VERITY®
knowledge base
article #40 in a series

HART intercivic™

Cleanliness at the Polling Place

Keeping in mind concerns about COVID, influenza (flu), and other contagious diseases, Hart recommends the following best practices for polling place cleanliness.

Cleaning Hart Equipment

Touchscreens and other contact surfaces of Hart Verity equipment should be cleaned using a clear Isopropyl Alcohol / De-ionized water-based solution using a lint-free wipe. To clean and sanitize it is best to use a 70/30 mix solution, 70% isopropyl alcohol and 30% deionized water. Do not use other ingredients or fragrance-based solutions.

To ensure cleanliness and to avoid damage to Hart equipment, follow these best practices:

- **Wipe polling place devices and booths with a lint-free cloth that has been slightly dampened with 70% clear isopropyl alcohol.** It is best to do this after each voter uses the equipment.
- To avoid spotting, make certain that equipment screens are wiped dry. **Do not spray or pour cleaning solutions on equipment, and do not leave puddles.**
- **Do not use any other type of ammonia, bleach or detergent-based solutions on Hart equipment**, as these will be harmful to the touchscreens or the plastics surrounding the displays.

Sanitization and Paper Ballots/Duo PVR Paper

Both paper ballots and Duo PVR paper can become damaged and rendered unscannable if they become wet from hand sanitizer or alcohol-based sanitizing solutions. Hart encourages jurisdictions to provide hand sanitizer at the polling place exit, *but not to voters prior to handling paper ballots.* **Liquids, including hand sanitizer, can smear paper ballots of any type and make them unreadable.**

Touchscreen Styluses

For customers who would prefer to provide a disposable touchscreen stylus or a reusable stylus that is sanitized after each voter use, **do not use a stylus with a point**. Long Q-tip® type disposable styluses work well, for example.

Additional Recommendations:

- Provide single-use, disposable, ear covers for device headphones, and replace them after each voter.
- Remind poll workers and staff at voter check-in stations to regularly wash their hands with soap for at least 20 seconds and wipe down voter check-in equipment and polling place contact surfaces throughout the day.

VERITY™
knowledge base
article #6 in a series

HART intercivic™

Best Practices - Verity Hardware Keys

About Verity Hardware Keys

Each Verity voting device (Verity Touch Writer, Verity Scan, Verity Touch, Verity Controller, etc.) requires a set of three hardware keys to set up and operate. To avoid confusion among pollworkers and staff, Hart recommends that jurisdictions develop a hardware key labeling system. In addition to limiting confusion, a proper key labeling system can help ensure that access to each key type is limited to the pollworker and staff with the proper security clearance to use that key.

There are three hardware keys associated with each device:

- The key used to open the device case
- The key used to lock and unlock the device tablet
- The key used to lock and unlock the vDrive compartment and/or ballot box

The "Stoplight" Method of Labeling

Color-coding each key using the "Stoplight" method (Green, Yellow, and Red) is a simple way to avoid confusion:

- **Green Key**: The first key a poll worker would use, to open the outside of the Verity device case.
- **Yellow Key**: The second key a poll worker would use, to lock and unlock the Verity device tablet. This is a more important key than the Green key, but still one that any of the pollworkers can use.
- **Red Key**: This key accesses any compartment that stores ballot information - the vDrive compartment and/or the ballot box. This is the most important key for device security. As such, only the lead poll worker or an elections staff member would have authority to use this key.

VERITY®
knowledge base
article #17 in a series

HART intercivic™

Verity Security Features

About this Document

Verity system security was designed following the most current best practices in voting and computer technology. In addition, Verity has been thoroughly tested by a voting system test laboratory (VSTL) accredited by the U.S. Election Assistance Commission (EAC), to ensure proper security and software functionality. The Verity system provides security in depth, with multiple, overlapping levels of physical and digital security features combined with comprehensive auditing capabilities. This document explains several of the most important security features of the Verity system, including:

- Device Physical Access Controls
- Kiosk Mode
- Device Secure Boot Process
- The 'Trust List'
- Tamper Evidence
- User Authentication
- Audit Logging
- Vote Security

Device Physical Access Controls

Non-standard physical connections are used for external ports on Verity devices, including the USB ports used for Verity Touch Writer printers, and the Verity Controller & Touch DRE booth connection cables. The use of non-standard port connections prevents unauthorized users from inserting any standard or commercial of-the-shelf cables or devices. In addition, the physical ports use non-standard wiring, which prevents any non-Verity device from being recognized.

