Elite Security Hardening Guide

KEYper ASSA ABLOY

Rev	Date	Editor	Description	ECN

A	01/26/2022	John Bishop	Document placed under control	
B	12/2/2020	John Bishop	Added Version History Table	
C	10/28/2021	Justin Flatt	Added SQL encryption information	
D	01/23/2024	Elizabeth Tingley	Changed branding to KEYper ASSA ABLOY	

Contents

Customer Care Contact Information

Most items detailed in this guide require assistance from our customer care team to ensure proper configuration. For assistance with the content found in this hardening guide or any issues related to your system, please contact our customer care team using one of the methods below:

Business Hours Tech Support

Call – 704.455.9400
8:00am – 5:00pm EST, Monday – Friday

After Hours Tech Support

Call – 704.455.9400
5:00pm – 11:00pm EST, Monday – Friday
8:00am – 11:00pm EST, Saturday – Sunday

Online Support Request Form

https://www.keypersystems.com/support/

Internet Security Policy

KEYper Systems should not be assigned a Public IP Address or made publicly accessible on the internet. We do not recommend a publically exposed internet connection for our products due to the associated security concerns. Ultimately it is your decision and there may be a particular reason you wish to configure the system in this way, but we want to ensure that you are aware of the associated risks. If you wish to configure your system to be publically available on the internet, you can complete the form at the following link Internet Security Acknowledgement Form.

Data Privacy Protection Recommendations

Plain Text Fields

Due to the way pertinent information associated with plain text field entries is displayed throughout the Elite applications it is recommended to avoid using sensitive personal information when filling out details for any plain text field. Considerations for entering information under assets and users are detailed below:

Assets

The asset name, description, and attributes are visible when filtering in the kiosk application, viewing reports in the web admin, or when a report is emailed out. Please take this into consideration when entering asset details during the registration process.

Users

The user first name, last name, and description are visible when filtering in the kiosk application, viewing reports in the web admin, or when a report is emailed out. Please take this into consideration when entering user details during the registration process.

Digital Images and Biometric Templates

Two optional features of the Elite platform are a biometric scanner and digital camera. The biometric scanner may be implemented to allow users of the system to login with their fingerprint. The digital camera may be implemented to capture a digital image of each transaction or exception event. It is recommended that users and administrators of the system understand how this information is used and stored by the Elite applications. Considerations for each are detailed below:

Digital Images

By default, systems are equipped with a camera so that the organization can record a photo of each user at login as well as during an exception event (illegal action by the user). The organization can choose whether to use this camera or deactivate it. Images obtained are stored locally in the onboard PC that resides inside the kiosk cabinet.

Biometric Templates

By default, systems are equipped with a biometric scanner so that the organization can offer a fast and effective way for users of their system to login. The organization can choose whether to use this biometric scanner or deactivate it. During the “enrollment process”, a digital value obtained from a few specific locations on the finger, called the “template”, is transferred from the finger reader to the Elite database (within the “master cabinet”). During operation of the cabinet (i.e. a user identifying themselves with their finger to access the cabinet), the sensitive data is processed entirely within the reader/DLL, and the value output by the reader is essentially a data record reference number. Biometric templates are permanently deleted from memory upon user deletion. Templates are encrypted throughout the Elite applications using AES-256 (in-motion and at-rest) in versions of the software greater than or equal to 7.0.7492.

Database Access

Our support staff utilize data access to your system to provide unrivaled support and diagnostic troubleshooting. Our database configurator application can be used to change the SQL account password assigned to your system's database. To request a password change simply visit the Client Info Portal on our website at the link below.

https://www.keypersystems.com/products/client-info-portal/

We offer several options for KEYper's level of access to the database:

Unattended Access

Support can access the database without assistance from the end user. In this scenario, your database password is unchanged from the one which was assigned when your system was produced.

Attended Access

Support can access the database only when the end user is present. In this scenario, your password is changed to your selection and KEYper maintains a copy of the password to be used with your explicit and recorded approval during a support scenario.

