Genetec Security Center
Mobile 2.1
Installation and User Guide

Click here for the most recent version of this document.
Contents

Preface ........................................................................................................................................... v
  Who should read this guide ........................................................................................................... vi
  What's in this guide ....................................................................................................................... vi
  Terminology used in this guide ..................................................................................................... vii
  Where to find more information .................................................................................................. vii
  About Security Center documentation ......................................................................................... vii
  Additional information ................................................................................................................ viii
  How to provide feedback ............................................................................................................... viii
  Contacting Genetec Technical Assistance ................................................................................... ix

Chapter 1: Introducing Security Center Mobile

About Security Center Mobile ....................................................................................................... 2
  Security Center Mobile architecture ............................................................................................... 2
  Security Center Mobile features .................................................................................................... 3

Security Center Mobile 2.1 Release Notes .................................................................................. 5
  What's new in Security Center Mobile 2.1 ..................................................................................... 5
  Supported mobile devices ............................................................................................................. 6
    Apple Multi-Touch devices ....................................................................................................... 6
    BlackBerry devices ................................................................................................................... 6
    Android devices ........................................................................................................................ 6
  Supported web browsers ............................................................................................................. 7
  Scalability .................................................................................................................................... 7
  Security Center requirements ....................................................................................................... 7
  Security Center interoperability .................................................................................................... 8
  Omnicast Federation requirements ............................................................................................... 8
  Security Center Mobile Client/Server compatibility ................................................................... 8
  Security Center Mobile Server hardware requirements ............................................................... 9
  Security Center Mobile Server software requirements .............................................................. 9
  About the Genetec feedback server ............................................................................................. 9
  Known limitations ....................................................................................................................... 10
Chapter 2: Installing Security Center Mobile Server

Before you install

- Review the Release Notes
- Configure Users and User Groups in Security Center
- Install Omnicast compatibility packages
- Configure ports on Security Center Mobile Server and firewall

Install Security Center Mobile Server

Upgrade Security Center Mobile Server

Chapter 3: Configuring Security Center Mobile Server

Initial configuration

About Security Center Mobile Admin Tool

- Log on to the Security Center Mobile Admin Tool
- Log off the Security Center Mobile Admin Tool
- View Security Center Mobile Admin Tool home page

Viewing license details

Configuring the Security Center Mobile Server

- Configure connection settings to Security Center
- Configure Security Center Mobile Admin Tool SSL certificates
- Configure Security Center Mobile Admin Tool settings
- Configure Security Center Mobile Client connections
- Configure BlackBerry OTA and push notifications
- Configure Apple push notifications
- Configure Android OTA and push notifications

Monitoring the Security Center Mobile System

- Open Security Center Mobile Admin Tool Monitoring pages
- About monitoring sessions
- About monitoring video
- About monitoring doors
Chapter 4: Installing Security Center Mobile Client

Before you install
- Review the Release Notes
- Prerequisites for BlackBerry devices
- Prerequisites for Apple Multi-Touch devices
- Prerequisites for Android devices
- Prerequisites for firewall

Install Security Center Mobile Client on a Blackberry
- Install Security Center Mobile Client from BlackBerry App World
- Install Security Center Mobile Client using BlackBerry Desktop Manager
- Install Security Center Mobile Client using OTA deployment

Install Security Center Mobile Client on Apple mobile devices

Install Security Center Mobile Client on Android devices
- Install Security Center Mobile Client from Android Market
- Install Security Center Mobile Client using OTA deployment

Chapter 5: Using Security Center Mobile Client

Security Center Mobile Client Basics
- About Security Center Mobile Client
- About Security Center Mobile Client application icons
- Open Security Center Mobile Client
- Configure Security Center Mobile Client options
- Log on to Security Center Mobile Client
- Use the same mobile device on a different server
- Log off Security Center Mobile Client

Viewing video
- Browse and select cameras
- Using the camera controls

Viewing doors
- Browse and select doors
- Viewing door events
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using door controls</td>
<td>62</td>
</tr>
<tr>
<td>Viewing alarms</td>
<td>65</td>
</tr>
<tr>
<td>About alarm notifications</td>
<td>65</td>
</tr>
<tr>
<td>View an alarm</td>
<td>66</td>
</tr>
<tr>
<td>Turn alarms on and off</td>
<td>68</td>
</tr>
<tr>
<td>Using Favorites</td>
<td>69</td>
</tr>
<tr>
<td>Add an entity to Favorites</td>
<td>69</td>
</tr>
<tr>
<td>Delete an entity from Favorites</td>
<td>69</td>
</tr>
<tr>
<td>Searching for specific entities</td>
<td>70</td>
</tr>
<tr>
<td>About searching</td>
<td>70</td>
</tr>
<tr>
<td>Search for entities on Apple devices</td>
<td>70</td>
</tr>
<tr>
<td>Search for entities on BlackBerry devices</td>
<td>71</td>
</tr>
<tr>
<td>Search for entities on Android devices</td>
<td>71</td>
</tr>
</tbody>
</table>
Preface

This section includes the following topics:

- "Who should read this guide" on page vi
- "What’s in this guide" on page vi
- "Terminology used in this guide" on page vii
- "Where to find more information" on page vii
- "How to provide feedback" on page viii
- "Contacting Genetec Technical Assistance" on page ix
Who should read this guide

This guide is for two types of readers: system administrators and Genetec Security Center Mobile users.

- **System administrators.** People responsible for deploying and supporting Security Center Mobile in their enterprise environment. This guide assumes the system administrator has the following:
  - Basic understanding of network and system administration.
  - Working knowledge of BlackBerry Enterprise Server administration.
  - Working knowledge of Apple iTunes and a basic understanding of the Apple Push Notification Service.
  - Working knowledge of Google Android Market and Google Cloud to Device Messaging service.
- **Security Center Mobile users.** People who will use the Security Center Mobile Client on their mobile device.

What's in this guide

This guide is organized as follows:

- **Chapter 1, “Introducing Security Center Mobile”.** This section describes the main functionalities of Security Center Mobile. It also includes the Security Center Mobile release notes.
- **Chapter 2, “Installing Security Center Mobile Server”.** This section describes the things you need to know and do before you install Security Center Mobile Server.
- **Chapter 3, “Configuring Security Center Mobile Server”.** This section explains how to use the Admin Tool to configure the Security Center Mobile Server and monitor Security Center Mobile systems.
- **Chapter 4, “Installing Security Center Mobile Client”.** This section explains how to install the Security Center Mobile Client on the Apple Multi-Touch devices (iPhone, iPod, iPad), BlackBerry devices, and Android devices.
- **Chapter 5, “Using Security Center Mobile Client”.** This section explains how to use the main features of Security Center Mobile Client.
Terminology used in this guide

This guide uses the following terminology:

- Apple Multi-Touch devices. iPad, iPhone, and iPod touch mobile devices.
- APNS. Apple Push Notification Service.
- BES. Blackberry Enterprise Server.
- OTA deployment. Over the Air deployment.
- C2DM. Cloud to Device Messaging.

Where to find more information

Security Center includes documentation to help you get started, as well as provides detailed information about the product features. The latest version of the documentation is available from the Genetec Technical Assistance Portal (GTAP).

NOTE You’ll need a username and password to log on to GTAP.

About Security Center documentation

The documentation for Security Center is available on the Security Center DVD in the Documentation folder. Security Center includes the following documentation:

- **Security Center Release Notes.** Describes the release in detail, including new features, fixed issues, and known issues.
- **Security Center Installation and Upgrade Guide.** Describes the prerequisites for installing Security Center and provides instructions for installing and upgrading Security Center on your system.
- **Security Center Administrator Guide.** Provides all the instructions and conceptual information you’ll need to set up, configure, and administer your Security Center system. This guide is also available from the Config Tool online Help.
- **Genetec Security Desk User Guide.** Provides the instructions and conceptual information you need to get started with Security Desk, to monitor and generate reports for AutoVu LPR, Omnicast video surveillance, and Synergis access control systems. This guide is also available from the Security Desk online Help.
- **Security Center Video Unit Preconfiguration Guide.** Provides task-oriented information about how to preconfigure a video unit before integrating it to Security Center.
- **Security Center Portable Archive Player User Guide.** Explains how to use the Portable Archive Player to view exported video files.
Additional information

In addition to the product documentation, you can use the following resources to find out more about Security Center:

- Genetec’s Technical Assistance Portal (GTAP). Provides in-depth support information, including FAQs, knowledge base articles, product forums, as well as product assistance tools for our full suite of IP security solutions. Go to http://gtap.genetec.com/.
- Genetec Solutions Training. In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience and can be customized to meet your specific needs and objectives. Go to http://www.genetec.com/English/Support/Training.

How to provide feedback

Comments, corrections, and suggestions on Genetec documentation can be sent to documentation@genetec.com.

You can also let us know the improvements or related information you would like to see in the guide, by filling out or documentation feedback form at: https://spreadsheets.google.com/viewform?formkey=dDB6X2NYeUFpWJGNDVWnIVa2xPUXc6MQ.
Contacting Genetec Technical Assistance

For more information or support, you can contact Genetec’s Technical Assistance Center (GTAC) in the following ways:

- Genetec’s Technical Assistance Portal (GTAP): For in-depth product technical information and assistance, customers can log in to the portal at http://gtap.genetec.com.
- GTAP Forum: https://gtapforum.genetec.com
- Telephone: 1-514-856-7100. Toll Free (USA & Canada): 1-866-338-2988, from Monday to Friday, 8:00 AM to 8:00 PM (Eastern time, GMT -5h).
  Europe: +800 01818200 (Please visit gtap.genetec.com for a list of covered territories.)

No matter how you contact us, you’ll need to have all relevant product information available, including System ID and product version. This information is available from the Help menu.
Introducing Security Center Mobile

This section describes the main functionalities of Security Center Mobile. It also includes the Security Center Mobile release notes.

This section includes the following topics:

• "About Security Center Mobile" on page 2
• "Security Center Mobile 2.1 Release Notes" on page 5
About Security Center Mobile

Security Center Mobile is a mobile application that allows you to remotely monitor and control your security system over any wireless IP network.

The client application incorporates the pinch/swipe/touch functionality on Apple, Android, and BlackBerry devices, as well as the iPad’s additional real-estate, to let you easily search for, monitor, and control thousands of cameras and doors. It also uses push technology, letting you receive system alarms, view entities attached to alarms, and acknowledge alarms in the field.

This section includes the following topics:

- "Security Center Mobile architecture" on page 2
- "Security Center Mobile features" on page 3

Security Center Mobile architecture

Security Center Mobile is based on a client/server model that includes the following components:

- **Security Center Mobile Server.** The server application that connects all mobile devices to Genetec Security Center. Once connected to Security Center, Security Center Mobile Server pulls video streams directly from the cameras, transcodes the video to M-JPEG, and then streams the video over the network to Security Center Mobile Clients. Security Center Mobile Server also pushes events and automated alarms to Security Center Mobile Client users through the Apple Push Notification Service (APNS), BlackBerry Enterprise Server (BES), and Google Cloud to Device Messaging service (C2DM).