As an added security measure, integral sliding port covers are included that may be secured with tamper-evident seals by the jurisdiction when the ports are not in use. Tamper-evident seals may also be fastened to the Verity device handles, and on locations that store ballots or vote data (for example, the vDrive compartments on Verity Scan or Controller and the external doors on the Verity Ballot Box). In addition, keyed locks are used to prevent unauthorized access to the vDrive compartment, ballot box, and device cases.

Kiosk Mode

All Verity workstations and voting devices operate in what is known as kiosk mode. In kiosk mode, users can only work in the Verity voting applications, thus preventing access to the desktop or operating system of the computer or device. This prevents introducing unauthorized applications to the computer, prevents malicious changes to the operating system itself, and enhances overall system security. Because of this enhanced security, all tasks that involve transfer of data to or from an external source (importing data, exporting data, saving archives, etc.) must be completed using external USB data storage devices.

Device Secure Boot Process

Software startup for each Verity voting device may take several minutes, due to security and data integrity checks performed by the Verity software. This process is included in the design of the Verity voting system to verify the authenticity of the software before allowing it to operate on the device, and is known as a secure boot process. The secure boot process includes write-protection technologies to prevent the installation of viruses and malware, and employs integrity checks on all software applications before they are allowed to run. These integrity checks validate that the software is in fact the trusted, authorized program (and not a malicious program with the same name).

The Trust List

The Verity system uses a "trust list" to block all unauthorized applications from running on the system. Use of a trust list limits the applications that are permitted to run on a system. If a particular application attempts to execute on a system that uses a trust list, the system checks the application against a list of permitted applications (the 'trust list'). Verity is also configured to hash check all executables, without exception, against that list. Anything that fails validation is prevented from running. In short, if the application is not on the list, Verity won't allow it to run.

A 'trust list' is the opposite of a 'block list', which is the method used by many antivirus programs. With a block list, applications that appear on the block list are blocked, while any that do not appear on the list are allowed to run. The block list must be constantly updated as new threats emerge, and often cannot provide protection until after the system may already be infected. The disadvantage of a block list is that it is 'reactive' (responding only to viruses, applications, and malware that are already known to be a threat), while use of a trust list is proactive (responding to any new threat that may occur, and eliminating the need to constantly update the list of malicious applications that must be blocked).

This method allows the Verity system to protect itself both against the threats that exist today, as well as those that may exist in the future, without the need for the computer to be updated via the Internet or any other means.

Tamper Evidence

All Verity software on Verity workstations and voting devices is tamper evident; any attempts to alter the function of the software would be evident when tested. Testing may be performed at any time, using built-in functionality that allows the user to export the **Hash Values** of the installed software on both Verity workstations and voting devices. A Hash Value is the digital 'fingerprint' of a software application; Hash Values can be externally compared to the trusted software build on file with the Election Assistance Commission (EAC), to ensure that the installed software is identical to the software certified by the EAC. For more information on **Hash Testing**, see the Verity Knowledge Base article *Hash Testing for Verity Software and Devices*.

In addition to the tamper-evidence of the software itself, Verity digitally signs certain data (e.g. election definition files, vDrives, etc.) to provide tamper evidence while maintaining transparency.

User Authentication

Verity applications are designed to ensure that they are accessible only by authorized users. Authorized users, in turn, are required to identify themselves using a login name and password prior to gaining system access.

Authorization

Role-based permissions determine the operations that each user can perform. Only users with the proper privileges can view or change data. Administrators assign a **user role** to each user, ensuring that each user has access only to the abilities and information authorized by the administrator.

Passwords and Authentication

In addition to an assigned user role, each Verity user also has a unique login name and password. Verity password management rules are modern and flexible. When each user logs in, Verity ensures that the user name and password are valid before the user can access the software. An administrator can configure user accounts for Verity in each jurisdiction. Hart recommends that all jurisdictions follow standard security best practices in regards to password complexity and the storage of user credentials.

Verity Key

Verity Key is a small security device that election staff program for each election. An authorized user must write a Verity Key for *each* new election, making the Key specific to that election. User passwords for Verity Key may be election-specific and user-specific.

Verity Key is part of the Verity Voting **two-factor authentication** process. Two-factor authentication requires that each user have something (a programmed Verity Key, inserted into the workstation or device) and know something (a relevant passcode associated with the Key). Verity must authenticate both the user passcode and the Verity Key together. Each Verity Voting application requires the Key before allowing certain operations to occur. Critical operations within the Verity Voting system require the user to insert the Verity Key and enter the passcode. Only when the Verity system authenticates the Verity Key and password will it allow the operation to continue.