No Access

Support has no access to the database. In this scenario, your password is changed and KEYper does not keep any record of your new password. If your password is lost or forgotten, KEYper may be able to re-install SQL Server and restore your database from a backup but data loss may occur in the process.

SQL Server Encryption Options

Microsoft SQL Server offers several layers of encryption to help you protect your data.

SQL Server Always Encrypted (Column level encryption)

Always Encrypted allows for the client application to transparently encrypt data in specific columns in the database (Ex. User data) without revealing the secret keys to the database engine. This ensures that database administrations or other high-privileged unauthorized users from being able to access the encrypted data.

Requirements

- Minimum SQL Server 2016 (SQL Server 2019 also allows for Secure Enclaves)
- Database server must be installed on a separate server from the rest of the application to prevent secret keys from being stored on the same server as the database.

SQL Server Transparent Data Encryption (TDE)

** This functionality is not available for Express editions of SQL Server **

Transparent Data Encryption utilizes real time I/O encryption of data and log files using a database encryption key (DEK). Data is encrypted at the page level before being written to the filesystem and decrypted when read into memory. This functionality helps protect data if physical drives or backup tapes are stolen.

Requirements

- Requires Standard or Enterprise editions of SQL Server

Remote Support Access

Our support staff utilize eBLVD remote access software to provide unrivaled support and diagnostic troubleshooting. The level of remote access to your system can be changed at any time. To request a remote access change simply visit the Client Info Portal on our website at the link below.

https://www.keypersystems.com/products/client-info-portal/

We offer several options for KEYper's level of remote access to your system:

Unattended Access

Support can access the system without assistance from the end user.

Attended Access

Support can access the system only when the end user is present.

No Access

Support has no remote access to the system.

If you need further clarification on the above options for database/remote support access or wish to change the access level of your system at any time, please contact support.

Command Center Biometric Template Exclusion

One of the functions of the KEYper Command Center application is to maintain and secure a backup of your system's database in the cloud to be used in the case of an emergency. The cloud backup can be configured to exclude biometric templates by toggling a system setting. Details on the two different options are explained below:

Biometric Templates Included

When biometric templates are included in the cloud backup of your system's database, sensitive personal data is stored in the cloud but will result in a seamless transition from inoperable to operable in the event that your database requires restoration from the cloud backup.

Biometric Templates Excluded

When biometric templates are excluded from the cloud backup of your system's database, sensitive personal data is not stored in the cloud but will require all users to re-enroll their fingerprint in the event that your database requires restoration from the cloud backup.

Enhanced Elite Web Admin Login Security

The default credential used to login to the Elite web admin application is a numeric PIN. The system can be configured to require the use of a username and password instead (using this feature does not alter the functionality of the user's PIN code for logging into the Elite Kiosk application).

Password Requirements

Password must be at least 8 digits in length and contain at least one non-alphanumeric character.

Failed Login Attempt Lockout

If a user attempts to login unsuccessfully more than 5 times their account will be locked out and require an admin level account to intervene and remove the lock.

Reset Password

A user may reset their password by providing the email address associated with their account. After verifying their email address a new password will be sent to it.

Dual Authentication

The default way of logging into the Elite kiosk application is by the user entering their credential (PIN/Biometric/Prox/Swipe) at the login screen to authenticate themselves. The system can be configured to require Dual Authentication which requires a second user to approve the login of the first user by providing their credentials as well. Dual Authentication is configurable per user by selecting whether the user 'requires dual authentication' when

logging in, can be a 'dual authenticator' and provide authentication to users requiring it, or both from the user profile page in the Elite web admin. Safeguards are in place to ensure that a user cannot authenticate their own login if they both require dual authentication and are permissioned to be a dual authenticator.

