

1. Keys	2
1.1 Import Keys	3
1.2 Assign to Users	5
1.3 Key Audit Setting	7
1.4 Key Generations, Key Types, and Special Regulatory Compliances	9
1.5 Key Status	11
1.6 Key LED Indications	12
1.7 Key Firmware Update Feature	14

Keys

Introduction

A key is a component that is used to unlock [cylinders](#) in the system. Keys are assigned to [users](#) and are serviced with [schedules](#) that establish which [openings](#) (door, gate, machine, cabinet, etc.) the keys will have access and at what times.



[Import Keys](#)

[Assign to Users](#)

[Key Audit Setting](#)

[Key Generations, Key Types, and Special Regulatory Compliances](#)

[Key Status](#)

[Key LED Indications](#)

Import Keys

Import Keys and Codebooks

The first step in setting up a new system is to import information regarding the keys and cylinders to be used in the system. If the system also includes the remote programmer accessory, specific information related to this special programmer will also need to be imported into the system. Medeco offers two different methods available to perform this informational import process.

One option is that Medeco can provide the key information in a file defined as security data packets or codebooks. There are codebook files for keys (key codebook), cylinders (cylinder codebook), and the remote programmer accessory (remote programmer codebook). Codebooks are emailed directly from the Medeco factory as attachments; the attachment containing the codebook for keys will have a .kbk file extension, the attachment containing a codebook for cylinders will have a file extension of .lbc, and the attachment for remote programmers will have a file extension of .rbk.

A second and more efficient option is to directly import codebooks from the factory. This option allows for an even greater ease to import the respective codebook information into the XT Web software.

Importing Codebooks from the Factory

Direct import of the codebooks from the Factory is a feature provided to those systems that are hosted on the Medeco XT Web servers.

Import Keys Directly

The codebook for keys is directly imported to the XT Web manager for systems that are hosted by Medeco. Once the codebook is successfully transferred to the Medeco hosted XT Web server, it is listed in the table on the **Import Codebooks** page as "Pending".

Step 1

The "Pending Codebooks" table lists the codebook type, quantity, and submission date, which are directly transferred by Medeco. The codebook record also displays an 'Accept' and a 'Remove' button. To complete the import process, select the 'Accept' button for the codebook. All key information is promptly imported and populated into XT Web. The 'Remove' button allows the codebook to be deleted from the table.

[Organization](#) | [Operation Logs](#) | [Import Codebooks](#) | [Remote Programmers](#) | [System Setup](#)

Import Codebooks

Codebook File

No file selected.

Pending Codebooks

Show 10 entries Search:

Codebook Type	Quantity	Date Submitted	
User Key	6	7/9/2014 2:04:18 PM	<input type="button" value="Accept"/> <input type="button" value="Remove"/>

Showing 1 to 1 of 1 entries

Step 2

After the import completes, select the **Keys** page of the Medeco XT Web manager. This page shows a table that lists the imported keys which can then be viewed and managed.

Import Keys via Email


Step 1

Attached with the email received by Medeco, save the key security data packet or codebook file to the computer.

Medeco NexgenXT

Sent: Thu 7/10/2014 11:24 AM

To: Jim Walters

Message |  Elements for System 0002 1-P0002 02042015 145735 2.kbk (580 B)

Dear Customer,

Thank you and congratulations on purchasing a Medeco XT system from Medeco Security Locks, Inc. Since 1968, Medeco has been an innovator in patented locking technologies and key control programs. As always, we pride ourselves on quality and service and the reputation we've developed as a leader in high security solutions.

Attached, please find your Medeco XT system data files. You will need to import the attached codebook file into the Medeco XT software to add these elements to your system and instructions on how to import these files into your system. Please save these files to a secure location.

If you have any questions or if you need technical support, please contact your dealer. Again, thank you for purchasing a Medeco XT system.

Best regards,

The Medeco E-Cylinder Team
Medeco Security Locks, Inc.

Step 2

To add keys into the Medeco XT Web Manager, select the **Administration** link located in the menu in the top, right corner. Then select the **Import Codebooks** link, as shown below.


[Organization](#) | [Operation Logs](#) | [Import Codebooks](#) | [Remote Programmers](#) | [System Setup](#)

Import Codebooks

Codebook File <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload"/>

Select the **Browse** button and select the codebook file (examplefile.kbk) saved to the computer. Then select the **Upload** button.