- **Security Center Mobile Client.** The client application installed on mobile devices. Authorized users use the Security Center Mobile Client to connect to the Security Center Mobile Server to receive alarms, access live video streams, view the status of doors, and more.

- **Security Center Mobile Admin Tool.** The web-based administration tool used to configure, administer, and monitor Security Center Mobile. From the Admin Tool you can
validate the license, configure the connection settings and push notifications, and monitor your Security Center Mobile system.

Security Center Mobile features

Security Center Mobile Application includes the following features:

- Remote monitoring of a Security Center system and Omnicast systems federated to the Security Center system. You can view video from all camera manufacturers and models supported by the Security Center version you are using, and the Omnicast video surveillance system. For a list of major camera manufacturers, see the Genetec web site. (www.genetec.com).
- Remote monitoring of Security Center doors and related events, such as access granted or access denied. You can lock/unlock doors remotely, override lock/unlock schedules, and view live video from cameras associated with doors.
- Receive, view, and acknowledge Security Center alarms, including access control and video alarms.
- User authentication and password protection, as well as encrypted communication between the Security Center Mobile Client and the Security Center Mobile Server.
- Support for iPod Touch / iPhone / iPad, BlackBerry mobile devices, and Google Android mobile devices.
- Send multiple video streams to several mobile devices at the same time.
• You can view one video stream on iPhone, iPod touch, Blackberry, and Android devices, and up to six video streams at the same time on an iPad.
• PTZ camera control including access to PTZ presets.
• Save snapshots for later viewing. Take a snapshot from a live video camera and save it to photo library on the smart phone.
Security Center Mobile 2.1 Release Notes

This section describes the supported devices, system requirements and known issues in Security Center Mobile 2.1.

This section includes the following topics:
- "What's new in Security Center Mobile 2.1" on page 5
- "Supported mobile devices" on page 6
- "Supported web browsers" on page 7
- "Scalability" on page 7
- "Security Center requirements" on page 7
- "Security Center interoperability" on page 8
- "Omnicast Federation requirements" on page 8
- "Security Center Mobile Client/Server compatibility" on page 8
- "Security Center Mobile Server hardware requirements" on page 9
- "Security Center Mobile Server software requirements" on page 9
- "About the Genetec feedback server" on page 9
- "Known limitations" on page 10
- "Known issues" on page 10
- "Resolved issues" on page 10

What's new in Security Center Mobile 2.1

Security Center Mobile 2.1 introduces the following new features and enhancements:

- **Security Center 5.0 SR1 and later support.** Security Center Mobile now supports Security Center 5.0 SR1 and later, which allows you to view video natively from Security Center. Viewing video through an Omnicast Federation is still supported, but is no longer required to view video.

- **Google Android support.** Security Center Mobile is now available on mobile devices that support the Google Android operating system, such as the Samsung Captivate smartphone, and Samsung Galaxy Tab.

- **Easier client download.** You can download the Security Center Mobile Client from Apple iTunes, BlackBerry App World, and Android Market. You can also use OTA (over the air) deployment to install the mobile client on Android devices.
Supported mobile devices

This release supports the following mobile devices.

- "Apple Multi-Touch devices" on page 6
- "BlackBerry devices" on page 6
- "Android devices" on page 6

Apple Multi-Touch devices

This release supports the following Apple Multi-Touch devices:

<table>
<thead>
<tr>
<th>Device</th>
<th>Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone</td>
<td>3G and later, iOS 3.1.2 and later.</td>
</tr>
<tr>
<td>iPod Touch</td>
<td>2nd generation and later, iOS 3.1.2 and later.</td>
</tr>
<tr>
<td>iPad</td>
<td>WiFi and WiFi + 3G, iOS 3.2 and later.</td>
</tr>
</tbody>
</table>

BlackBerry devices

This release supports the following BlackBerry mobile devices:

<table>
<thead>
<tr>
<th>Device</th>
<th>Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>9000, 9600, 9700, OS 4.6.1 and later</td>
</tr>
<tr>
<td>Curve</td>
<td>8530, 8900, 3G, OS 4.6.1 and later</td>
</tr>
<tr>
<td>Storm</td>
<td>1 and 2, OS 4.6.1 and later</td>
</tr>
<tr>
<td>Torch</td>
<td>9630, OS 4.6.1 and later</td>
</tr>
</tbody>
</table>

Android devices

This release supports the following versions of the Google Android operating system:

- Version 2.0 and later (minimum to view video, door events, etc)
- Version 2.2 and later (to receive push alarm notifications)

**NOTE** Please note the following:

- Genetec tested and documented Android functionality for Security Center Mobile based on the following Android devices: the Samsung Captivate smartphone, and Samsung Galaxy Tab. The basics of using other Android devices may slightly differ from those described in this guide, so best practice is to have your device's documentation on hand as a reference.
- The minimum recommended resolution for Android devices is 320 x 480.
Supported web browsers

In this release, Security Center Mobile Admin Tool is supported by the following web browsers:

- IE 7 and later
- Mozilla Firefox
- Chrome
- Opera
- Safari (desktop and mobile versions)
- BlackBerry browser
- Android browser

Scalability

Security Center Mobile can scale to the following specifications per Security Center Mobile Server.

Best practice: To achieve maximum scalability, use the highest-end server listed in "Security Center Mobile Server hardware requirements" on page 9.

**NOTE** To increase system scalability, add additional Security Center Mobile Servers.

- Maximum 50 different Security Center Mobile user accounts can be logged on to a Security Center Mobile Server at the same time.
- Maximum 50 different cameras can be monitored at the same time.
- A single user can log on using 300 different mobile devices.

Security Center requirements

To use Security Center Mobile 2.1:

- You must be connected to Security Center 5.0 SR1 or later.
- If connecting to Security Center 5.1 GA, then Hotfix 63615 or later must be installed on the computer hosting the Security Center server that Security Center Mobile Server connects to.

**NOTE** Security Center Mobile supports Security Center 4.0 systems if you federate those systems to the Security Center 5.0 SR1 or later. For more information about Security Center Federation, see the *Security Center 5.0 Administrator Guide*. 
Security Center interoperability

Security Center Mobile Server interoperates with Security Center as follows:

- If the server is streaming more than 10 cameras at the same time, it is best practice to install Security Center Mobile Server on a different computer than Security Center.
- If the server is streaming less than 10 cameras at the same time, you can install Security Center Mobile Server on the same computer as Security Center, but the computer must meet the high-end hardware requirements for Security Center Mobile Server. For more information, see "Security Center Mobile Server hardware requirements" on page 9.

Omnicast Federation requirements

In Security Center 5.0 SR1 and later, Omnicast Federation is no longer a prerequisite for viewing video. Video is available natively from Security Center. However, to view video from a federated Omnicast system, your Omnicast system must meet the following requirements:

- The federated Omnicast system must be version 4.4 or later.
- You must install the compatibility package for each version of Omnicast federated to Security Center on the Security Center Mobile Server computer. For more information, see "Install Omnicast compatibility packages" on page 13.

Security Center Mobile Client/Server compatibility

All versions of Security Center Mobile Client and Server are backward and forward compatible. This means that you can use any version of the client with any version of the server.

The only exception is if you want to use Android push notifications. In this case, you’ll need to install version 2.1 of both Security Center Mobile Client and Security Center Mobile Server.
Security Center Mobile Server hardware requirements

Security Center Mobile Server computer requirements depends on the number of cameras and mobile devices in your Security Center Mobile system.

<table>
<thead>
<tr>
<th>If your system includes:</th>
<th>Server requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 cameras streaming to 10 mobile devices, or six cameras streaming to 60 mobile devices.</td>
<td>Intel Core 2 Duo 3.0 GHz 2 GB RAM</td>
</tr>
<tr>
<td>30 cameras streaming to 30 mobile devices, or 18 cameras streaming to 180 mobile devices.</td>
<td>Quad Core Intel Xeon 2.13 GHz 4 GB RAM</td>
</tr>
<tr>
<td>50 cameras streaming to 50 mobile devices, or 30 cameras streaming to 300 devices.</td>
<td>2 Processors Quad Core Intel Xeon 2.5 GHz 4 GB RAM</td>
</tr>
</tbody>
</table>

Security Center Mobile Server software requirements

Security Center Mobile Server is supported on the following operating systems:

- Microsoft® Windows 7 Professional and Ultimate 32-bit/64-bit
- Microsoft® Windows XP Pro SP3 32-bit/64-bit
- Microsoft® Windows Vista SP1 Business and Ultimate 32-bit/64-bit
- Microsoft® Windows Server® 2003 Enterprise Edition SP1/SP2/R2 32-bit/64-bit
- Microsoft® Windows Server® 2008 Enterprise Edition SP2/R2 32-bit/64-bit

About the Genetec feedback server

Genetec must comply with a set of mandatory requirements and guidelines established by Apple Inc. (“Apple”) to allow Security Center Mobile to send push notifications through the Apple Push Notification Service (APNs). Apple's requirements state that Genetec must maintain a centralized feedback server for all Security Center mobile servers that are installed throughout the world.

If you want to receive push notifications from Security Center Mobile, all of your Security Center mobile servers in operation must connect to the Genetec feedback server in order to exchange the Security Center System ID and device token IDs.

You don't need to install or configure the Genetec feedback server, but you should verify that it is running using the Security Center Mobile Admin Tool. For more information, see "Configure Apple push notifications" on page 31.
Known limitations

Security Center Mobile 2.1 includes the following known limitations.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27142</td>
<td>In the list of entities on your mobile device, federated Omnicast entities always appear online (in black), even if they are offline. Other entities (doors, areas, cameras) appear in red when they are offline. To verify that your Omnicast Federation is working, try to view its associated video feed. If you can’t view the video feed, the Federation may need to be reestablished.</td>
</tr>
<tr>
<td>26245</td>
<td>There is a difference between the way entities are displayed in Security Desk and Security Center Mobile Client for users that do not have the required Security Center privilege to view the entities. In Security Center Mobile Client, entities are only visible if the user has the proper Security Center privilege to view them. The only exception is for areas in the root entities list. These areas are always visible, but their contents are hidden.</td>
</tr>
<tr>
<td>26249</td>
<td>When a “invalid credential” event is received, the mobile client does not automatically switch to the video feed on the side of the door where the event occurred. You’ll need to manually select the camera on that side of the door to view the video feed.</td>
</tr>
<tr>
<td>23796</td>
<td>There is a difference between the way door events are displayed in Security Desk and Security Center Mobile Client. In Security Center Mobile Client, when a cardholder is granted or denied access to a door, the cardholder’s picture is only displayed if the user monitoring the door has the Security Center privileges to view cardholders and visitors. If the user does not have the proper privileges, only the door event is displayed (access granted or access denied).</td>
</tr>
<tr>
<td>37010</td>
<td>When you perform a PTZ camera operation in the Security Center Mobile Client, that camera appears in Security Desk as being locked by an administrator, even if you are not logged on to the mobile client as an administrator.</td>
</tr>
<tr>
<td>37012</td>
<td>If you move an entity that was originally created within a non-visible area to a visible area, the entity will not appear in your mobile client’s entities list, even after you refresh the list. To view the entity, you need to log off the mobile client and then log back on.</td>
</tr>
</tbody>
</table>

Known issues

Security Center Mobile 2.1 does not include any known issues.