Triple Authentication

The default way of logging into the Elite kiosk application is by the user entering their credential (PIN/Biometric/Prox/Swipe) at the login screen to authenticate themselves. The system can be configured to require Dual Authentication which requires a second user to approve the login of the first user by providing their credentials as well. The system may also be configured to require Triple Authentication which requires a third user to approve the dually authenticated login. Triple Authentication is configurable per user by selecting whether the user 'requires Triple authentication' when logging in, can be a 'Triple authenticator' and provide authentication to users requiring it, or both from the user profile page in the Elite web admin. Safeguards are in place to ensure that a user cannot authenticate their own login if they both require triple authentication and are permissioned to be a triple authenticator.

Two Factor Authentication

The system can be configured to require two separate credentials to successfully login to the Elite kiosk application. When this feature is enabled, the first factor can be biometric, proximity card, or swipe card; the second factor is always numeric PIN code (a fob can be used in place of PIN if touchless features have been installed/enabled). Upon the user presenting their first factor (Biometric/Prox/Swipe), the login form will display a notification message to the user requesting them to enter their PIN code. If the correct PIN code is entered the user is successfully logged into the kiosk application. If either factor presented is invalid or both factors do not match the user's record then an error message will be displayed and the user will not be allowed to login.

Shielded Assets

The system can be configured to require a second authenticator to approve the checkout of assets marked as 'shielded'. An asset may be designated as shielded on the assets page in the web admin under the 'Manage Assets' tab. Once this designation is established, any attempt to check this asset out of the system will require an approved authenticator to enter their credentials to verify the transaction as legitimate.

Disable PIN Login

The default way of logging into the Elite kiosk application is by the user entering their credential (PIN/Biometric/Prox/Swipe) at the login screen to authenticate themselves. The system can be configured to prevent a user level role from logging in with a PIN. When this feature is enabled, any user level role user will only be able to login with Biometric/Prox/Swipe. Admin level role users are not prevented from using their PIN to login when this feature is

enabled. Please take into consideration your local legislation surrounding biometric scanning/template requirements when enabling this feature.

Disable Diagnostics

The Elite kiosk application contains a built in diagnostic tool that can be used for informational, troubleshooting, and firmware/software upgrade purposes. It is enabled by default. The on-board diagnostics section of the application can be disabled to restrict users/admins from accessing this space. If disabled, only customer support will be able to access system diagnostics.

Disable Login Form Information

The Elite kiosk application displays pertinent system information at the lower left hand corner of the login form. This information includes software version, firmware versions, primary web service connectivity status, primary database connectivity status, digital camera connectivity status, Kiosk name/ID#, and system IP addresses. The display of this information can be disabled, completely removing it from the form and preventing it from being visible to anyone.

User Expiration Date

The Elite kiosk application can be configured to prevent a user from removing assets from the cabinet after a defined expiration date. When this feature is enabled the checkout button will be disabled and un-clickable after the set date expires. The date can be configured per user under the user's profile page in the Elite web admin application.

Strengthened Numeric PIN Options

The default credential used to login to the Elite web admin application and kiosk application is a numeric PIN. The default PIN requirement is 4 digits. The system can be configured to extend the PIN length requirement to six, eight, or fourteen as well restrict the PIN from containing contiguously sequential or matching numbers.

Six Digit PIN
Numeric PIN must be at least 6 digits in length.

Eight Digit PIN
Numeric PIN must be at least 8 digits in length.

Fourteen Digit PIN
Numeric PIN must be at least 14 digits in length.

Restrict PIN

Numeric PIN may not contain any contiguously sequential (increasing/decreasing) or matching numbers. The 'Restrict PIN' feature may be applied in combination to any of the length requirements above.

