# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>2</td>
</tr>
<tr>
<td>Initial Login</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>My Profile</td>
<td>4</td>
</tr>
<tr>
<td>Manage Users</td>
<td>6</td>
</tr>
<tr>
<td>Edit User</td>
<td>7</td>
</tr>
<tr>
<td>Video (Optiflex)</td>
<td>9</td>
</tr>
<tr>
<td>IP Video</td>
<td>13</td>
</tr>
<tr>
<td>Configure E-mail</td>
<td>14</td>
</tr>
<tr>
<td>Configure Mobile</td>
<td>15</td>
</tr>
<tr>
<td>My KeyPad (BlackBerry)</td>
<td>16</td>
</tr>
<tr>
<td>My Keypad (iPhone &amp; iPod touch)</td>
<td>17</td>
</tr>
<tr>
<td>Edit Existing User Information</td>
<td>18</td>
</tr>
<tr>
<td>Event History</td>
<td>19</td>
</tr>
<tr>
<td>Remote Access</td>
<td>20</td>
</tr>
<tr>
<td>System Status</td>
<td>22</td>
</tr>
<tr>
<td>Zone Status</td>
<td>22</td>
</tr>
<tr>
<td>Device Control</td>
<td>23</td>
</tr>
<tr>
<td>Event History</td>
<td>23</td>
</tr>
<tr>
<td>Keypad</td>
<td>24</td>
</tr>
<tr>
<td>User Session Timeout/Logout</td>
<td>25</td>
</tr>
<tr>
<td>Communicating Through Text Messaging</td>
<td>26</td>
</tr>
</tbody>
</table>

©2008 Protection One, Inc. All rights reserved. No part of this document may be reproduced in any manner without the express written consent of Protection One, Inc. All inquiries should be addressed to:

Protection One, Inc.
1035 N. 3rd St. Suite 101
Lawrence, KS 66044

V073109 Copyright © 2008 Protection One, Inc.
Welcome to eSecure from Protection One

eSecure service gives you access to some of the most advanced technology available, integrating your security system into your daily activities with more control and information than ever before. Using the eSecure service through the Access Online Services gateway at www.ProtectionOne.com, you can securely access your security system remotely from the Web browser on your Internet-connected computer. Configure the service to automatically send event notifications to e-mail addresses you designate, and enable remote control of your system with text messages from cell phones and other portable devices.

As an eSecure user, you can manage and operate your security system, check its status, and receive event notifications from almost anywhere in the world. You can also enable other people to manage, operate or receive notifications from your system.

eSecure is rich with capabilities and flexible in supporting tasks with many communication methods:

<table>
<thead>
<tr>
<th>User Task</th>
<th>Communication Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing user profile</td>
<td>Web browser</td>
</tr>
<tr>
<td>Viewing security system status</td>
<td>Web browser or cell phone</td>
</tr>
<tr>
<td>Controlling the security system remotely</td>
<td>Web browser or cell phone (limited control)</td>
</tr>
<tr>
<td>Configuring e-mail and text-message notifications</td>
<td>Web browser</td>
</tr>
<tr>
<td>Viewing the security system event history</td>
<td>Web browser</td>
</tr>
<tr>
<td>Receiving system event notifications</td>
<td>E-mail or text messages to a cell phone</td>
</tr>
<tr>
<td>Receiving video event clips/images</td>
<td>E-mail or Web browser</td>
</tr>
</tbody>
</table>
Logging In
After your system has been activated and registered, you will receive a pair of Welcome text messages containing your Master User login and password (the password is sent separately for security reasons). During your initial login as Master User, you should change your password and verify that all of your account information is correct. You may also wish to enroll your Remote Command (SMS/mobile) devices, add Sub Users and configure e-mail and mobile services. You can access your eSecure service from any computer that has an active Internet connection.

Your eSecure service is provided through Protection One’s Sign On to Your Account gateway, which is found in upper-right area of the home page at www.ProtectionOne.com. To use your eSecure service, choose “eSecure” from the pull-down menu, located in the box, and click the yellow GO button.