The key codebook files must be uploaded individually. When a file is successfully uploaded, a message similar to the one shown below will appear near the top of the screen.

 Keys have been successfully imported into the system.

Step 3

By selecting the **Keys** page, a list of the imported keys can be viewed and managed.

Keys

Serial Number	User	Memory Type
000-506-808	Jim Walters	1X
000-544-005	Steve Brown	1X
000-549-496	John Smith	1X
000-642-743	Stephen Smith	2X
000-642-744	Susan Smith	2X

Memory Type - Keys designated with a "2X" Memory Type are extended memory keys that contain twice (2X) the memory size of standard keys (1X).

Assign to Users

Assign

Select the **Keys** tab in the horizontal menu near the top of the page. A list of all the keys that have been imported into the system will appear. If keys do not display in the table, refer to [Importing Keys](#).

To assign a key to a user, expand the [system tree](#) to view the user. Find the key that will be assigned to the user. In the example below, the key with the number 000-506-808 will be assigned to the user Jim Walters.

Once the desired key and user are found, select and hold the key number, and drag and drop it over the user name when the name highlights.

Keys

Enter Search Term...

- XYZ Company
 - Floor 1
 - Floor 2
 - Floor 3
 - 000-506-808
 - John Smith

Show entries

Serial Number	User	Memory Type	
000-506-808		1X	<input type="button" value="Delete"/>
000-544-005	Steve Brown	1X	
000-549-496	John Smith	1X	
000-642-743	Stephen Smith	2X	
000-642-744	Susan Smith	2X	

Showing 1 to 5 of 5 entries

The key assignment can be viewed in the Tree and on the Keys table.

Keys

Enter Search Term...

- XYZ Company
 - Floor 1
 - Floor 2
 - Floor 3
 - 000-506-808
 - John Smith

Show entries

Serial Number	User	Memory Type	
000-506-808	Jim Walters	1X	
000-544-005	Steve Brown	1X	
000-549-496	John Smith	1X	
000-642-743	Stephen Smith	2X	
000-642-744	Susan Smith	2X	

Showing 1 to 5 of 5 entries

Assigning Multiple Keys to a User

Note: A user can only have one key assigned. That is, a user and key assignment are a one-to-one relationship (1 user to 1 key). If more than one key is desired to be assigned to a user, then the user needs to be created for each additional key assignment. Please

note that when [creating the user](#), the login credentials must be uniquely defined. As an example, Jim Walters can be assigned key 000-506-808 and key 000-642-743 by creating the user Jim Walter twice noting that the login credentials are uniquely defined.

Users with more than one key assigned will display on the Schedule Table as respective rows.

Unassign

To unassign a key from a user, expand the node beside the user name in the tree to view the serial number of the currently assigned key. Right click the key number that appears under the user name, and select *Unassign* in the box that will appear below the key serial number. When the key is unassigned from the user, the name of the user will also be removed on the **Keys** table.

A key can also be unassigned by moving the key to another available user. When a key is not assigned to a user, it is then visible at the global or highest [group](#) level.

Serial Number	User	Memory Type
000-506-808	Jim Walters	1X
000-544-005	Steve Brown	1X
000-549-496	John Smith	1X
000-642-743	Stephen Smith	2X
000-642-744	Susan Smith	2X

Unassigning Keys and Active Key Schedules

Note: Keys cannot be unassigned from a User if the key is currently associated with an [active](#) key schedule. If so, the key schedule must first be [disabled](#) from the Schedule page before the key can be unassigned.

Key Audit Setting

Introduction

To effectively manage the available capacity of the key memory and the audit being recorded, the key audit memory can be configured to function in two different modes; a "Static Audit" mode or a "Rolling Audit" mode. More information on the description and selection of these specific key audit modes is presented below.

The audit mode of the Key is configured during the process of creating a [Schedule](#) for the key.

Static Audit

In the **Static Audit Mode**, the key will record audit events each time the key touches a cylinder. When the audit memory of the key is filled, the key will become disabled until the key is again serviced (refreshed). During servicing of the key, the audit is transferred from the key's memory to the database, and the key once again becomes active. The primary consideration in using a key configured in a Static Audit mode is that all audit

recorded by the key will be "forced" back into the software database during the required servicing of the key. This process should be considered when maintaining a full and accurate historical perspective of the system is desired.