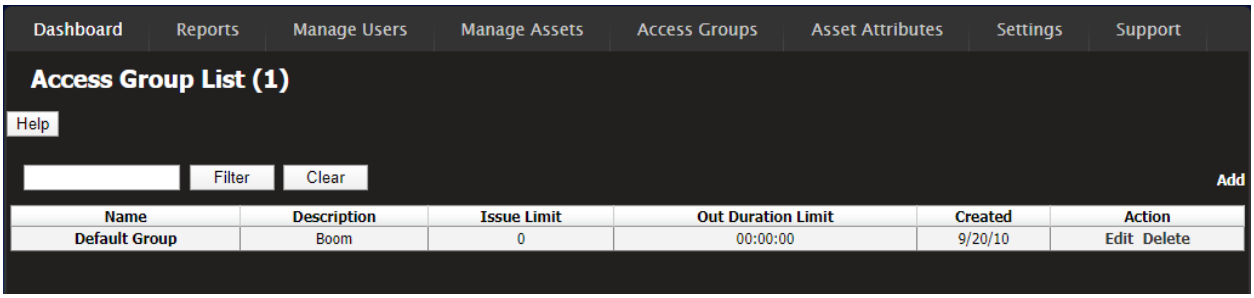
- Invalid Examples: 1111, 1234, 4321, 1297, 9813, 1152, 9931
- Valid Examples: 1357, 9753

Access Groups

Access Groups offer a way to restrict which assets users of the system have access. Restrictions can parameterized based on time, user, asset, or physical access (location, system, cabinet). Access Groups can be configured without assistance from the customer support team.

Default Access Group

There is a factory-loaded default **Access Group** named **Default Group**.



Edit Access Group Page

This facilitates rapid system configuration, quickly making the system operational. You may edit the default group, but DO NOT delete it. Standard settings for the Default Group are:

- 0 (Zero) Asset Issue Limit per user (0 = No Limit)
- 0 (Zero) Out Duration Limit per Asset (0 = No Limit)
- 24/7 access to remove and return Assets
- Access to all Locations, Systems, and Cabinets

Creating a New Access Group

- From the **Access Group** home screen click the **Add** button in the upper right.
- Fill In the desired **Name** for the access group (e.g. Managers).
- Fill in the **Description** for the access group (e.g. 3rd Shift Manager Access). **Not a required entry**
- Set the desired **Issue Limit** for the group. **0 indicates unlimited**
    - **Issue limit** – the number of keys each user in the group may have checked out of the system at any given time (e.g. If the limit is 10, each user in the group may have up to 10 keys checked out at any given time).
- Set the desired out duration time limit. **0 indicates unlimited**

- **Out Duration** – Once a key is out of the system past the set time limit, the assets status will change from **Out** to **Overdue,** and an alert will be sent to all recipients on the **Out Duration Exceeded Alert** list. 23 Hours, 59 Minutes is the maximum time that can be set for out duration.

- Click the **Save** button. This will add the group into the system and allow for configuration of the final settings.

Configuring Access Group Settings

*Note: Always click the 'Save' button after configuring or editing **Access Group** settings!*
From the **Access Groups** home screen, select **Edit** for the desired group.

Access Times

- Click the **Access Times** header to expand.
- Select **Add Time** from the upper right.
- Select the desired **Day**, **Start Time** and **End Time** (utilize 24 hr. format) and click **OK**.
- Repeat the process for each day of the week that you wish to allow users in the **Access Group** access to the system.

User List

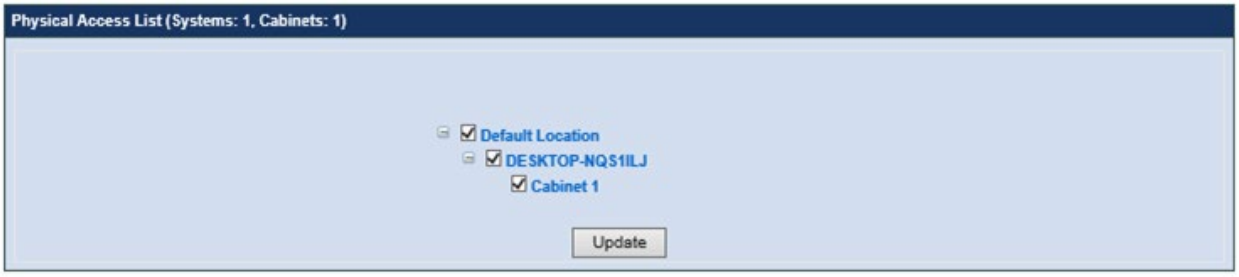
- Click the **User List** header to expand.
- Select **Edi**t to see the list of all users in the system.
- Choose **Select All** or use the check box to assign individual users to the group.
- Click **Save.**