Resolved issues

Security Center Mobile 2.1 does not include any resolved issues.
Installing Security Center Mobile Server

This section explains how to install and upgrade Security Center Mobile Server.

This section includes the following topics:

- "Before you install" on page 12
- "Install Security Center Mobile Server" on page 16
- "Upgrade Security Center Mobile Server" on page 17
Before you install

This section describes the things you need to know and do before you install Security Center Mobile Server.

This section includes the following topics:

- "Review the Release Notes" on page 12
- "Configure Users and User Groups in Security Center" on page 12
- "Install Omnicast compatibility packages" on page 13
- "Configure ports on Security Center Mobile Server and firewall" on page 14

Review the Release Notes

Read the "Security Center Mobile 2.1 Release Notes" on page 5 for any known issues and other information about this release.

Configure Users and User Groups in Security Center

In order to connect to Security Center, Security Center Mobile users must belong to a Security Center user group that is assigned specific user rights.

Best practice:

- In Security Center, create a separate user group for Security Center Mobile users.
- If using the video streaming feature only (without alarm notifications), then create one user account for all users. For example, you could create a user account called "Mobile Video" that all your users can connect to.

For more information about users and user groups in Security Center, see the Security Center Administrator Guide.

The following table shows the mandatory and optional Security Center user rights that are required to perform various Security Center Mobile tasks.

<table>
<thead>
<tr>
<th>Security Center Mobile Tasks</th>
<th>Mandatory User Rights</th>
<th>Optional User Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum required for all Security</td>
<td>• SDK Log on using the SDK</td>
<td>• N/A</td>
</tr>
<tr>
<td>Center Mobile users</td>
<td>• View areas</td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>• Alarm monitoring</td>
<td>• Acknowledge alarms</td>
</tr>
<tr>
<td></td>
<td>• View alarms</td>
<td></td>
</tr>
<tr>
<td>Video</td>
<td>• View cameras</td>
<td>• PTZ motor privileges</td>
</tr>
<tr>
<td></td>
<td>• View live video</td>
<td></td>
</tr>
</tbody>
</table>
Install Omnicast compatibility packages

Before installing Security Center Mobile Server, you need to install the Omnicast compatibility packages on your Security Center Mobile Server computer. You must install at least one compatibility pack, and additional compatibility packs for each version of Omnicast federated to Security Center. Compatibility packs are available in the Security Center Mobile installation package.

**IMPORTANT**
- Do not install the compatibility packs from the Security Center package.
- **Omnicast 4.8 federations.** To view video from Omnicast 4.8 systems, Mobile Server requires Omnicast compatibility packs 4.7 and 4.8. First install the Omnicast 4.7 compatibility pack, and then the Omnicast 4.8 compatibility pack. The Omnicast 4.8 compatibility pack is available for download from the GTAP Product download page, at https://gtap.genetec.com.

1. If required, uninstall all earlier versions of the Omnicast compatibility packages running on the Security Center Mobile Server computer.
2. Navigate to the Security Center Mobile installation package, and double-click setup.
3. In the Security Center Mobile Installation splash page, click Compatibility packs.
4. In the Compatibility Packs folder, open the folder that corresponds to the required compatibility pack.
5. Double-click setup.exe and follow the installer instructions.
Installing Security Center Mobile Server | Before you install

Configure ports on Security Center Mobile Server and firewall

The following diagram shows the port connections that you’ll need to configure to use the Security Center Mobile system. Refer to the following table for configuration information.

<table>
<thead>
<tr>
<th>Item</th>
<th>Port Information</th>
</tr>
</thead>
</table>
| A    | Connection is HTTP or HTTPS.  
To connect Security Center Mobile Client to Security Center Mobile Server, open the following ports on the company firewall:  
- **Main port**: HTTP (default port is 8100) or HTTPS (default port is 443).  
- **Video port**: HTTP (default port is 8101).  
- **BlackBerry OTA deployment**: HTTP or HTTPS (default port is 80). |
| B    | Connection is HTTP or HTTPS.  
To use Security Center Mobile Admin Tool outside the LAN, open the following server administration ports:  
- **HTTP protocol**: (default port 80).  
- **HTTPS protocol**: (default port 443). |
| C    | Security Center 5.0 SDK connection. Default port is TCP 5500. |
### Port Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Video streaming connection is TCP-UDP-Multicast.</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>Video streaming connection is TCP-UDP-Multicast.</td>
</tr>
<tr>
<td>F</td>
<td>Video streaming connection is TCP-UDP-Multicast.</td>
</tr>
<tr>
<td>G</td>
<td>Omnicast Compatibility Pack connection. Default port is TCP 5001.</td>
</tr>
<tr>
<td>H</td>
<td>Video streaming connection is TCP-UDP-Multicast.</td>
</tr>
<tr>
<td>I</td>
<td>BlackBerry push notifications. BlackBerry Enterprise Server and Mobile Data Service default port is 8080 (HTTP or HTTPS).</td>
</tr>
<tr>
<td>J</td>
<td>Android push notifications (HTTPS connection). If using the mobile device over a WiFi connection, open port 5228 inbound (TCP) on the company firewall.</td>
</tr>
<tr>
<td>K</td>
<td>Apple push notifications. Open port 2195 outbound (TCP) so that the Security Center Mobile Server can communicate with gateway.push.apple.com to send push notifications on that port. If using the mobile device over a WiFi connection, open port 5223 inbound (TCP) on the company firewall.</td>
</tr>
</tbody>
</table>

1. HTTPS not supported for video data.
2. When using HTTPS on the Security Center Mobile Admin Tool port, you need to install an SSL certificate, and use the SSL certificates page of the Admin Tool to bind the SSL certificate to the IP port.
Install Security Center Mobile Server

If you are installing Security Center Mobile Server on a machine that does not have a previous version already installed, follow the steps provided in this section.

**IMPORTANT** It is recommended that you always install Security Center Mobile Server on a different computer than Security Center. For more information about installing Security Center Mobile Server and Security Center on the same computer, see "Security Center interoperability" on page 8.

Before you begin: read "Before you install" on page 12.

1. Install Omnicast compatibility packages. See "Install Omnicast compatibility packages" on page 13.
2. Navigate to the Security Center Mobile installation package, and double-click setup.exe.
3. In the Security Center Mobile Installation splash page, click GSC Mobile Server.
4. Follow the installer instructions.
5. In the Server Admin Tool Parameters page, you can choose the HTTP port for the Security Center Mobile Admin Tool, and click Next.
   The default is 80.
6. When the installation is complete, click Finish.

After you are done: See "About Security Center Mobile Admin Tool" on page 21.
Upgrade Security Center Mobile Server

If you are upgrading Security Center Mobile Server from a previous version, you don't need to uninstall the earlier version before installing the new one.

**IMPORTANT** It is highly recommended that you always install Security Center Mobile Server on a different computer than Security Center. If you want to install them both on the same computer, refer to "Security Center interoperability" on page 8 for more information.

1. **Stop the Security Center Mobile Server service.**
   From your Windows Control Panel, click Administrative Tools > Services, and then stop the Genetec Security Center Mobile Server service.

2. **Uninstall all earlier versions of the Omnicast compatibility packages.**

3. **Install Omnicast compatibility packages.** See "Install Omnicast compatibility packages" on page 13.
   **IMPORTANT** If you are federating Omnicast 4.8 to Security Center, you need to install compatibility packs 4.7 and 4.8.

4. **Install Security Center Mobile Server.**
   See "Install Security Center Mobile Server" on page 16.

**After you are done:** See "About Security Center Mobile Admin Tool" on page 21.
Configuring Security Center Mobile Server

This section explains how to use the Admin Tool to configure the Security Center Mobile Server and monitor Security Center Mobile systems.

This section includes the following topics:

- "Initial configuration" on page 20
- "About Security Center Mobile Admin Tool" on page 21
- "Configuring the Security Center Mobile Server" on page 24
- "Monitoring the Security Center Mobile System" on page 35
Initial configuration

This section lists the steps required to set up the Security Center Mobile Server for the first time using the Security Center Mobile Admin Tool.

Before you begin: This section assumes you have already installed Security Center Mobile Server. For more information on installing the server, see Chapter 2, "Installing Security Center Mobile Server" on page 11.

The initial configuration of Security Center Mobile Server includes the following steps. For more information on the steps in each task, click the link or refer to the page number.

1. "Log on to the Security Center Mobile Admin Tool" on page 22
2. "Configure Security Center Mobile Admin Tool settings" on page 27
3. "Configure connection settings to Security Center" on page 24
4. (Optional) Configure alarm push notifications, see the following:
   - "Configure BlackBerry OTA and push notifications" on page 29
   - "Configure Apple push notifications" on page 31
   - "Configure Android OTA and push notifications" on page 33

After you are done: For more information on how to use the Security Center Mobile Admin Tool, see the sections "Configuring the Security Center Mobile Server" on page 24, and "Monitoring the Security Center Mobile System" on page 35.
The Security Center Mobile Admin Tool is the web-based administration tool used to configure, administer, and monitor Security Center Mobile. From the Admin Tool you can validate the application license, configure the connection settings and push notifications, and monitor your mobile system.

The Security Center Mobile Admin Tool home page displays the configuration settings (license, connection, and system status) of your mobile system. The Overview section displays any warnings or errors with your server, if applicable.

**NOTE** The home page is the only page that is automatically refreshed. All other pages must be refreshed manually for changes to be displayed.

This section includes the following topics:

- "Log on to the Security Center Mobile Admin Tool" on page 22
- "Log off the Security Center Mobile Admin Tool" on page 22
- "View Security Center Mobile Admin Tool home page" on page 22
Log on to the Security Center Mobile Admin Tool
Before you begin: To log on to the Security Center Mobile Admin Tool, you’ll need to know the IP address of the Security Center Mobile Server computer.

1. Open a web-browser, and in the address bar, type one of the following:
   - If you’re logging on to the default port 80 using HTTP, type http://<<Security Center Mobile Server computer IP address or host name>>/GSCMobileAdmin/main.aspx.
   - If you’re logging on to a port other than 80 and/or using HTTPS, type <<http or https>>://<<Security Center Mobile Server computer IP address or host name>>:<<port number>>/GSCMobileAdmin/main.aspx.
   The Security Center Mobile Admin Tool log on page appears.

2. In the log on page, type your username.
   The default is Admin. By default, there is no set password.

3. Click Log on.
   The Security Center Mobile Admin Tool home page appears.

After you are done: Best practice is to change the default password, see “Configure Security Center Mobile Admin Tool settings” on page 27.

Log off the Security Center Mobile Admin Tool
You are automatically logged off Security Center Mobile Admin Tool after 15 minutes of inactivity.

- From the Security Center Mobile Admin Tool, click Log Off on the top right of the window.

View Security Center Mobile Admin Tool home page
To return to the Security Center Mobile Admin Tool home page, click the Security Center Mobile Admin Tool link on the top left of the window.
Viewing license details

You can view information about your license, your system ID, and Genetec Technical Assistance contact information from the License page.