Rolling Audit

In the **Rolling Audit** Mode, the Key will manage audit events on a First-In-First-Out (F-I-F-O) basis. When the audit memory of the key is filled, the key will continue to function by actively managing the filled memory condition by "rolling" out the first recorded audit event (oldest event recorded on the key) and recording or storing the most recent audit event. The primary consideration in using a key configured in a Rolling Audit mode is that only the audit events that are stored on the key at the time of servicing will be transferred back to the software database. If the key has exercised a F-I-F-O condition (meaning that the key memory has filled), then some audits may have been processed off the key prior to the key being serviced. As a result, any audit removed from the key based on the F-I-F-O condition will not be transferred to the software database and, therefore, will not be historically retained. However, keys having the Rolling Audit mode selected at time of servicing will never need to be serviced based on the audit memory being filled.

Key Generations, Key Types, and Special Regulatory Compliances

Key Generations

The following summarizes the various generations of the Medeco XT keys.

- Generation 1 (G1) – Standard memory size (1X). This generation key is no longer available.
- Generation 2 (G2) – Expanded memory size (2X).
- Generation 3 (G3S) - Enhanced to allow for new features and increased performance. Target release date Q4 2016.
- Generation 3 (G3B) - Includes all features of G3 with added Bluetooth capability. Target release date Q4 2016.

Key Types

A Medeco XT key can be serviced to unlock cylinders, audit cylinders, remove and install cylinders, or load blacklists onto cylinders. These include the following different key types:

Operator Key – standard key used for unlocking cylinders. The Operator key is serviced with a key schedule containing a list of cylinders associated with the access points (doors, gates, machines, etc.) and with an authorized time duration of the schedule. The Operator key also records an audit for every authorized or unauthorized attempt to open a cylinder. During opening of a cylinder, the Operator key will retrieve from the cylinder the last three most recent unauthorized key opening attempts that the cylinder has stored.

Audit Key – key used for collecting audits from cylinders. The Audit key is serviced with a key schedule containing only the authorized time duration of the schedule. The Audit key can retrieve audit from any cylinder in the system. When creating a schedule for an audit key, the amount of audits to be retrieved from each cylinder is selectable, from 1, to a maximum of 2751. Audit keys do not open cylinders. Audit keys are serviced using the **Static Audit** mode by default. The **Rolling Audit** option does not apply to Audit keys.

Operator Plus Audit Key – This key type allows users to access openings in your system. Key and cylinder activity is logged and will be uploaded to the system when serviced.

Setup Key – key used to load blacklists into cylinders. The Setup key is serviced with a key schedule containing a list of the cylinders to receive the key blacklist, the authorized time duration of the schedule, and a list of keys to be blacklisted. When the Setup key contacts the cylinder, the cylinder stores the key blacklist. The term "blacklist" pertains to a list of keys (active or inactive) whose access will be overridden or blocked by the cylinder. An example of when to consider a key for blacklisting is if a key is lost or stolen. Setup keys do not open cylinders. Setup keys are serviced using the **Static Audit** mode by default. The **Rolling Audit** option does not apply to Setup keys.

Control Key – is a special-use key to install and remove Small Format Interchangeable Core (SFIC) cylinders. This key type is only needed for systems containing Medeco's Medeco XT SFIC cylinders. The Control key is serviced with a key schedule containing a list of cylinders (to be installed or removed) and with an authorized time duration of the schedule. Additional details on the function of the Control key for managing SFIC cylinders (installing and removing the core) can be obtained by contacting Medeco Technical Services. Control keys are serviced using the **Static Audit** mode by default. The **Rolling Audit** option does not apply to Control keys.

A Note on Regulatory Compliances, Generation 3 Keys with Bluetooth Capability (G3B)

Contains:

FCC ID: VR3-20736

IC: 7465A-20736

HVIN: EA-020736

BLE 20736S module over which Medeco retains control of the final installation.