Audit Logging

Verity records comprehensive logs for all activity performed in the Verity Voting system, as it occurs. Each Verity component (application or device) maintains its own log. Logs are a critical part of maintaining security by providing an audit trail. Logs are created uniformly across applications and voting devices.

Each Verity component writes two logs:

- **Audit log**: Contains election-specific logging events, such as any changes to an election and any exceptions or errors encountered in the application.
- **System log**: Contains events pertaining to system actions such as logins, password changes, etc.

Reading Audit and System Logs

Verity Audit and System logs use plain language, and are designed to be clear and easy-to-read. Audit logs allow the auditor to clearly see a list of events, the time the events occurred, and the user logged in when the event occurred. Log data includes the following information:

- The Verity application name and full version number (in header)
- The election ID (in header)
- Information for each event:
  - The date and time when the event occurred
  - The voting device serial number or workstation ID
  - The user logged in at time of event
  - The event name (in plain text)
  - The event details (in plain text)

Users may export application Audit Logs and System at any time, for the desired date/time range, from the appropriate workstation. Users may filter and export Device Audit Logs from Verity Count. Users can export logs as comma-separated values (CSV) to allow for external data searching and additional filtering.

Vote Security

The ballot choices of each voter are stored in the Verity System as Cast Vote Records (CVRs). To protect voter privacy, CVRs are not stored in any discernable order. In addition, CVRs do not contain voter information connecting a ballot (or CVR) to a specific voter. The use of digital signatures makes CVRs tamper-evident. CVRs are stored in multiple locations for security and auditability, risk mitigation, and disaster recovery. Users can filter and export CVR data for external auditing purposes using the Verity Count Auditing Dashboard. CVR data may be filtered by any one or a combination of several criteria, including location (polling place, precinct, or district), voting equipment type, voting type, and ballot content (contest or choice).

VERITY®
knowledge base
article #20 in a series

HART intercivic™

Rechargeable Battery Best Practices

overview

This document outlines the best practices for the use of rechargeable system batteries in Verity devices. If you have any questions regarding these procedures, please contact the Hart Customer Support Center at 1-866-ASK HART.

battery specifications

Hart rechargeable batteries are lithium-ion Smart Batteries. Smart Batteries constantly communicate with the processor to determine voltage and discharge rate when active, and have built-in over voltage/over current protection. Hart system batteries are fully rechargeable (up to 500+ cycles) and include an integrated tester. Batteries are not shipped with a full charge. Batteries should be charged fully before their first use in an election. Battery life specifications are listed below:

- A fully charged battery will provide not less than 2 hours of backup power when installed in a device.
- A fully charged battery loses less than 10% of its charge over 90 days while connected to a device that is powered off, and 1% per day while the device is powered on and running on AC power.
- IMPORTANT: Avoid allowing batteries to completely discharge to less than 10%; A completely depleted battery may become damaged to the point where it can no longer be recharged.

IMPORTANT: Do not expose system batteries to temperatures above 60C (140F). Do not mishandle or disassemble battery modules. Failure to follow these instructions may present risk of explosion, fire, or high temperatures.

proper shut down procedures

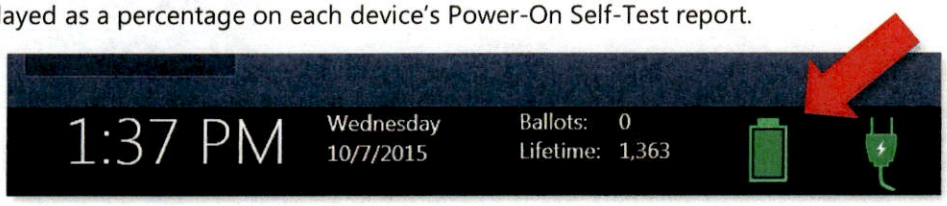
IMPORTANT: When powering off a Verity device, it is important to press the red power button on the back of the Verity device to power it down, and wait for the Verity device to be completely powered down and showing a black screen before unlocking the tablet and removing it from the cradle.

Removing the Verity tablet before the device has completely shut down will cause the Verity tablet to enter a 'hibernation' mode, which will deplete the system battery if the battery is left connected. If a battery becomes fully depleted, the battery may become permanently damaged, and unable to be recharged.