You will then see the eSecure home page displayed in your browser. This is where you can enter your username and password into the fields in the Access Remote Control boxes in the upper-right area of the page.

For easy access in the future, you can create a shortcut to ProtectionOne.com on your PC desktop. To do so, put your mouse cursor over the browser address bar, click and drag it onto your desktop.
Introduction
After you log in to your eSecure service site, the first screen you will see is the Introduction page. This page allows you to access the eSecure menu structure. Most of the pages and screens allow you to personalize eSecure to your own preferences. The top-level menu choices are User Guide, Introduction, My Profile, Edit Device Names, Remote Access, Video, Configure E-mail, Configure Mobile, Event History, and Logout. LIVE CHAT and various Protection One service pages are also available near the top of your eSecure service site.

My Profile
This page displays the information for the person who is currently logged into the site. Upon initial login, this should be the first window you access. From this screen, you can change your password and username, both of which must be a minimum of eight (8) characters in length and be a combination of letters (A-Z) and numbers (0-9).

It is also important to make sure that the name, e-mail address and phone numbers listed for the viewer is correct. Each user can update his/her own user information in the My Profile area. Users can update contact phone numbers, contact e-mail addresses, and can add their devices for mobile communication.

Note: E-mail addresses stored in My Profile do not produce e-mail event notifications.
My Profile

If you plan to use the remote, mobile access functions in eSecure, you may enroll such devices by adding their phone number(s) upon initial login, or you may return at any time to add them. Two devices capable of sending SMS text messages are allowed per user. Capable devices include cellular phones, smart phones, PDAs, etc. You may want to verify that your mobile service provider supports SMS Short Code upon which the remote access capability relies.

The top of this screen displays the required user information and the bottom displays the information for enrolled mobile phones for remote access and time preference setting.

If you change settings, or enter or change phone numbers for mobile devices, click on Update Information to add the new information, and confirm the update when prompted. If no changes have been made, select Exit to Main Menu page.

Changes are not saved if you Exit to Main Menu page, unless you have confirmed those changes first.
Manage Users
This screen allows you (as Master User) to create Sub User logins for your eSecure service, grant remote access of your security system to others, and enable and disable those Sub User logins. When you create a Sub User, access is enabled by default. To deny access to a Sub User, you can check the “Disable” check box for that user. In the “Disable” check box, True (checked) = Disabled and False (unchecked) = Enabled. You can also edit existing information for Sub Users.

When adding a user, enter his login information (Username and Password), an e-mail address for contact purposes (not e-mail notification) and his real name and phone number. Click Add User to save the information.
Edit User
To create and save a Sub User login, go directly to the Edit User screen so you can adjust additional settings for the Sub User; you may also return at any time in the future to change Sub User settings. From this screen, you can enable and disable a Sub User’s access, enroll phone numbers for mobile access, determine authority levels, and select the systems the Sub User is able to access. The Master User can see and edit settings for all Sub Users, and the Sub Users can see and edit the settings of other Sub Users if their logins have the authority (set by Master). This screen is organized into several sections.

Required Information: In this section, you can review the user information you entered in the previous screen, such as username, password, e-mail address, etc.

Disable Login: To activate login leave box unchecked.

Mobile Phones for Remote Access: If the Sub User is permitted to use the Remote Command functions, Sub User mobile phone devices are enrolled here. A Sub User may also enroll these devices directly in My Profile, if they have been granted authority to do so by the Master User.
Authority Level: This section allows the Master User to grant the authority levels that he/she wishes the Sub User(s) to have in his/her eSecure service. To grant authority levels, choose the features that you wish to assign from the **Features that may be assigned** window (left side) and transfer them to the **Features that have been assigned** window (right side).

Two of the available features that may be assigned are **E-mail Configure** and **Manage Users**. The E-mail Configure option allows a Sub User to configure e-mail information in order to receive e-mail notices on pre-designated events. The Manage Users option grants authority to add and edit other users. You may assign one, both or none of these options. In most cases, we recommend that Sub Users **NOT** be granted Manage Users authority.