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. this device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

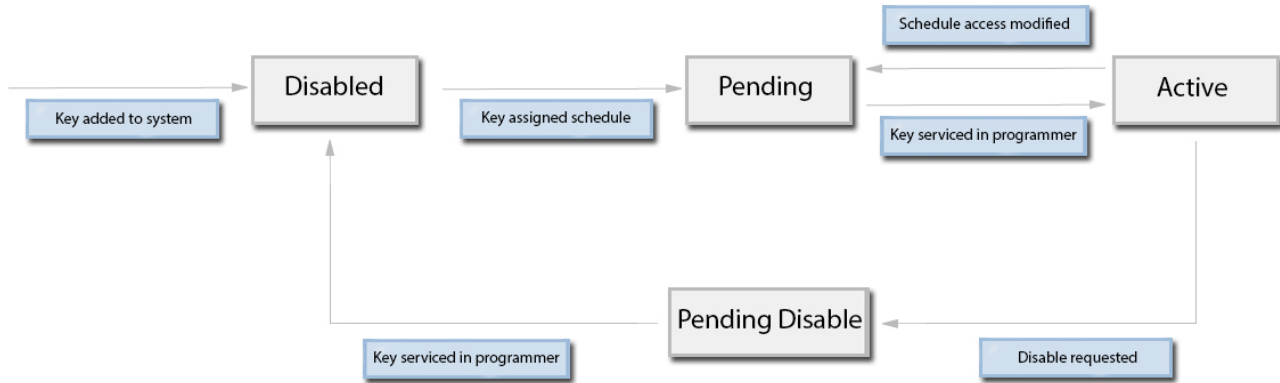
This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement

Key Status

Introduction

A key can be in a state of **Active**, **Pending**, **Pending Disabled**, or **Disabled**. When the key is initially imported into the system, it is placed in a "Disabled" state. This state persists until a key is assigned to a user. If any changes are made to the key schedule, the key will change to a "Pending" status until the change is transferred to the key hardware by physically servicing it. When a key is serviced with a Pending status, the status of the key will change to "Active". A key can be disabled by selecting "Disable" on the Schedules page and then by physically servicing the key. If a key cannot be physically serviced because it is lost or stolen, and it needs to be disabled, the "Force Disable" option can be used. See the flow chart below for additional info:







Key LED Indications

Key LED Indications

The Medeco XT Key contains both a red and green LED indicator for providing status or feedback to the key holder with regard to key activity or operations. The keys provide indications during both key servicing and during key operation with the Medeco XT Cylinder. The LED indications are briefly summarized below.

Key LED Indications During Typical Servicing



When the key is being serviced, the following LED indications apply and are listed in the general order in which they appear:




Event Description	Green LED	Red LED	Notes	Key Client Indication
Audit being processed from the key	On	On	Occurs during typical key servicing	 Processing Audits
Key receiving schedule	On	On	Occurs during typical key servicing	 Receiving Schedule
Key servicing successful	On	Off	On until Key removed from Programmer	 Programming Complete
Key servicing unsuccessful	Off	On	On until Key removed from Programmer	 Programming Complete

Key LED Indications During Servicing with Key Firmware Update

From time to time, the "firmware" (or software) that is currently installed or residing on Medeco XT keys may be updated to support new Medeco XT Web Manager software features or enhancements. When the key's firmware is updated, the update will occur during normal key servicing.

When the key is being serviced and the firmware update is being performed, the following LED indications apply and are listed in the general order in which they appear:

Event Description	Green LED	Red LED	Notes	Key Client Indication
Audit being processed from the key	On	On	Occurs during typical key servicing	 Processing Audits
Key firmware update in progress	On	On	A progress bar will appear to show status	
Key initializing firmware update	Flashing	Off	Key is finalizing the Firmware Update	None

Key receiving schedule	On	On	Occurs during typical key servicing	 Receiving Schedule
Key servicing successful	On	Off	On until Key removed from Programmer	 Programming Complete
Key servicing unsuccessful	Off	On	On until Key removed from Programmer	 Programming Complete

Key LED Indications During Cylinder Operations

When the key is in a cylinder, the following LED indications apply:

Event Description	Green LED	Red LED	Notes
Authorized Opening	On	Off	Occurs during the opening of a cylinder
Unauthorized Opening	Off	On	Occurs during the unauthorized access of a cylinder
Retrieving Cylinder Audit	Flashing	Off	Occurs when the key is in the cylinder and retrieving Audit.
Low Battery	Quick Flash	Quick Flash	The LED will flash Green and Red for 1/20th of a second
Dead Battery	Off	Off	When the battery is dead, no LEDs display

Key LED Indications when Charging

When the key is in a programming station, or a charging station the following LED indications apply:

Event Description	Green LED	Red LED	Notes
Charging in Progress		Slow Flashing	When the key is charging in a programming station, the light on the programming station will flash red. When the key is charging in a charging station, the key's LED will flash red.
Charging Complete	Slow Flashing		When the key is fully charged in a programming station, the light on the programming station will flash green. When the key is fully charged in a charging station, the key's LED will flash green.

