An update to the TycoAI suite including new features and security fixes is released approximately every 6-8 months.

3.4.0 Customer specific testing

If a customer requires specific testing (for example, deployed architecture and configuration) on a TycoAI suite, the Cyber Protection Team is available to provide consultation and response directly to the testing team. For assistance, contact TSPCyberProtection@jci.com

The TycoAI suite regularly undergoes repeated security tests during the development process including network vulnerability scans. Web application scans are done on a regular maintenance schedule. Web applications are also tested during development to identify flaws such as cross-site injection points and missing security flags. Proprietary code is analyzed during the development cycle for items such as buffer overflow points, null dereference points and memory leaks. Third party and open source code is continuously scanned to identify released security flaws.

3.4.1 Vulnerability assessment

Vulnerabilities discovered in TycoAI suite proprietary software are assessed on the CVSS v3 score.

CVSS v3 Score, Assessment

≥ 9, Critical

≥ 7, High

< 7, Medium

3.4.2 Vulnerability assessment – third party components

Vulnerabilities discovered in TycoAI suite proprietary software are assessed on the CVSS v3 score.

CVSS v3 Score	Assessment
≥ 9	Critical
≥ 7	High
< 7	Medium

3.4.3 Vulnerability assessment – third party software

Tyco must use commercially reasonable efforts to monitor third party and open source software included within the TycoAI suite for disclosed vulnerabilities from the product vendors and open source communities. Vulnerabilities that are discovered and disclosed will be assessed first on its assigned CVSS v3 score from the product vendor or the National Vulnerability Database and then on the ability to be exploited within the TycoAI suite.

CVSS v3 Score	Exploitability	Assessment
≥ 9	Exploitable	Critical
≥ 9	Not Exploitable	High

≥ 7	Exploitable	High
≥ 7	Not Exploitable	Medium
< 7	Exploitable	Medium
< 7	Not Exploitable	Low

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

3.4.4 TycoAI suite vulnerability reporting

To better protect our customers and honor the trust they put in us, we are firm believers in responsible coordinated disclosure. Security Researchers, consultants and others who believe they may have found a potential security vulnerability in a Security Product can make immediate notice to our Cyber Protection Team through email to **TSPCyberProtection@jci.com** or by the **Building Products Vulnerability Reporting** webpage to make immediate notice to our Product Security Incident Response Team (PSIRT).

Those working directly on behalf of a Security Products customer should also notify their local Security Products representative. Thank you for your partnership with us in creating a smarter, safer more sustainable world

Additionally, Tyco Technical Support staff have direct access to the Cyber Protection team to help assess and resolve any issues.

Appendix A.1 Operating system level user accounts (non-interactive)

The following built-in operating system level user accounts are used for non-interactive processes:

Known Limitation: The TycoAI suite has Linux built-in accounts present on the operating system. These accounts are non-interactive and there is no log on to these accounts

User	Description
Lp	This account is used for printer systems.
Man	This account is used to run the man page.
nobody	Owns no files and is used as a default user for unprivileged operations.
chrony	Chrony Daemon
messagebus	This account is a combination of a common data model, a common command set, and a messaging infrastructure to allow different systems to communicate through a shared set of interfaces.
Rpc	This account is used to route requests between clients and servers.

statd	It is used by the NFS file locking service, rpc.lockd, to implement lock recovery when the NFS server machine crashes and reboots.
Ntp	Account is used by the operating system which sets and maintains the system time of day.
sshd	Performs unprivileged operations for the OpenSSH Secure Shell daemon.
dhcpd	Account is used by the dhcp server daemon.
oprofile	A system-wide statistical profiling tool for Linux.
polkitd	This account provides the org.freedesktop.PolicyKit1 D-Bus service on the system message bus.
pulse	Account is for the pulse audio daemon. It is used for the push-to-talk audio feature.
rtkit	RealtimeKit
systemd-coredump	systemd Core Dumper
systemd-network	systemd Network Management
systemd-timesync	systemd Time Synchronization
srvGeoClue	User for GeoClue D-Bus service
vnc	user for VNC
gdm	Account is used for the display manager

Appendix A.2 Operating system level service accounts (non-interactive)

Operating system level service accounts (non-interactive)

The following accounts are non-interactive and only used to run TycoAI suite services on the operating system.

User	Description
postgres	Used to run the database server.
TycoAI	This account is used to run all TycoAI suite application services
wwwrun	This account is used to run the Apache webserver.
couchdb	Used for the UI and API databases.
epmd	Used to run the erlang port mapper daemon for couchdb.
rabbitmq	Used for internal TycoAI event notifications.