Select MAC for User Authorization: This section allows you to choose which system or systems a Sub User will have access to. Available systems will appear in the User Defined Device Identifier column. To grant access, check the “Authorize” box next to the system you want the new user to have access to. **Selecting global “Authorize” will authorize access to all listed systems.** To save information, click Update Information.
**Protection One eSecure Video**
Clicking the Video option on the introduction-page menu will prompt you to connect to either the Protection One Optiflex or IP Video service. If you had one or more video cameras installed with your Protection One security system, you can use this option to view live video remotely. Click Launch Video System to start the selected application.

**OPTIFLEX**
Once you’ve connected to your cameras, you’ll see them displayed in separate windows in the viewer screen. The P1 Optiflex system allows you to view up to six (6) live video feeds.

**Menu**
By clicking on Select from Menu, you can control many of the settings in the P1 Optiflex Viewer, including which camera views to display, the preset size of those displays, playback, archiving, on-demand recording, video and system setup, streaming preferences and more.

**Preset Size**
Change your video screen(s) by selecting Preset Size option under the Select from Menu. Choose either 25%, 50%, 100% or 200% screen size for custom viewing.
**Playback**
After selecting Playback on your menu, a video player will appear in a separate window. Choose the source from which you Select a clip, the list and click the play button. To help capture the entire event, each clip contains a few seconds of video immediately before the event and a few seconds of video immediately following the event. Freeze the video by hitting the Stop button.

**Clip Archiving**
The Protection One Optiflex controller can store up to 19 video clips of events in its local Flash memory. When a 20th clip is captured, the oldest, unlocked clip in Flash memory is deleted to make room. Up to 100 of your most recent clips are simultaneously stored in the off-site Service Archive, which also deletes the oldest clip when its limit is exceeded. Finally you also have the option to store up to 500 clips on your local PC hard drive, which are permanent files and must be deleted to make room if the limit is exceeded.

**Record Clip**
Use this option to record directly from a camera you are viewing. Simply pull your options down from the Menu and click on the camera from which you wish to record.
Setup
Use this menu option on initial setup or at anytime to make adjustments to your eSecure camera and recording settings, including external monitor viewing, or change your system settings through NTSC Setup (see below). Click OK to save setting changes.

Select System under the Setup menu option for a detailed view of your Protection One Optiflex system settings. For assistance or questions, call 1-800-GET-HELP (438-4357).
Streaming Video
Select Stream under the Select from Menu to view and adjust streaming video. Use this option to select either a higher frame rate or higher quality, clearer images of streaming video. This feature also allows you to select either high bandwidth or low bandwidth Internet connections for maximum performance.

E-mail|Archive
Select from the E-mail|Archive option in the dark-gray bar above Select from Menu. Set up your e-mail notification settings to deliver event-triggered video clips via e-mail and images via mobile phone. Specify the e-mail addresses on your video distribution list, select which cameras are e-mail enabled and which will send whole clips. Set video e-mails to occur at specific days, hours and minutes with the scheduler. Then click Save Email Properties to save your new settings.
**IP Video**

If you have chosen the IP Video option, you will log in to the IP Video viewer. On the viewer, you will see snapshots from your cameras on the right side of the screen and a main viewing window near the middle. To view live video from one of your cameras, double-click on the snapshot that represents the camera you would like to view in the main viewing window.

To close your eSecure IP Video viewer, simply click on the **Close** button at the bottom-left of the viewer window.
Configure E-mail
You may wish to configure e-mail notifications on your initial login. If so, the Configure E-mail page is the next logical place to visit. This screen will enable you (or any authorized Sub Users) to designate the events that will generate an e-mail notification message, the subject and content of a notification, and to whom the notification will go.