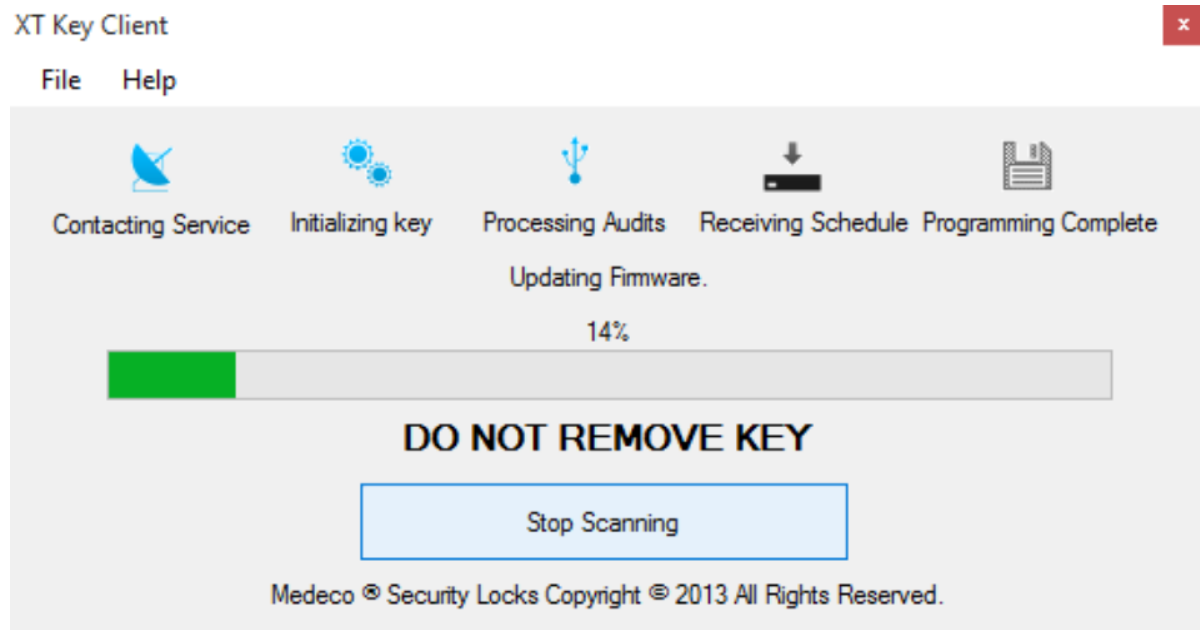
Key Firmware Update Feature

From time to time, the "firmware" (or software) that is currently installed or residing on Medeco XT keys may be updated to support new Medeco XT Web Manager software features or enhancements. The key firmware update process is governed by the Key Client application and is designed to occur during normal key servicing.

The following steps outline the key firmware update process:

1. The keyholder returns their key to the Key Programmer for routine schedule updating.
2. The keyholder inserts the key into the key Programmer.
3. The Key Client begins the typical process to service the key.
 - a. The key is Initialized
 - b. Audits are removed from the key and stored in the database
4. At this point, the Key Client application will interrupt the routine scheduling process to download the file containing the new firmware to the key.
 - a. The Key Client begins to download the new firmware file to the key.

During the entire time that the firmware file is downloaded to the key, the Client application will display a progress bar indicating the % complete. Typically this process takes approximately 50-60 seconds.



1. After the file is successfully downloaded to the key, the key will retrieve the file and complete the firmware installation.
2. When the firmware installation is complete, a message will display to remove the key and reinsert the Key. The Key Client will complete the final steps of the routine scheduling process.

Key Firmware Update

As is typical during key servicing, the key should not be removed from the Key Programmer until a successful Green LED or Red LED is illuminated on the key. For more information, please refer to the section, [Key LED Indications](#).