**NOTE** You activate your Security Center Mobile license from the Security Center Server Admin. This page displays the portion of the Security Center license that pertains to Security Center Mobile. For more information on license activation, see the Security Center Administrator Guide.

1. Log on to the Security Center Mobile Admin Tool.
2. On the Security Center Mobile Admin Tool home page, click the Configuration list, and select License. The License page appears.
Configuring the Security Center Mobile Server

This section explains how to configure Security Center Mobile using the Security Center Mobile Admin Tool.

This section includes the following topics:

- "Configure connection settings to Security Center" on page 24
- "Configure Security Center Mobile Admin Tool SSL certificates" on page 25
- "Configure Security Center Mobile Admin Tool settings" on page 27
- "Configure Security Center Mobile Client connections" on page 28
- "Configure BlackBerry OTA and push notifications" on page 29
- "Configure Apple push notifications" on page 31
- "Configure Android OTA and push notifications" on page 33

Configure connection settings to Security Center

You configure the Security Center connection settings in the Security Center Mobile Admin Tool Security Center page.

**NOTE** Security Center Mobile Server can only connect to Security Center through the Security Center Administrator account.

**Before you begin:** You’ll need the Security Center Administrator account and password.

1. Log on to the Security Center Mobile Admin Tool.
2. On the Security Center Mobile Admin Tool home page, click the Configuration list, and select Security Center.
   The Security Center page appears.

3. Configure the following:
• **Directory.** Specify the Security Center Directory IP address or hostname.
• **Password.** Specify the Security Center administrator password.
• **Port.** Specify the port that you want to use to connect to Security Center.
• **State.** Indicates if you are Connected to Security Center.
• **User group (Optional).** Do one of the following:
  • Specify the Security Center user group that includes Security Center Mobile users.
  • Do not specify a user group. When this field is empty all Security Center users can log on from a mobile device.

The State fields indicate if the user group you specified is a valid user group in Security Center.

4. Click **Apply**.

**Configure Security Center Mobile Admin Tool SSL certificates**

You can view the SSL certificates installed on your machine, and bind them to your IP port in the Security Center Mobile Admin Tool SSL certificates page. You must have at least one valid SSL certificate selected to connect to Security Center using the HTTPS protocol.

**NOTE** If you’re using Android OTA deployment with HTTPS, you’ll need to have an authentic SSL certificate, such as from VeriSign, to successfully download the mobile client. Self-signed certificates will not work for OTA deployment over HTTPS. For more information, see “Configure Android OTA and push notifications” on page 33.

1. Log on to the Security Center Mobile Admin Tool.
2. On the Security Center Mobile Admin Tool home page, click the Configuration list, and select **SSL certificates**.

The SSL certificates page appears.
3 From the list of displayed certificates, click Select next to the certificate you want to use. The certificate will be highlighted, and the State field will indicate whether or not the certificate is valid.
   - **Clear selection.** Clears the selected certificate if there are no ports using HTTPS.
   - **Generate test certificate.** Creates an SSL certificate for testing purposes.
     Although this test certificate allows you to connect using HTTPS, it is not a valid SSL certificate, and is only intended for testing your HTTPS connection. When you attempt to log in using this certificate, you will receive the following message:

   ![Certificate Warning Message]

   Click Continue to this website (not recommended) to logon with your test certificate.
   - **Ports.** Indicates which ports are currently using HTTPS.

4 Click Apply.
Configure Security Center Mobile Admin Tool settings

You configure the Security Center Mobile Admin Tool port, user name, and password in the Security Center Mobile Admin Tool Server Administration page.

Before you begin: If using HTTPS, then you need to install an SSL Certificate, and bind the SSL certificate to the IP Ports. For more information, see “Configure Security Center Mobile Admin Tool SSL certificates” on page 25. Contact your system administrator for more information on SSL certificates.

1 Log on to the Security Center Mobile Admin Tool.

2 On the Security Center Mobile Admin Tool home page, click the Configuration list, and select Server Administration.

   The Server Administration page appears.

3 Configure the following:
   - **Port.** Specify the Security Center Mobile Admin Tool port. The default is 80.
   - **Use HTTPS.** Select to encrypt communications between the Security Center Mobile Admin Tool and Security Center Mobile Server.
     **NOTE** The shortcut to the Security Center Mobile Admin Tool in your Windows start menu will not work if you change the default port number or use HTTPS. You’ll need to type the Admin Tool’s URL into your browser manually. For more information, see "Log on to the Security Center Mobile Admin Tool” on page 22.
   - **Username.** Security Center Mobile Admin Tool username.
   - **Change password.** Select if you want to change the logon password.
   - **New password.** Type new password.
   - **Confirm new password.** Retype new password.

4 Click Apply.
Configure Security Center Mobile Client connections

You configure the connection ports between Security Center Mobile Server and Security Center Mobile Clients in the Security Center Mobile Admin Tool Mobile Connectivity page.

1. "Log on to the Security Center Mobile Admin Tool" on page 22.
2. On the Security Center Mobile Admin Tool home page, click the Configuration list, and select Mobile Connectivity.
   The Mobile Connectivity page appears.

3. Configure the port settings for the main communication port between Security Center Mobile Server and Security Center Mobile Clients:
   - **Main port.** Specify the port.
   - **Use HTTPS.** Select to encrypt communications (user information and configuration) between Security Center Mobile Server and Security Center Mobile Clients.
   - **State.** Indicates if the port is open and if it can be used with HTTP (default) or HTTPS.
   - **Test link.** Click to verify that the port is open.

4. Configure the port settings for video streaming from Security Center Mobile Server to Security Center Mobile Clients:
   - **Video port.** Specify the port that will stream video.
   - **Test link.** Click to verify that the port is open.
   - **State.** Indicates if the port is open.
   - **Session timeout (seconds).** Specify how long a user can remain inactive before being logged out of the mobile application.
- **Video streaming timeout (minutes).** Specify how long the mobile application can continuously stream video before being stopped by the server. If you select None, video streaming will continue indefinitely unless stopped by the user, or the mobile device enters "sleep" mode.

5 Click Apply.

**Configure BlackBerry OTA and push notifications**

You configure BlackBerry OTA deployment and the BES push notification ports in the Security Center Mobile Admin Tool BlackBerry page.

1 Log on to the Security Center Mobile Admin Tool.

2 On the Security Center Mobile Admin Tool home page, click the Configuration list, and select BlackBerry.

![Security Center Mobile Admin Tool](image)

3 Configure the BlackBerry OTA settings:

- **Port.** Specify the port for OTA deployment between Security Center Mobile Server and BlackBerry Security Center Mobile Clients.

- **Use HTTPS.** Select to encrypt communications between Security Center Mobile Server and Security Center Mobile Clients (port 80 cannot be used for HTTPS). If you want to reassign the port currently being used for HTTP (for example, port 8080) to HTTPS, do the following:
  1. Enter a different port number (for example, 8081), make sure to clear Use HTTPS, then click Apply.
ii Enter the number that you were previously using for HTTP (8080 in this example), select Use HTTPS, then click Apply.

- **Virtual folder name.** Type the name of the folder that contains the BlackBerry application files. Only alpha-numeric characters are allowed.
  
  **NOTE** The path to the application on the server appears in Server local folder path field.

- **State.** Indicates if the port is open, and if it can be used with HTTP (default) or HTTPS.

- **Test link.** Click to verify that the link to the virtual folder works. This is the link used by users to install Security Center Mobile Client using OTA deployment.

4 Configure the BES push notification settings:

- **Enable.** Select to allow push alarm notifications between Security Center Mobile Server and the BES.

- **BlackBerry Enterprise Server address.** Specify the BES web address.

- **BlackBerry push listening port.** Specify the port on BlackBerry Security Center Mobile Clients dedicated to listening for push alarm notifications.
  
  **NOTE** This port should only be changed if your BlackBerry device is already using port 100 for another application.

  A warning state indicates that the BES cannot push the notification to some devices.

5 Click Apply.
Configure Apple push notifications

You configure Apple push notifications in the Security Center Mobile Admin Tool Apple page.

When the Security Center Mobile Server sends a push notification, it first verifies that the user of the mobile device has logged on to the Security Center Mobile Client within the last seven days. If the user has not logged on in the last seven days, push notifications are disabled for that user, and an email is sent from Security Center informing the user of the issue. Push notifications are re-enabled automatically the next time the user logs on.

**CAUTION** The performance of the Apple Push Notification Service is not under Genetec’s control. As a result, delivery of critical alarms is dependant on any restrictions applied to the service by Apple.

1. Log on to the Security Center Mobile Admin Tool.
2. On the Security Center Mobile Admin Tool home page, click the Configuration list, and select Apple.
   
   The Apple page appears.

3. Select Enable to turn on push notifications to Apple Security Center Mobile Clients.

   The State field validates that Security Center Mobile Server can establish a secure connection to Gateway.push.apple.com port 2195. It also validates the Apple Push Notification certificate. This certificate is installed when you install Security Center Mobile Server.

   The Genetec feedback service ensures that push notifications are sent to Apple devices that have Security Center Mobile installed. It is required to comply with Apple’s terms and conditions regarding the Apple Push Notification Service. If you see “Warning” in this field, it means that the feedback service is unable to contact Genetec, and you should contact Genetec Technical Assistance immediately. For more information see “Contacting Genetec Technical Assistance” on page ix.

4. Click Apply.
Apple push certificate expiry

Apple generates push certificates that are valid for one year. Approximately one month before your Apple push certificate is set to expire, the mobile client will attempt to download a new certificate from Genetec. If the client is unable to download a new certificate, the certificate will expire and the State field will display the following message:

If this occurs, make sure that your firewall settings allow the server to contact http://downloads.genetec.com. If the server is still unable to download a new certificate, contact Genetec Technical Assistance. For contact information, see "Contacting Genetec Technical Assistance" on page ix.
Configure Android OTA and push notifications

You configure Android push notifications in the Security Center Mobile Admin Tool Android page.

**CAUTION** The performance of the Android C2DM (Cloud to Device Messaging) framework is not under Genetec’s control. As a result, delivery of critical alarms is dependant on any restrictions applied to the service by Android. In addition, the C2DM service is currently in a preliminary beta phase, and therefore Genetec cannot guarantee its performance.

1. Log on to the Security Center Mobile Admin Tool.
2. On the Security Center Mobile Admin Tool home page, click the Configuration list, and select Android.
   
   The Android page appears.

3. Configure the Android OTA settings:

   **NOTE** You need an authentic SSL certificate, such as from VeriSign, to use Android OTA deployment with HTTPS. For more information, see “Configure Security Center Mobile Admin Tool SSL certificates” on page 25.

   - **Port.** Specify the port for OTA deployment between Security Center Mobile Server and Android Security Center Mobile Clients.
   - **Use HTTPS.** Select to encrypt communications between Security Center Mobile Server and Security Center Mobile Clients (port 80 cannot be used for HTTPS). If you want to reassign the port currently being used for HTTP (for example, port 8080) to HTTPS, do the following:
i  Enter a different port number (for example, 8081), make sure to clear Use HTTPS, then click Apply.

ii Enter the number that you were previously using for HTTP (8080 in this example), select Use HTTPS, then click Apply.