Depending on your system configuration, up to eight events can be reported (default settings usually show four, but more can be added if your system supports them). For your convenience, we usually start out with Notification 1 (N1) configured to send e-mail for general Arm and Disarm (Reports On and Off) and N2 configured to send you e-mail when the AC power to your security panel is off (Reports Off). You may have your security panel configured by the Installer to substitute other functions for these Notifications, and/or to send notification about additional events (N3, N4, N5-8).

The configure e-mail page is very flexible, so it can be set to match the actual configuration of your system. It also allows Users with authority to edit the subject and text content of the e-mail notifications according to User preference, to enable or disable the individual notification e-mail for each configured event, and to enroll up to six (6) e-mail destinations for the notifications. Each of the enabled notifications is sent to each of the enrolled notification destinations. If a configured event occurs and the notification for that event is individually disabled in the configure e-mail page, the event is still recorded in the Service History.
Configure Mobile
This screen must be completed by or for every user who plans to use the Remote Command (SMS and/or Mobile Access) features of eSecure. The upper section of this page displays the user-defined system name (Device) that is enabled for SMS/Mobile Access communications. Each system has a “short code,” which is called an **SMS System Abbr Name** in the Configure Mobile page. You can use any SMS system name you prefer; it should be an easy-to-recognize term based on where the system is located or its purpose. We suggest abbreviations such as “Home,” “Office” or other short words, numbers or phrases. The SMS system name can not have spaces in it.

Each user must check the box(es) next to his/her phone number(s) listed to enable Mobile/SMS access from that phone. Each enrolled mobile device may be enabled for SMS Control or enabled for Mobile Control (My Keypad) or both. Each user must accept the **Terms & Conditions** in order to save the information and authorize the SMS/Mobile Access service.

Enter 8-digit number here and same number on Mobile device when validating installation.

Box must be checked to activate phone numbers for SMS communications.

If you choose to use your user Code (on-site keypad code) as your Mobile PIN, check box before installation.

A text message will be sent to your phone. Use the Web browser in your phone to go to the Internet address contained in the text message and the download process will begin. System abbreviation and phone data will saved.

Clicking Save authorizes SMS communications, as well as saves the information.
My KeyPad (Mobile Access)
After you have clicked on the Send Installation URL button, a text message with a Web address will arrive on your device. Use your device’s Web browser to go to that address. Follow the directions to download the keypad application. After you have installed the eSecure keypad application on your mobile device, look for the My KeyPad icon (see Fig.1) and select it to access and control your home or business security system from anywhere.

When logging in to your My KeyPad application, you will first enter your 4-digit Mobile PIN that you designated on the Configure Mobile page. Keeping this PIN confidential will help prevent others from accessing your My KeyPad application. After you have entered the correct Mobile PIN, you’ll be asked to enter your User Code, which is the same 4-digit number you enter on your physical keypad at your home or business. This will connect you to your My Keypad virtual display (see Fig.2). **Note: If you check Mobile PIN is same as User Code” on the Configure Mobile Page, prior to installation on your Mobile Device, you will not be required to enter User Code.**

Once you have entered the correct User Code you will have access to your My KeyPad application functions. The design on the My Keypad interface will vary depending on the make and model of your mobile device.

Select function from your device menu, you can open your Remote Control Functions menu.

Your Remote Control Functions include Disarm, Arm Away, Arm Stay, Bypass, Output On, Output Off and Go to Partition. Just scroll until the desired function command is highlighted and select it. The command will be quickly sent to your home or business alarm control panel as if you were sending it from a physical keypad on the wall. Press the menu button to exit application.
My eSecure Keypad — iPhone™ & iPod touch®
The My eSecure Keypad for your iPhone or iPod touch is an application or “app” and can be downloaded by going to the iTunes store or by the same method you use to download other apps. Once you have downloaded and installed the My eSecure Keypad app, log in to your security system by entering your four-digit Mobile PIN, followed by your user code (same 4-digit code you enter on your physical keypad). Use your My eSecure Keypad like you would use the keypad, or select the Functions button to open a screen that allows you to directly select from a list of common functions. At any time, you may return to the keypad screen. Logging off of My eSecure Keypad is as easy as selecting the Log Off button in the lower-right corner of the keypad interface.
Manage Users

