Consumer Technology Association™

CONNECTED HOME SECURITY CHECKLIST

Use this paper checklist to assist you during installation and configuration at the client site, if you are unable to access the Online Tool.

After completing the checklist, copy this information into the Online Tool (CTA.tech/checklist) to receive a rating and report showing the scoring system. You can then email a copy of the report to your customer or yourself.

Passwords

□ Critical step: Change default username and create unique, not obvious, username OR verify manufacturer used a unique, serialized username and password on a per-device basis.
□ Use strong passwords.
□ Get permissions in writing for managing client passwords for all relevant systems.
□ Use password encryption.
□ Use different passwords for all devices and systems.

INSTALLATION TIPS

- Ensure the client is using a password management tool (paper or electronic).
- Be selective with any password hints.
- Update passwords regularly or schedule password updates in a maintenance agreement.

Networking

□ Critical step: Change default username and passwords for all networks.
□ Use strong passwords on all networks.
□ Recommend installing up-to-date anti-virus and anti-malware tools on customers' computers, or recommend they seek professional help.
□ Create a log-in without administrative privileges for client.
□ Limit access from outside physical structure of the client site.
□ Ensure live Ethernet connections are not available outside the home.
□ If the system is utilizing power line networking technology, block the signal for outdoor power receptacle.

Segment the Network for Different Purposes

□ Critical step: Change default username and passwords for each VLAN.
□ Use strong passwords for each VLAN.
□ Create segmented VLAN for different uses.
□ Separate Wi-Fi channels among the segments.
□ Separate physical cable networks.
□ Use a separate network or VLAN for gaming systems.
□ Ensure port forwarding and UPnP are disabled on the WAN.
□ Use a hardwired network when available.

Set Up Basic Security

INSTALLATION TIPS

- Take snapshot of current device configuration to compare to in the future.
- Use network monitoring app.
- Use automated tools to help with configuration and change tracking.
- A/V Components - Apply security guidance here as well.

□ Minimize DHCP range.
□ Disable port forwarding on unused functions, if applicable.
□ Take snapshot of network's 'as-built' configuration for reference.
□ **Critical step:** Secure the Wi-Fi Network to the highest available level of security.
□ **Critical step:** Enable Wi-Fi Encryption.
□ Disable a network DMZ, if applicable.
□ Change the router's default SSID.
□ Turn off router SSID broadcasting.
□ Disable WPS (Wi-Fi Protected Setup).
□ For a higher level of security, enable wireless MAC Filtering.
□ Set up a guest network with separate password protection and SSID.
□ Determine available VPN protocols for installation compatibility, performance and security requirements in all supported devices.

Modems and Routers

□ Install a stand-alone modem instead of an all-in-one router/modem.
□ Install a stand-alone router instead of an all-in-one router/modem.
INSTALLATION TIP: If using a modem/router from the ISP, disable DHCP & Wi-Fi. Connect via bridge mode to your router.
□ Install the latest available firmware on router.
INSTALLATION TIP: Check to see if the ISP is updating the box firmware.
□ Critical step: Change default administrator username and password on router.
□ Use strong password on router.
□ Disable port forwarding on the router, if possible.
□ Disable WAN UPnP and HNAP on the router.
□ Disable WPS on the router.
□ Enable the router firewall.
□ Disable port forwarding on the router.
INSTALLATION TIP: Unblock ports used by consumer's applications.
□ Use nonstandard port values on the router for applications.
□ Segment remote access on a separate network.
INSTALLATION TIP: Partner with a vendor that provides additional network security.
□ Check the private network with a port scanning tool.
□ Log out of admin services when done configuring the router.

Consumer Network Management Tools and Devices

□ **Critical step:** Change default username and create unique, not obvious, username OR verify manufacturer used a unique, serialized username and password on a per-device basis.
□ Use strong passwords on all devices connected to the CNMD.
□ Use whitelist, blacklist and other resources to minimize hacking, intrusion and other malware and limit access to suspicious social networks, search engines and websites.
□ Limit access on all network connected devices to firmware updates and content related to their specific purpose.
□ Identify and set-up parameters and document ongoing maintenance needs.

VPN

□ Critical step: Change default username and passwords.

□ Use strong passwords.