- Virtual folder name. Type the name of the folder that contains the Android application files. Only alpha-numeric characters are allowed.
  
  **NOTE** The path to the application on the server appears in **Server local folder path** field.

- Test link. Click to verify that the link to the virtual folder works. This is the link used by users to install Security Center Mobile Client using OTA deployment.

- State. Indicates if the port is open, and if it can be used with HTTP (default) or HTTPS.

4 Enable push notifications.

- **Enable.** Select to allow push alarm notifications between Security Center Mobile Server and the Android server.

  The State field validates that Security Center Mobile Server can establish a secure connection to the Android server.

5 Click Apply.
Monitoring the Security Center Mobile System

This section explains how to monitor your Security Center Mobile system using the Security Center Mobile Admin Tool.

This section includes the following topics:

- "Open Security Center Mobile Admin Tool Monitoring pages" on page 35
- "About monitoring sessions" on page 35
- "About monitoring video" on page 36
- "About monitoring doors" on page 37
- "About monitoring devices" on page 38
- "Delete Device" on page 39

Open Security Center Mobile Admin Tool Monitoring pages

1. Log on to the Security Center Mobile Admin Tool.
2. On the Security Center Mobile Admin Tool home page, click the Monitoring list, and select either Sessions, Videos, Doors, or Devices.

About monitoring sessions

You can monitor the user connections to your Security Center Mobile systems from the Security Center Mobile Admin Tool Sessions page. The top of the page displays the total number of sessions at that point in time.

![Security Center Mobile Admin Tool](image)

The Sessions page lists the following information about each user connection:

- **Username**: Security Center Mobile Client username.
- **Session count**: The number of sessions the user is logged onto.
- **Log Off**: Force user account logoff. This stops video and door streaming to all mobile devices associated with the user account.
When a user's privileges are changed in Security Center, the Security Center Mobile Client only reflects the change when the user logs off and logs back on to the client. Forcing logoff is a quick way to update all mobile devices associated with a particular user account. Users are automatically logged back on after a forced logoff.

- **Username.** Security Center Mobile Client username.
- **Last access.** The last time the Security Center Mobile Client accessed the Security Center Mobile system.
- **Device model.** Product model name.
- **Client version.** Security Center Mobile Client version running on the device.
- **Client IP.** IP address of the mobile device.

### About monitoring video

You can monitor the video streams to your Security Center Mobile systems from the Security Center Mobile Admin Tool Videos page. The top of the page displays the total number of video streams at that point in time.

**NOTE** If you lose connection to the video stream on the server side, Apple and BlackBerry devices receive an error message immediately, but Android devices make take up to two minutes to receive the error message.

The Videos page lists the following information about each user connection:

- **Camera name.** The name of the camera in the Omnicast system.
- **Connection state.** The following status is displayed:
  - **Starting.** Trying to connect to Omnicast.
  - **Connected (waiting for video stream).** Connected to Omnicast and waiting for the video stream.
  - **Streaming.** Video content is being sent to connected devices
  - **Closed.** Closing connection because the are no mobile device watching this camera.
  - **Clients connected.** The number of Security Center Mobile Clients viewing the camera video stream.
• fps. The maximum frame rate per second that is sent by the Security Center Mobile Server. The actual framerate may vary, depending on the available bandwidth to the connected device.
• KB/s. The amount of bandwidth, in kilobytes per second, used by Security Center Mobile Server to stream the transcoded M-JPEG video.
• Omnicast directory. The location of the camera in the Omnicast directory.
• Instance ID. Unique identification number assigned by the camera by Omnicast.

About monitoring doors

You can monitor the access points (doors and elevators) streamed to your Security Center Mobile system, as well as any camera streams associated with those access points, from the Security Center Mobile Admin Tool Doors page. The top of the page displays the total number of doors/elevators being monitored at that point in time.

The Doors page lists the following information about each user connection:
• Door name. The name of the door in the Security Center system.
• Clients connected. The number of client applications monitoring the door.
Configuring Security Center Mobile Server | Monitoring the Security Center Mobile System

About monitoring devices

You can monitor the user connections to your Security Center Mobile systems from the Security Center Mobile Admin Tool Devices page. The top of the page displays the total number of devices that have connected to the Security Center Mobile Server.

The Device page lists the following information about each user connection. Click any of the column headings to sort the list alphabetically by that heading:

- **Name**: Name assigned to the mobile device.
- **Username**: The last user log on name for the device.
- **Device model**: The product model name.
- **Notification**: Indicates if the server has push notifications enabled on that device.

**NOTE** Any Apple or Android devices with disabled push notifications are displayed in yellow.

- **Phone number**: The device phone number.
  - **Apple phone numbers are never displayed, and are listed as Not available.**
BlackBerry users can specify whether or not to display their phone numbers. If they choose not to display their numbers, the BlackBerry device shows Unknown Number to applications accessing it. This message is set by BlackBerry and cannot be changed.

- OS version. The operating system used by the device.
- Client version. The Security Center Mobile Client version running on the device.
- Last logon. The last time the user logged on.
- Last notification. The last push notification sent to the device.

Delete Device

When a device is no longer in use, you should remove it from the Security Center Mobile system so that push notifications are no longer sent to that device.

1. Log on to the Security Center Mobile Admin Tool.
2. On the Security Center Mobile Admin Tool home page, click the Monitoring list, and select Devices.
Installing Security Center Mobile Client

This section explains how to install the Security Center Mobile Client on the Apple Multi-Touch devices (iPhone, iPod, iPad), BlackBerry devices, and Android devices.

This section includes the following topics:

- "Before you install" on page 42
- "Install Security Center Mobile Client on a Blackberry" on page 44
- "Install Security Center Mobile Client on Apple mobile devices" on page 45
- "Install Security Center Mobile Client on Android devices" on page 46
Before you install

This section describes the things you need to know and do before you install Security Center Mobile Client.

This section includes the following topics:

- "Review the Release Notes" on page 42
- "Prerequisites for BlackBerry devices" on page 42
- "Prerequisites for Apple Multi-Touch devices" on page 42
- "Prerequisites for Android devices" on page 43
- "Prerequisites for firewall" on page 43

Review the Release Notes

Read the "Security Center Mobile 2.1 Release Notes" on page 5 for any known issues and other information about the release.

Prerequisites for BlackBerry devices

BlackBerry devices need the following prerequisites to receive alarm notifications and stream video on your cellular network.

<table>
<thead>
<tr>
<th>Feature</th>
<th>BlackBerry prerequisite</th>
</tr>
</thead>
</table>
| Receive alarm notifications       | • Connected to the cellular network.  
|                                   | • Activated on the BES server. |
| Use video streaming on a cellular network | Enable the APN settings.  
|                                   | For information on how to configure the APN settings, see [http://www.blackberryfaq.com/index.php/Carrier_specific_APN/TCP_settings](http://www.blackberryfaq.com/index.php/Carrier_specific_APN/TCP_settings). |

Prerequisites for Apple Multi-Touch devices

To receive push alarm notifications on Apple Multi-Touch devices, the device must be configured as follows:

- Apple devices must have access to the Internet.
- iPod devices without 3G connectivity must connect to a WiFi network that allows access to the Internet. You’ll also need to open port 5223 inbound (TCP) on the company firewall.
Prerequisites for Android devices

To receive push alarm notifications on Android devices, the device must be configured as follows:

- Push alarm notifications are supported on Android versions 2.2 and later.
- The Android device must have access to the Internet.
- Each Android device must be associated to a valid Google Account.
- If the device is connecting to the internet using a WiFi network, you’ll need to open port 5228 inbound (TCP) on the company firewall.

Prerequisites for firewall

In order to log on to Security Center Mobile Server, the firewall on Security Center Mobile Server computer must be configured to allow port 8100 and 8101 to connect.
Installing Security Center Mobile Client on a Blackberry

This section explains the different ways to install Security Center Mobile Client on your Blackberry device.

This section includes the following topics:

- "Install Security Center Mobile Client from BlackBerry App World" on page 44
- "Install Security Center Mobile Client using BlackBerry Desktop Manager" on page 44
- "Install Security Center Mobile Client using OTA deployment" on page 45

Install Security Center Mobile Client from BlackBerry App World

To use App World, the BlackBerry device must be connected to the Internet. You’ll also need an App World account.

1. From App World, search for Genetec.
2. Download Genetec Security Center Mobile.

The Security Center Mobile icon appears on the Home screen as GSC Mobile.

After you are done: "Open Security Center Mobile Client" on page 51.

Install Security Center Mobile Client using BlackBerry Desktop Manager

You use the Blackberry Desktop Manager and a USB connection to install Security Center Mobile Client from your computer to your BlackBerry.

1. Connect your BlackBerry to your computer using a USB cable.
2. On your computer, open BlackBerry Desktop Manager.
3. Click Add, and navigate to the Security Center Mobile BlackBerry program folder containing the BlackBerry ALX files. Select the folder for the version of your BlackBerry operating system, and then select the.alx file.
4. Click OK.
   The application appears in the list of installed software.
5. Click Next.
   The manager installs Security Center Mobile Client on your BlackBerry.

Security Center Mobile appears in the BlackBerry Applications folder.

After you are done: "Open Security Center Mobile Client" on page 51.
Install Security Center Mobile Client using OTA deployment

You can download Security Center Mobile Client from a browser over a wireless network.

Before you begin: You need to configure your APN (Access Point Name) as follows:

1. From your BlackBerry device, go to Options > Advanced Options > Browser.
2. Under Default browser configuration, select Internet Browser.
3. Press the Back key, and then select Save.
4. Go to Options > Advanced Options > TCP/IP and configure the following:
   - APN Settings. Select to enable.
   - APN. Enter your wireless provider's Access Point Name (for example, the Rogers Wireless APN is “internet.com”). You can find your provider's APN at http://www.blackberryfaq.com/index.php/Carrier_specific_APN/TCP_settings.
5. Press the Back key, and then select Save.

To download Security Center Mobile Client:

1. Your system administrator will send you an email with a download link.
   The required link is displayed in the Security Center Mobile Admin Tool. For more information, see "Configure BlackBerry OTA and push notifications" on page 29.
2. Click the link and follow the on-screen instructions to install Security Center Mobile Client.
   Security Center Mobile Client is installed to the Download folder.
3. Restart the BlackBerry.

After you are done: "Open Security Center Mobile Client" on page 51.

Install Security Center Mobile Client on Apple mobile devices

On Apple devices, you download the Security Center Mobile Client from the App Store.

To use the App Store, the Apple device must be connected to the Internet. You’ll also need an iTunes App Store account.

1. From the App Store, search for Genetec.
2. Download Genetec Security Center Mobile.

The Security Center Mobile icon appears on the Home screen as GSC Mobile.

After you are done: "Open Security Center Mobile Client" on page 51.
Install Security Center Mobile Client on Android devices

This section explains the different ways to install Security Center Mobile Client on your Android device.

This section includes the following topics:

- "Install Security Center Mobile Client from Android Market" on page 46
- "Install Security Center Mobile Client using OTA deployment" on page 46

Install Security Center Mobile Client from Android Market

To use Android Market, the Android device must be connected to the Internet. You’ll also need an Android Market account.