Use the Manage Users page to edit the profile and authority information of an existing user (this is the same Edit User page seen in the initial User Setup process). You can change or update any stored information about an existing User, and you can rescind access. To disable a previously authorized User, check the Disable Login box for that User. When the Disable User box is checked, that particular User is disallowed access to the application. This page displays enrolled Users in a table. Individual User settings can be accessed by clicking on the name of the user in the table view.

Clicking a name opens up the Edit User screen.

Clicking this button will bring up the screen to enter a new user’s information.

Check box to deny access to this application.
Event History
This screen displays a record of events that have occurred in the eSecure service. It includes dates and approximate times. Events are included in the System History, if they are configured in your system, regardless of the Notification Enabled check boxes on the “configure e-mail” page.

Note: If you want to see the alarm signal and event history stored in your system’s local memory, use Remote Access in eSecure to connect to your system. When you connect, you can either use the System Knowledge tab titled Event Log (if your system is 320P1), or use the regular alpha keypad Event Log commands (if your system supports the Virtual Keypad features) to view the log contents.
Remote Access
This screen enables you to access and control your security system using an emulated or **Virtual Keypad**. The emulation is fast and realistic. If your security system is a Protection One 320P1, you may also be able to interact with it through advanced System Knowledge tabs within the Remote Access application. To access your security system, select the name of the system using the drop-down menu. Then click the Launch Keypad button.

Remote Access
When you click the **Launch Keypad** button, the Remote Connect applet window appears on your PC display screen. Click anywhere in that window to start the Remote Connect Applet. **[If your security panel is a model other than Protection One’s 320P1 (including legacy and Commercial Vista systems), you will land on the Virtual Keypad.]** Your system can be operated in the same manner as on a local keypad, except that you **CANNOT** activate functions that require buttons to be pressed simultaneously. In most cases this means you cannot initiate **keypad emergency functions** through the Virtual Keypad. (Refer to instructions in your control panel user guide for operating the system.)

**If your security panel is a Protection One 320P1 enabled for advanced features,** enter your four-digit security system user code on the first security screen. When you then click the **OK** button, you will see a set of System Knowledge tabs near the top of the applet window, and you will land on the **System Status tab**. One of the System Knowledge tabs (to the right side) is the Virtual Keypad described in the preceding paragraph.

In the lower-left corner of the applet window, you can see that your system is currently securely connected to the Internet. If you were to lose remote communication with your system, a message will appear in lower left and indicate the Java applet has stopped, at which point you may attempt to login to your eSecure service again.
If your communicator is a wired-IP connection, you will see **PC-type icons** in the lower left, which, when flashing green, indicates your system is communicating with the service via IP network and Internet.

Although we’re working hard to make sure the eSecure service always performs to your satisfaction, it is possible for unexpected disruptions to occur. If the connection to your security panel is disrupted or if the service can’t connect, you may see “UNABLE TO CONNECT” or “CONNECTION LOST” messages. If that happens, close the applet screen, and click Launch Keypad again. If the problem continues, you may want to wait a few minutes and then try to re-establish the connection.

When you land on the advanced System Knowledge tabs in the applet window and move between tabs, you may notice a few seconds during which information is being refreshed from your system’s records. This brief retrieval process is normal and provides real-time information at your fingertips. The screen below will appear first when you access your security system (with advanced features) remotely.

**Notes:** The first remote session will require an exchange of information between your alarm system and eSecure for configuration purposes. This may take longer than you expected, but there is no cause for concern. Future sessions will connect much more quickly and only contain information about changes.

Remote Access runs on Java, so the current version of **Java must be present on your PC**. A link to the Sun Java Download appears on the bottom of the page. You can follow the Sun Java Download link to check for or install the current version. In some cases, if Java needs to be installed or updated on your PC, you may be prompted to install it. Just follow the on-screen prompts.