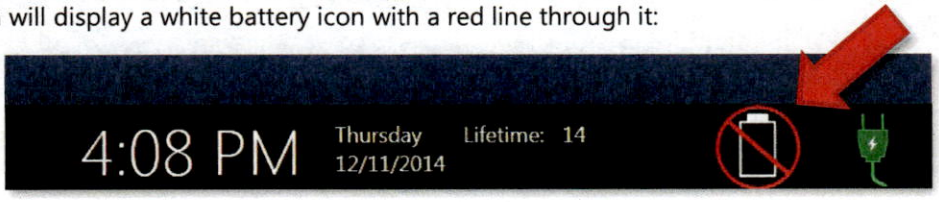
general use recommendations

When properly installed, and fully charged, a system battery will provide not less than 2 hours of backup power. Verity devices will automatically switch to available backup battery power if the device is disconnected from AC/wall power.

The relative charge of the system battery is displayed via a green battery icon on the Verity device screen, in the lower right corner (except during voting sessions). This icon shows only the approximate charge of the battery; the current charge level is displayed as a percentage on each device's Power-On Self-Test report.



If the device does not have access to backup battery power (the battery is disconnected, depleted, damaged, or not present), the screen will display a white battery icon with a red line through it:



charging recommendations

Use only Hart-approved battery charging stations; two sizes of charger are available: a single bay battery charger and a six-bay battery charger.

Batteries should be removed from storage, fully recharged and installed in the Verity voting devices no more than 30 days before an election. This will maximize the battery backup time available in the event of an AC power loss to the device. Charging time may vary depending on the current charge level of the battery, and may take up to 4 hours for a fully depleted battery.

battery storage

After an election, batteries should be removed from devices, tested, and stored in a cool, dry location. To maintain the working life of the battery and for improved battery safety, batteries should be stored with a charge of between 40%-60% (for instructions on testing the battery charge, see below).

IMPORTANT: Batteries should never be left in the device for long term storage (i.e. between elections).

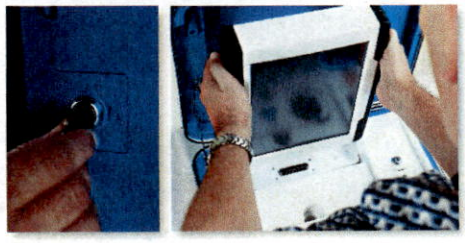
installing, removing, and testing system batteries

IMPORTANT: Ensure that the Verity device is completely powered down before disconnecting the tablet and accessing the system battery.

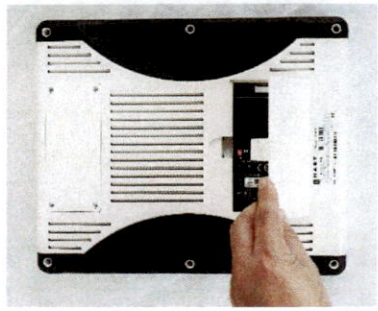
To access the system battery (to test, remove, or replace):

1. Press the red power button on the back of the device to turn it off. **Wait for the Verity device to be completely powered down and showing a black screen before unlocking the tablet and removing it from the cradle**

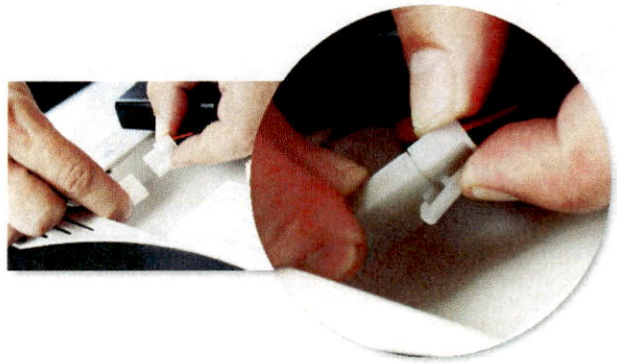
2. Unlock and remove the device tablet from its cradle.



3 On the back of the tablet, open the battery door.



4 To connect the battery, the tab on the connector coming from the battery must snap over the tab on the wire coming from the tablet. Failure to connect the battery properly can result in fire and damage to the device. To disconnect a battery, hold the white plastic connecters at both sides with your fingers, press on the tab, and pull gently.



5 Press the "TEST" button on the front left of the new battery to test the battery charge. Green lights should illuminate indicating the approximate charge. The charge level indicated is the *maximum* charge, in increments of 20% (e.g. if the lights indicate a charge level of 40, then the battery has between 21%-40% charge).