1. From Android Market, search for Genetec.
2. Download Genetec Security Center Mobile.

The Security Center Mobile icon appears on the Home screen as GSC Mobile.

After you are done: "Open Security Center Mobile Client" on page 51.

Install Security Center Mobile Client using OTA deployment

You can download Security Center Mobile Client from the Android browser over a wireless network.

1. Your system administrator will send you an email with a download link.
   The required link is displayed in the Security Center Mobile Admin Tool. For more information, see "Configure Android OTA and push notifications" on page 33.
2. Click the link and follow the on-screen instructions to install Security Center Mobile Client.

After you are done: "Open Security Center Mobile Client" on page 51.
Using Security Center Mobile Client

This section explains how to use the main features of Security Center Mobile Client. This section includes the following topics:

- "Security Center Mobile Client Basics" on page 48
- "Viewing video" on page 55
- "Viewing doors" on page 59
- "Viewing alarms" on page 65
- "Using Favorites" on page 69
- "Searching for specific entities" on page 70
This section provides the basic information and tasks you need to get started using Security Center Mobile Client.

**NOTE** To use Security Center Mobile Client, your mobile device must be part of a WiFi or cellular network. The video frame rate may vary, depending on your available bandwidth.

This section includes the following topics:

- "About Security Center Mobile Client" on page 49
- "About Security Center Mobile Client application icons" on page 50
- "Open Security Center Mobile Client" on page 51
- "Configure Security Center Mobile Client options" on page 52
- "Log on to Security Center Mobile Client" on page 53
- "Use the same mobile device on a different server" on page 53
- "Log off Security Center Mobile Client" on page 54
About Security Center Mobile Client

Security Center Mobile Client is the client component of Security Center Mobile that is installed on mobile devices. You use the Security Center Mobile Client to receive alarms, view door status and events, perform door actions, or view live video streams from your Security Center system. Video streams are displayed as M-JPEG at a maximum of 8 frames per second, depending on your available bandwidth and the device’s CPU.

The Security Center Mobile Client incorporates the tap, swipe, and touch functionality available on Apple, BlackBerry, and Google Android-supported touchscreen devices. On the iPad, the client uses the additional real-estate to display up to six video camera streams.

Best practice: The Google Android operating system is supported on many different types of mobile devices. Genetec used a Samsung Captivate smartphone to show the functionality of the Security Center Mobile Client, but you should also have your device’s documentation on hand as a reference, as the procedures in this chapter may differ slightly from what is required for your specific device.
About Security Center Mobile Client application icons

Security Center Mobile Client application icons give you one-click access to many of the Security Center Mobile features.

The way icons are displayed on the screen depends on the type of mobile device you are using. For example, on BlackBerry devices the icons are displayed down the left side of the screen, while on Android devices the icons are displayed at the top of the screen. On Apple iPhone and iPod, icons appear in a tab bar at the bottom of the screen, while on the iPad, you need to click the Menu icon to display the application icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Entities browser icon" /></td>
<td>Entities browser</td>
<td>View a list of areas in your Security Center system. The entities in the Entities browser represent the Area entities in your Security Center system. Cameras are grouped under Areas. In the Entities browser, you can browse the cameras and doors in each area, and select the camera/door you want to view.</td>
</tr>
<tr>
<td><img src="image" alt="Alarms icon" /></td>
<td>Alarms</td>
<td>View a list of unacknowledged alarms and select the alarm you want to view.</td>
</tr>
<tr>
<td><img src="image" alt="Favorites icon" /></td>
<td>Favorites</td>
<td>View a list of areas and cameras you have added to Favorites.</td>
</tr>
<tr>
<td><img src="image" alt="Options icon" /></td>
<td>Options</td>
<td>View and configure Security Center Mobile Client settings, including the connections settings to Security Center Mobile Server, Security Center username and password, encryption, cellular network, and alarm notification.</td>
</tr>
<tr>
<td><img src="image" alt="Menu icon" /></td>
<td>Menu</td>
<td>(iPad only) View pop-up screen that displays a browser and a tab bar with the Entities, Alarms, Favorites, and Options buttons.</td>
</tr>
<tr>
<td><img src="image" alt="Log on icon" /></td>
<td>Log on</td>
<td>(BlackBerry only) Click to log on.</td>
</tr>
<tr>
<td><img src="image" alt="Log off icon" /></td>
<td>Log off</td>
<td>(BlackBerry only) Click to log off.</td>
</tr>
</tbody>
</table>
Open Security Center Mobile Client

To open the Security Center Mobile Client, do one of the following:

- BlackBerry devices, navigate to the folder where you saved Security Center Mobile, and click the GSC Mobile icon. By default Security Center Mobile is saved to your Downloads folder.

The first time you start Security Center Mobile Client, you are asked to confirm the following:

- "Do you wish to receive http messages". Click Yes to receive alarm notifications.
- "Do you wish to allow the use of your user data". Click Yes to allow outgoing connections between Security Center Mobile Client and Security Center Mobile Server.

- Apple Multi-Touch devices and Google Android devices, from the Home screen, tap the GSC Mobile icon.

**NOTE** The first time you use Security Center Mobile on an Apple device, a pop-up message appears asking if Security Center Mobile can send you push notifications. Click OK to continue.

The Security Center Mobile log on screen appears.
Configure Security Center Mobile Client options

The first time you open the Security Center Mobile Client, you'll need to configure the connection settings to Security Center Mobile Server from the Options screen.

From the Options screen, you can also choose to encrypt the user data (not video streams) that is sent between Security Center Mobile Client and Security Center Mobile Server, use your cellular network to send and receive data and video streams, and turn alarm notifications on or off.

1. **Open Security Center Mobile Client.**
2. **Tap Options.**
   - BlackBerry devices, select Options.
   - Apple and Android devices, tap the Options icon (⚙️ or ⚙️).

   The Security Center Mobile Options screen appears.

3. **Configure the settings as follows:**
   - **Server.** The IP address of the Security Center Mobile Server.
   - **Port.** Set port. The default is 8100.
   - **Username and Password.** Enter your Security Center logon name and password.
   - **Use HTTPS.** Turn encryption on this port on or off. Default is Off.
     - **NOTE** Video streams are not encrypted.
   - **Allow Cellular data.** Specifies whether or not to use your cellular network to connect to Security Center Mobile Server. When off, you can only connect using Wi-Fi. Default is Off.
   - **Push alarms.** Turn alarm notifications on or off. Default is Off.
NOTE When you turn alarm notifications on, Android registers the mobile device with Google C2DM.

4 Save your changes.
   - (Apple and Android devices). Tap Save to save your changes and return to the logon screen.
   - (BlackBerry devices). Press the Back key, choose Yes to save your changes, then press the Back key again to return to the logon screen.

Log on to Security Center Mobile Client

You will remain logged on to Security Center Mobile until you log off.

Best practice: Use the following best practices when logging on:
   - You should set the access code to protect access to your mobile device.
   - For Apple and Android devices, turn off WiFi on your mobile device if you want to log on using 3G only. If you leave WiFi on, and the device detects an available WiFi network, it will switch to WiFi automatically, and you may lose connectivity to Security Center Mobile Server.

To log on to Security Center Mobile Client:
1 Open Security Center Mobile Client.
2 Tap or select Log on.

Use the same mobile device on a different server

You can use your mobile device on a different server, but you may receive duplicate push notifications for the same alarm. As a workaround, do one of the following:
   - On your mobile device, before you log on to a different server, turn push alarms off for your current server. For more information on turning push alarms on and off, see "Turn alarms on and off" on page 68.
   - From the Security Center Mobile Admin Tool, delete your mobile device from the server you won't be using. For more information on how to delete a device from the server, see "Delete Device" on page 39.
Log off Security Center Mobile Client

1. Do one of the following:
   - On Apple Multi-Touch devices, click the Close button ("X") at the top of the screen. On iPhone and iPod touch, you have to navigate back to the root list in the Entity browser to view the Close button.
     
     **NOTE** If your Apple device supports multi-tasking, pressing the Home button does not log you out, it only minimizes the application (it's still running in the background). To close the application, press the home button twice to view the applications running in the background, touch the Security Center Mobile application icon for a few seconds, and then tap the minus icon.

   - On BlackBerry, press the Menu key and select Close. Or, press the Back key until you return to the home screen, and select Log out.

   - On Android, press the Back key until you are prompted to log off.
Viewing video

With Security Center Mobile Client, you can view a live video stream from a camera in your Security Center system. On the iPad, you can view up to six video streams.

**NOTE** When opening a new video stream, users are prompted to retry later if the server is too busy (too many video streams already in progress).

This section includes the following topics:
- "Browse and select cameras" on page 55
- "Using the camera controls" on page 57

**Browse and select cameras**

You use the Entities browser to find and select the entities you want to view.

In Security Center Mobile Client, the entities in the Entities browser represent the Area entities in your Security Center system. Cameras are grouped under Areas.

1. Open Security Center Mobile Client.
2. Do one of the following:
   - (iPhone, iPod touch, BlackBerry, and Android devices) Tap or select the Entities browser icon.
   - (iPad) Tap the Menu icon ☰, and then select the Entities browser icon.

The Entities browser appears.
3 Swipe or scroll through the Entities list, and tap or select an entity. If you select an area, a list of cameras linked to the area appears. Cameras are offline when they appear in red.

4 Swipe or scroll through the cameras list, tap a tile (iPad), and tap or select a camera icon 📺. The camera window appears.
## Using the camera controls

You can use the controls on the camera window to zoom in and out on the camera display. If available on the camera, you can use the flip (rotate camera 180 degrees) and PTZ features. You can also take a snapshot from a live video camera and save it to the photo library on the mobile device.