□ Encrypt all data going out of the network using VPN Router/Service.

□ Select hosted "cloud" VPN services based on logging policies and other user privacy protections.

□ Use recommended, current encryption protocols such as Transport Layer Security (TLS 1.2 or higher).□ Set up secure remote access through VPN or vendor specific applications.

INSTALLATION TIPS

- Follow and document requirements for VPN installation for remote access.
- Follow and document requirements for VPN installation for "cloud" servers.

Z-Wave

□ Critical step: Change default username and passwords on Z-Wave control devices and software.

□ Use strong passwords on Z-Wave control devices and software.

□ Record the unique Z-Wave home ID for all installations and keep confidential.

□ Always create unique home IDs; never recycle or reuse.

□ Password protect the primary controller and/or gateway to ensure only authorized individuals can maintain, change or add to the designated Z-Wave mesh network.

□ At time of installation, document all products to ensure all points on the Z-Wave mesh network are known and can be reliably maintained for security.

□ If a home ID is compromised, regenerate a new Home ID for this installation and assign to all documented products in the installation via the primary controller.

□ Use Z-Wave AES 128 network security keys and keep them confidential.

□ Use lowest possible RF power settings with Z-Wave products.

□ Critical step: Ensure any Internet connected Z-Wave gateways are properly firewalled and protected.

□ Limit access and provide physical security for Z-Wave primary controllers/gateways.

ZigBee

□ Critical step: Change default username and passwords on Zigbee control devices and software.

□ Use strong passwords on Zigbee control devices and software.

□ At time of installation, document all installed ZigBee products to ensure all points on the ZigBee mesh network are known and can be reliably maintained for security.

□ Critical step: Ensure any Internet connected ZigBee gateways are properly firewalled, filtered and protected on an installation.

□ Use ZigBee's AES CCM security suite to establish an 802.15.4 network encryption key, where possible.

□ Enable ZigBee application layer security, if available, for enhanced protection of designed installations.

□ Limit access and provide physical security for ZigBee coordinators/gateways.

Beacons (NFC/RFID)

□ Critical step: Change default username and passwords on Beacons.

□ Use strong passwords on Beacons.

□ Install NFC readers so as to minimize unwanted physical access.

□ Install RFID readers so as to minimize unwanted physical access.

□ Install beacons so as to minimize unwanted physical access.

Bluetooth

□ At time of installation, document all installed Bluetooth products to ensure all devices are known and can be reliably maintained for security.

□ Enable all Bluetooth 128 bit encryption and/or password/PIN authentication mechanisms.

□ Verify all applicable Bluetooth devices are non-discoverable after initial installation and provisioning.

□ Confirm internet-connected Bluetooth applications are properly firewalled, filtered and protected.

□ Verify visible beacons on Bluetooth low-energy applications do not contain sensitive information.

A/V Components

□ **Critical step:** Change default username and passwords on A/V Components.

□ Use strong passwords on A/V Components.

□ Disable and/or cover built-in cameras when applicable.

□ Use wired network connections over Wi-Fi whenever possible.

□ Implement process for managing streaming account credentials.

INSTALLATION TIPS:

- Minimize replication of streaming accounts across multiple source components.
- Require clients to create strong credentials for streaming accounts.

Home Security Devices

□ Maintain system policies on activation, testing and turnover.

□ **Critical step:** Have client change master code and store in safe place.

□ **Critical step:** Change default username and passwords on secure.

□ Use strong passwords on security devices.

□ Leave client clear instructions on how to change and manage master codes.

□ As a dealer, only maintain installer codes, not master codes.

INSTALLATION TIPS:

- If the customer wants the dealer to maintain codes, ensure a written agreement is used.
- Protect the content of client-monitoring agreements by storing them securely.

Mobile Devices

□ **Critical step:** Change default username and passwords on mobile devices.

□ Use strong passwords on mobile devices.

□ Don’t let mobile device save passwords, require user to enter every time used.

□ Ensure client knows how to manage system passwords and updates to software.

□ Ensure client knows how to administer remote and local access on mobile devices (across all platforms).

□ Ensure client has set up remote administration of mobile devices, including remote access and back-ups; in case of loss or theft.

INSTALLATION TIP: Share best practices with all users of system (i.e., don’t share passwords).