Asset List

- Click the **Asset List** header to expand.
- Select **Edit** to see the list of all assets in the system.
- Choose **Select All** or use the check box to assign individual assets to the group.
- Click **Save.**

Physical Access List

- Click the **Physical Access List** header to expand.
- The **System Map** displays.
- Select the check box next to all **Locations**, **Systems** and **Cabinets** that you wish to assign to this group.
- Click the **Update** button.



Access Group Physical Access List

Once you have completed all of the above steps, click **Save** under **'Update Access Group Information'** to lock in all of your changes

System Alerts & Alarms

Data Privacy Protection Disclaimer: alerts may contain the first/last names of users

There are eight different alerts that will trigger an email and/or SMS alert from the system. Any user properly configured in the system can receive these alerts. Email settings and Alert settings can be configured without assistance from the customer support team by following the steps detailed below:

1. Configure phone number/phone service carrier and/or email addresses per user under the user's profile.
2. To setup a user to receive a specific alert, select the edit button in the upper right corner of the desired alert under alert settings in the Elite web admin, then select the check box next to the desired user name(s), click save, and then click close.

Illegal Asset Removal
An asset removal occurred without following the proper checkout procedure.

Out Duration Exceeded
An asset has not been returned to the system in the allotted time allowed as specified by the user's Access Group.

Door Open
A user has illegally opened a door to the system or failed to close it within the allotted time allowed during a check-in/out process.

Nightly Reports
A report listing all assets with a status of 'Out' at the time the alert is sent.

System Power Loss
The system has recovered from an unexpected loss of power.

Cabinet-to-Kiosk Communication Loss
Serial communication between the PC and the hardware inside the cabinet has failed or become intermittent.

Asset Not Locked In (lock-in systems only)
A fob inside the cabinet is not in not fully secured and locked into the socket.

Check In Mismatch
The user that removed the asset is not the user that returned the asset.

Some of these alerts have accompanying **Alarms** that require configuration by KEYper® Support. These alarms include the **Door Open** Alarm, **Illegal Asset Removal** Alarm, **Asset Not Locked In** Alarm (lock-in systems only), and a **Power Loss** alarm that triggers when the Kiosk experiences an unexpected loss of power. An audible siren can be configured to sound when the system is alarming. In addition to the siren, the Elite kiosk application login form flashes red and requires an admin level role user to login and acknowledge/clear the alarm. Our reporting suite documents the entire process and provides an audit trail showing the cause of the alert/alarm, with a date/time stamp of which user caused the event where applicable and a date/time stamp of which admin acknowledged/cleared the event.

Increased Hardware Fortification

Additional Cabinet Pad Lock
Puck lock and hasp, Production or Retrofit

12 Gauge Steel Cabinet
Default is 16 gauge, currently only offered in small cabinet size

NUC Enhancement
TPM Module available

Rear Cabinet Knockout
Knockout available for small/large cabinet size on the rear exterior of the cabinet allowing for Ethernet and DC power concealment.

USB Port Declaration
USB ports are located on the exterior or interior of the cabinet depending on manufacture date. For some this may pose an inherent security concern. The USB ports can be disconnected/disabled to prevent them from being accessible/active.

Uninterruptable Power Supply options (UPS)

Uninterruptable power supplies help to ride through power outages and brownout conditions.

Option 1
390Watts / 650VA, 120VAC, runtime less than one hour and dependent on use

Option 2
700Watts / 1.0kVA, 120VAC, runtime around two hours and dependent on use