### Task

<table>
<thead>
<tr>
<th>Task</th>
<th>Apple Multi-Touch device</th>
<th>Blackberry Bold</th>
<th>BlackBerry Storm/Torch</th>
<th>Android devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zoom in/out¹</td>
<td>Pinch screen.</td>
<td>Press the “I” button to zoom in, and the “O” button to zoom out.²</td>
<td>Tap screen to zoom in.</td>
<td>Pinch screen Press the Menu key, and select Zoom in or Zoom out.</td>
</tr>
<tr>
<td>Change display orientation</td>
<td>Rotate device. The display adjusts to the new orientation.³</td>
<td>Not supported</td>
<td>Rotate device. The display adjusts to the new orientation.</td>
<td>Rotate device. The display adjusts to the new orientation.</td>
</tr>
<tr>
<td>Pan and tilt¹</td>
<td>Swipe left/right to pan.</td>
<td>Move Up/Down/Left/Right on the trackpad.</td>
<td>Swipe left/right to pan.</td>
<td>Swipe left/right to pan.</td>
</tr>
<tr>
<td></td>
<td>Swipe up/down to tilt.</td>
<td></td>
<td>Swipe up/down to tilt.</td>
<td>Swipe up/down to tilt.</td>
</tr>
<tr>
<td>Flip the image 180 degrees</td>
<td>Tap the flip icon.</td>
<td>Press the Menu key, and select Flip.</td>
<td>Press the Menu key, and select Flip.</td>
<td>Press the Menu key, and tap Flip.</td>
</tr>
<tr>
<td>Return PTZ camera to home position¹</td>
<td>Tap the home icon.</td>
<td>Press the Menu key, and select Home.</td>
<td>Press the Menu key, and select Home.</td>
<td>Press the Menu key, and tap Home.</td>
</tr>
</tbody>
</table>
Using Security Center Mobile Client | Viewing video

<table>
<thead>
<tr>
<th>Task</th>
<th>Apple Multi-Touch device</th>
<th>Blackberry Bold</th>
<th>BlackBerry Storm/ Torch</th>
<th>Android devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PTZ presets</strong>¹</td>
<td>Select from the available presets.</td>
<td>Press the Menu key. Select from the available presets, or press the number of the preset on the keypad.</td>
<td>Press the Menu key and select from the available presets.</td>
<td>Press the Menu key, tap Preset, and select from the available presets.</td>
</tr>
<tr>
<td><strong>Take snapshot</strong></td>
<td>(iPad) Tap the Snapshot button. (iPhone, iPod Touch) Tap the camera icon.</td>
<td>Press the Menu key and select Take Snapshot.</td>
<td>Press the Menu key and select Take Snapshot.</td>
<td>Press the Menu key, and tap Take Snapshot.</td>
</tr>
<tr>
<td><strong>Maximize or minimize tile (iPad only)</strong></td>
<td>Tap the Fullscreen button.</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>Remove entity from tile. (iPad only)</strong></td>
<td>Tap the Clear button.</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>Select or deselect tile (iPad only)</strong></td>
<td>• Tap screen to select tile. • Double-tap the screen to deselect tile.</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>Return to Entities browser list of cameras.</strong></td>
<td>(iPad) Tap the Menu icon , and then select the Entities browser icon. (iPhone, iPod touch). Tap the back button to navigate to the previous area, or tap the Entities browser icon to go to the root entities list.</td>
<td>Press the Back key.</td>
<td>Press the Back key.</td>
<td>Press the Back key.</td>
</tr>
</tbody>
</table>

1. When you perform a PTZ camera operation in the Security Center Mobile Client, that camera appears in Security Desk as being locked by an administrator, even if you are not logged on to the mobile client as an administrator.

2. In the previous version of Security Center Mobile, the +/− buttons were used to zoom in and out. In this version, the I/O buttons are used to zoom in and out. This may be initially confusing because the BlackBerry keyboard shares the same key for “I” and “−”, and the same key for “O” and “+”.

3. Make sure that the “lock orientation” feature on your Apple device is disabled.
Viewing doors

With Security Center Mobile you can view the status of access points (doors and elevators) in your Security Center system, and perform door-related actions such as locking and unlocking, or overriding lock/unlock rules. You can also view live video from any cameras associated with your doors or elevators.

This section includes the following topics:
- "Browse and select doors" on page 59
- "Viewing door events" on page 60
- "Using door controls" on page 62

Browse and select doors

You use the entities browser to find and select the doors you want to view.

In Security Center Mobile Client, the doors in the Entities Browser represent the door entities in your Security Center system. Doors can be listed as individual entities, or as entities within areas, depending on how they are configured in your Security Center system.

1. Open Security Center Mobile Client.
2. Do one of the following:
   - (iPhone, iPod touch, BlackBerry, and Android devices) Tap or select the Entities browser icon.
   - (iPad) Tap the Menu icon , and then select the Entities browser icon.

The Entities browser appears.
3. Swipe or scroll through the Entities list, select a tile (iPad), and tap or select a Door icon. If you don’t see a Door icon in the root entities list, tap or select an area, and then tap or select a Door icon. Doors are offline when they appear in red.

The door window appears.

**Viewing door events**

The Door window displays the various door-related events and actions as they occur in Security Center. For more information on door events

The door events are:

- **Access granted.** The most common event. Access has been granted through a door to a cardholder according to the access rules governing the door or area.

- **Access denied.** Access has been denied to a door according to the access rules governing the door or area.

  Cardholders can be denied access for the following reasons:

  - **Unassigned credential.** At a door or area, a credential has been used that has not been assigned to any cardholder.
  
  - **Unknown credential.** A credential has been used that is unknown to the Security Center.
  
  - **Expired credential.** An expired credential has been used.
  
  - **Inactive credential.** A credential with an inactive profile has been used.
  
  - **Lost credential.** A credential that has been declared as lost has been used.
  
  - **Stolen credential.** A credential that has been declared as stolen has been used.
- **Inactive cardholder.** A cardholder with an inactive profile has attempted to use his or her credential.
- **Door open too long.** The door has been held open for too long.
- **Door forced open.** The door has been forced open. This event is unavailable with a readerless door.
- **Door manually unlocked.** In Security Desk, a user has manually unlocked a door.
- **Request to exit.** Someone has pressed the door release button or has triggered a request to exit motion detector.
- **Hardware tamper.** The tamper input on a unit has been triggered.
- **Manual station activated.** Someone has pulled the door emergency release (manual pull station).
- **Input trouble - short.** A supervised input has detected a short-circuit.
- **Input trouble - open.** A supervised input has detected an open-circuit.
Using door controls

You can use the controls in the Security Center Mobile Client to perform door-related actions, such as locking/unlocking a door, or overriding lock/unlock schedules. You can also view live video from cameras associated with doors. For more information on how to control the cameras associated with your doors, see "Using the camera controls" on page 57.

<table>
<thead>
<tr>
<th>Task</th>
<th>Apple Multi-Touch device</th>
<th>Blackberry Bold</th>
<th>BlackBerry Storm/Torch</th>
<th>Android devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>View cameras associated to the door.</td>
<td>Tap Cameras. Tap a camera on Side A, Side B, or tap Do not display a camera to conserve bandwidth (a Door icon is displayed instead of video).</td>
<td>Press Menu button and select Change camera. Select a camera on Side A, Side B, or select Do not display a camera to conserve bandwidth (a Door icon is displayed instead of video).</td>
<td>Press Menu button, or tap screen, and select Change camera. Select or tap a camera on Side A, Side B, or select Do not display a camera to conserve bandwidth (a Door icon is displayed instead of video).</td>
<td>Tap Change camera. Select or tap a camera on Side A, Side B, or select Do not display a camera to conserve bandwidth (a Door icon is displayed instead of video).</td>
</tr>
<tr>
<td>Task</td>
<td>Apple Multi-Touch device</td>
<td>Blackberry Bold</td>
<td>BlackBerry Storm/ Torch</td>
<td>Android devices</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Switch to camera controls from</strong></td>
<td>(iPhone, iPod Touch)</td>
<td>Press Menu button and select Full Menu.</td>
<td>Press Menu button, or tap screen, and select Full Menu.</td>
<td>Press Menu button.</td>
</tr>
<tr>
<td><strong>the Door window</strong></td>
<td>(iPad) Not required. Door and video controls both displayed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Unlock door for a few seconds</strong></td>
<td>Tap the lock/unlock icon</td>
<td>Press Menu button and select Unlock.</td>
<td>Press Menu button, or tap screen, and select Unlock.</td>
<td>Tap the lock/unlock icon.</td>
</tr>
<tr>
<td><strong>View override options</strong></td>
<td>Tap the Override button.</td>
<td>Press Menu button and select Override lock schedule.</td>
<td>Press Menu button, or tap screen, and select Override lock schedule.</td>
<td>Tap the Override button.</td>
</tr>
<tr>
<td><strong>Unlock for maintenance mode</strong></td>
<td>From the override options window, tap the Maintenance mode icon, then tap Apply.</td>
<td>From the override options window, select Maintenance mode, then select OK.</td>
<td>From the override options window, select Maintenance mode, then select OK.</td>
<td>From the override options window, tap the Maintenance mode icon, then tap Apply.</td>
</tr>
</tbody>
</table>
| **Specify an override schedule** | From the override options window, tap the temporary override icon, and configure the settings as follows:  
  - Tap Lock or Unlock.  
  - Tap Relative, then specify a fixed override duration.  
  - Tap Absolute, then specify a beginning and end for the override.  
  - Tap Apply. | From the override options window, select Temporarily override lock schedule, click OK, then configure the settings as follows:  
  - Select Locked or Unlocked.  
  - Select Override for a fixed duration, then specify the duration.  
  - Select Schedule an override, then specify a beginning and end for the override.  
  - Select OK. | From the override options window, select Temporarily override lock schedule, click OK, then configure the settings as follows:  
  - Select Locked or Unlocked.  
  - Select Override for a fixed duration, then specify the duration.  
  - Select Schedule an override, then specify a beginning and end for the override.  
  - Select OK. | From the override options window, tap the temporary override icon, and configure the settings as follows:  
  - Tap Lock or Unlock.  
  - Tap Relative, then specify a fixed override duration.  
  - Tap Absolute, then specify a beginning and end for the override.  
  - Tap Apply. |
### Using Security Center Mobile Client | Viewing doors

<table>
<thead>
<tr>
<th>Task</th>
<th>Apple Multi-Touch device</th>
<th>BlackBerry Bold</th>
<th>BlackBerry Storm/Torch</th>
<th>Android devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cancel overrides</strong></td>
<td>From the door window, tap the Override button.</td>
<td>From the door window, press the Menu button, then select Cancel overrides.</td>
<td>From the door window, press the Menu button, or tap screen, then select Cancel overrides.</td>
<td>From the door window, tap the Override button.</td>
</tr>
<tr>
<td><strong>Change display orientation</strong></td>
<td>Rotate device. The display adjusts to the new orientation.</td>
<td>Not supported</td>
<td>Rotate device. The display adjusts to the new orientation.</td>
<td>Rotate device. The display adjusts to the new orientation.</td>
</tr>
</tbody>
</table>

1. Make sure that the “lock orientation” feature on your Apple device is disabled.
Viewing alarms

With Security Center Mobile you can receive, view, and acknowledge alarms from Security Center. You can also turn on and off alarm notification.

This section includes the following topics:

- "About alarm notifications" on page 65
- "View an alarm" on page 66
- "Turn alarms on and off" on page 68

About alarm notifications

Security Center Mobile uses push notifications to alert you to new alarms in Security Center.

Before you begin: To receive an alarm notification from Security Center, the mobile device’s push notification feature must be configured in Security Center Mobile Server and the Push Alarms option must be turned on in Security Center Mobile Client.

- On BlackBerry devices, alarm notifications appear as a pop-up on your screen.
- On Apple Multi-Touch devices:
  - If Security Center Mobile is not open or is running in the background, then a pop-up appears, and a numbered badge appears on the GSC Mobile icon showing the current number of unacknowledged alarms.
  - If Security Center Mobile is running, then a sound alerts you to a new alarm, a pop-up appears, and a numbered badge appears on the Alarm tab.
  - (iPad) The number of active alarms is displayed in brackets in the title bar.
- On Android devices, alarm notifications are displayed in the notification bar at the top of the screen, to the left of the other indicator icons (battery level, signal strength, etc).

You can choose to View the alarm or Ignore the alarm. When you ignore the alarm, the alarm appears as an unacknowledged alarm in the Alarm window.

To receive an alarm notification from Security Center, the Apple, BlackBerry, and Android push notification feature must be configured in Security Center Mobile Server, and the Push Alarms option must be turned on in Security Center Mobile Client.

For more information on how to configure alarm notifications, see the following sections:

- "Configure BlackBerry OTA and push notifications" on page 29
- "Configure Apple push notifications" on page 31
- "Configure Android OTA and push notifications" on page 33
- "Configure Security Center Mobile Client options" on page 52
View an alarm

You can view a list of all unacknowledged Security Center alarms from the Alarms window. From each alarm window you can view information about the alarm, including the event that triggered it, when it was triggered, and the alarm’s identification number. You can also view a live video stream from cameras that are attached to the alarm, and acknowledge the alarm.

**NOTE** Acknowledged alarms do not appear in the Security Center Mobile Client.

1. **Open Security Center Mobile Client.**
2. **Do one of the following:**
   - (iPhone, iPod touch, BlackBerry) Tap or select the Alarms icon 🔄.
   - (iPad) Tap the Menu icon ❓, and then tap or select the Alarms icon 🔄.
   - (Android) Tap or select the Alarms icon 🔄.

   The Alarms window appears.

3. On BlackBerry devices, you can acknowledge the alarm from the Alarms window. Press the Menu key, and select Acknowledge Alarm.
4. On Android devices, acknowledge an alarm by touching and holding the alarm until the Acknowledge window pops up, then tap Acknowledge.
5. To acknowledge all alarms that appear in the Alarms window, do one of the following:
   - On Apple Multi-Touch devices, tap Ack All.

   **NOTE** (iPad only) After you tap Ack all, a dialog box appears with only the option to choose Yes. If you don’t want to acknowledge all the alarms on the page, tap outside the dialog box.
6 To view alarm details, scroll through the Alarms list, and tap or select an alarm. The alarm window appears.

7 To view a live video stream from a camera attached to the alarm, do one of the following:
   - On Apple Multi-Touch devices and Android devices, under Attached Entities, tap the camera.
   - On BlackBerry select the camera.
   For information on using the camera controls, see "Using the camera controls" on page 57.

8 To acknowledge the alarm, do one of the following:
   - On Apple Multi-Touch devices and Android devices, tap Acknowledge.
   - On BlackBerry devices, press the Menu key, and select Acknowledge Alarm.
Turn alarms on and off

You can turn alarm notifications on and off from your mobile device.

Before you begin: You must be logged on to the Security Center Mobile Client.

1. Do one of the following:
   - On Apple Multi-Touch devices or Android devices, tap the Options icon.
   - On BlackBerry devices, from the home screen, select the Options icon.

2. Do one of the following:
   - On Apple Multi-Touch devices, tap Push Alarms to select On or Off, tap Save, and then log off and log back on to Security Center Mobile Client.
   - On BlackBerry devices, select Push Alarms to clear the check box.
   - On Android devices, tap Push alarms to select On or Off, then tap Save.

NOTE You can also turn off alarms by doing the following:

- Disable push notifications on your Apple device. From the Home screen, tap Settings > Notifications > GSC Mobile, and set each option to OFF.
- Disable push notifications from Security Center Mobile Server. You can disable push notifications for each device type. For more information, see the following sections:
  - "Configure BlackBerry OTA and push notifications" on page 29
  - "Configure Apple push notifications" on page 31
  - "Configure Android OTA and push notifications" on page 33
Using Favorites

The Security Center Mobile Client allows you to add your most frequently viewed entities to a list of favorites. This allows you to quickly access only the entities that you need.

**NOTE** Entities listed in your Favorites do not appear in red when they are offline.

This section includes the following topics:

- "Add an entity to Favorites" on page 69
- "Delete an entity from Favorites" on page 69

Add an entity to Favorites

You can add entities (areas), doors, and cameras you want to monitor to your Security Center Mobile Favorites.

1. To add an entity to Favorites, do one of the following:

   - On Apple iPhone and iPod Touch, tap or select the Entities browser icon , and then tap the Favorites icon next to the entity. The Favorites icon turns yellow .
   - On Apple iPad, tap the Favorites button in the dashboard.
   - On BlackBerry devices, from the home screen, select the Entities browser icon . Select the entity, and press the Menu key, and then select Add to Favorites.
   - On Android devices, touch and hold the entity you want to add until the Add to favorites pop-up window appears, then tap Add to favorites.

Delete an entity from Favorites

To delete an entity from Favorites, do one of the following:

- On Apple iPhone and iPod Touch, tap or select the Entities browser icon , and then tap the Favorites icon next to the entity. The Favorites icon turns grey .
- On Apple iPad, tap the Favorites button in the dashboard.
- On BlackBerry devices, from the home screen, select the Entities browser icon , the press the Menu key, and select Favorites.
- On Android devices, touch and hold the entity you want to remove from Favorites until the Remove from favorites pop-up window appears, then tap Remove from favorites.
The Security Center Mobile Client provides a search feature that you can use to locate specific entities. This option is useful when entities are nested under one or more areas.

This section includes the following topics:
- "About searching" on page 70
- "Search for entities on Apple devices" on page 70
- "Search for entities on BlackBerry devices" on page 71
- "Search for entities on Android devices" on page 71

About searching

When searching for entities, note the following:

- If you enter text in the Search field (for example “door”), the application searches the page of entities you are currently on, as well as all areas and nested areas, for entity names that contain the word “door”.
- If you leave the Search field blank, but tap Include doors to narrow your search to door entities, the application only searches for doors on the current page of entities. It does not search for doors in areas and nested areas. To search for doors in areas and nested areas, you’ll need to tap Include doors and Include areas (the same applies for cameras).

Search for entities on Apple devices

To perform a search:

1. Tap Entities.
   The entities list appears.
2. Tap the Search field, then do one of the following (if you don’t see the search field, scroll to the top of the page):
   - Tap All to search for areas, cameras, and doors.
   - Tap Custom to narrow your search, then tap the back button to return to the main search window.
     **NOTE** If you tap back to the main search screen, you’ll need to first tap All before you can tap Custom to return to the custom search screen.
3. Enter the name or partial name of the entity you’re looking for, then tap Search.

To clear the search field and return to the root Entities list:

1. After you’ve finished your search, tap the “x” to the right of the search field.
   You’ll return to the main search screen.
2 Tap Search with an empty search field.
You’ll return to the root Entities screen.

Search for entities on BlackBerry devices

To perform a search:
1 Select Entities.
The entities list appears.
2 Scroll up to the Search field.
The search options appear.
3 Do one of the following:
   • Enter the name or partial name of the entity you’re looking for, then select Search to
     search for areas, cameras, and doors.
   • Press the Menu key, select Advanced search, select areas, cameras, or doors to nar-
     row your search, then select Search.

Search for entities on Android devices

To perform a search:
1 Tap Entities.
The entities list appears.
2 Press the Menu key, then tap Search, or use your Android device’s search button.
3 Tap on Areas, Cameras, or Doors to narrow your search results.
4 Tap the Search field, enter the name or partial name of the entity you’re looking for,
   then tap the search icon  
   .
Index

A
Access denied
see Door events
Access granted
see Door events
Alarms
about alarm notifications, 65
receiving duplicates, 53
turning on/off, 68
viewing, 65
Android
configuring OTA deployment, 33
Android push notifications
configuring, 33
not working, 33
Apple push notifications
configuring, 31, 33
not working, 31, 33

B
BlackBerry
configuring OTA deployment, 29

C
Camera controls, 57
Changing password, 27
Configuring
Security Center Mobile Server, 24
SSL certificates, 25

D
Door controls, 62
Door events
viewing, 60
Door forced open
see Door events
Door manually unlocked
see Door events
Door open too long
see Door events
Doors
viewing, 59
Duplicate alarms, 53
Duplicate push notifications, 53

E
Elevators
see Door controls
Events
see Door events
Expired credential
see Door events

F
Favorites
using, 69
Flip
see Camera controls

H
Hardware requirements, 9
Hardware tamper
see Door events

I
Inactive cardholder
see Door events
Inactive credential
see Door events
Input trouble - open
see Door events
Input trouble - short
see Door events

Installing
- Security Center Mobile Client, 41
- Security Center Mobile Server, 16

Interoperability, 8

K

Known issues, 10
Known limitations, 10

L

Log off
- Security Center Mobile Admin Tool, 22
- Security Center Mobile Client, 54

Log on
- Security Center Mobile Admin Tool, 22
- Security Center Mobile Client, 53

Lost credential
- see Door events

M

Manual station activated
- see Door events

Monitoring
- devices, 38
- doors, 37
- sessions, 35
- using Security Center Mobile Admin Tool, 35
- video, 36

O

Omnicast compatibility
- installing compatibility packages, 13

Options screen, 52

OTA deployment, 29, 33

P

Pan and tilt
- see Camera controls

Password
- changing, 27

Port configuration
- for Security Center Mobile Server, 14

Presets
- see Camera controls

PTZ presets
- see Camera controls

Push notifications, 31, 33
- receiving duplicates, 53

R

Release notes, 5

Request to exit
- see Door events

Resolved issues, 10

S

Search
- using, 70

Security Center
- configuring users and user groups, 12
- connecting with Security Center Mobile Server, 24
- interoperability, 8
- Security Center 5.1 GA requirements, 7

Security Center Mobile
- about, 2
- features, 3
- known issues, 10
- known limitations, 10
- release notes, 5
- resolved issues, 10

Security Center Mobile Admin Tool
- about, 2
- configuring Android OTA deployment, 33
- configuring Apple push notifications, 31, 33
- configuring BlackBerry OTA deployment, 29
- configuring settings, 27
- configuring SSL certificates, 25
- log off, 22
- log on, 22
- monitoring, 35
- monitoring devices, 38
monitoring doors, 37
monitoring sessions, 35
monitoring video, 36
Server administration, 27
supported web browsers, 7

Security Center Mobile architecture
about, 2

Security Center Mobile Client
about, 2, 49
application icons, 50
before installing, 42
configure options, 52
control cameras, 57
control doors, 62
how to open, 51
installing on Apple devices, 45
installing on BlackBerry devices, 44, 46
log off, 54
log on, 53
using favorites, 69
viewing alarms, 65
viewing door events, 60
viewing doors, 59
viewing video, 55

Security Center Mobile Server
about, 2
configuring, 24
configuring connection to client, 28
configuring ports, 14
connecting to Security Center, 24
connecting to Security Center Mobile Client, 28
hardware requirements, 9
installing, 16
interoperability, 8
pre-installation tasks, 12
software requirements, 9
upgrading, 17
Server
connecting to client, 28
Server administration, 27
Settings
configuring Security Center Mobile Admin Tool, 27
Snapshot
see Camera controls
Software requirements, 9

SSL certificates, 25
Stolen credential
see Door events
Supported devices, 6
Supported web browsers, 7

U
Unassigned credential
see Door events
Unknown credential
see Door events
Upgrading
Security Center Mobile Server, 17
Users and user groups
configuring in Security Center, 12

V
Video
control cameras, 57
viewing, 55
Video controls
see Camera controls
Viewing
alarms, 65
doors, 59
video, 55

W
Web browsers
see Supported web browsers

Z
Zoom
see Camera controls