Upon initial connection, systems with advanced features display a screen in which your User Code is entered to confirm your identity and authority level to your security system. Systems with Vista Keypad or Quick Secure Keypad display do not require this entry and do not display the screen.
System Status
This screen presents a status overview of several key system functions, including Power, Battery and System, all of which are lit green to indicate if status is ok or normal. This screen also provides a few quick shortcuts for common security system activities and commands, including the ability to arm or disarm the entire system. Most systems operate entirely in the main partition. To have access to multiple partitions, click on the Name Partition sub tab under the main Setup tab, and uncheck the “Show Single Partition” box.

Zone Status
This screen provides a view of all the zones for the system, or in a selected partition. Zones can be bypassed or made active again as desired. Additionally, you can add or edit the eSecure description of a zone. If you edit an existing zone description (descriptions can be edited on the Setup tab), that description will be retained for that zone in Remote Access but will not appear on the system’s local keypads or on the Virtual Keypad. Keypads always display the descriptions programmed into the security panel.

In systems that support Virtual Vista Keypad or Quick Secure Keypad display, zone status is indicated by a green Ready icon that behaves like the green Ready LED on the system’s actual keypad. When the Ready Icon is not lit (one or more zones are not ready), faulted zone can be displayed in the Virtual Keypad display window by the command that would do so on the system’s actual keypad — usually, by pressing the *(Status) key one or more times.
Device Control
This screen displays the current status of output devices (typically control relays and lighting modules) programmed in your security system and enables you to remotely turn them on or off. Simply click on a device to highlight it, and then click the On or Off button below for control. Output device descriptions can also be added/edited in the Setup tab.

In systems that support Virtual Vista or QuickSecure Keypad display, device control relies on keypad commands like those for the system’s actual keypad. Though they are similar, the output control commands vary a bit from system to system. Please refer to the User Guide for your system to see the correct commands.

Event History
This screen allows the user to see the security panel’s log of system

In systems that support Virtual Vista or Quick Secure Keypad display, event history may be available (depending on user authority) by keypad commands like those for the system’s actual keypad. The logged events are displayed in the Virtual Keypad display window as they would be in the system’s actual keypad display window. Though they are similar, the event log commands vary a bit from system to system. Please refer to the User Guide for your system to see the correct commands.

Other Features In systems with advanced features, several additional screens may be available to help you manage the features. A more detailed User Guide that includes information about these screens and how to use them is available after you have logged into your e-Secure account.
Keypad
The Keypad tab enables you to control the security system using an emulated keypad. Functions are performed in the same manner as on a local keypad. If your system is equipped with Custom Alpha keypads, you will find the Virtual Keypads comfortable and familiar. If your system is equipped with Icon display “Fixed English” keypads, you will find Virtual Keypads provides you with significantly more information and control, but you WILL NOT be able to initiate panics. (Refer to your control panel user guide for instructions on operating the system.) Note that you can also use the number keys on your keyboard to perform most actions.
User Session Timeout

If a remote session has been open for 10 minutes without activity, the service will warn the user of impending, automatic disconnection by displaying “Move Mouse over App to stop disconnect.” To stop disconnection, move over or click anywhere on the application.

If, after 10 minutes, activity is not detected, the remote session will disconnect.

Logout

We strongly recommend you take reasonable precautions to preserve the security of your system and service. One way to do this is to ALWAYS LOG OUT of the service when you are finished using it, to prevent another person from passing by your computer and gaining access, should you step away or be distracted.

Another note on security: We also recommend that you NEVER share your login or password, and that you use care in creating and sending Remote Command messages, to help prevent someone seeing your user code by looking over your shoulder, for example. If possible, we recommend you delete Remote Command messages from your phone’s Sent Items (if it has one) and the response messages you receive from your system that may be in your phone’s Inbox if it has one.
Remote Command: Communicating Through Text Messages

To communicate with your security system through text messaging, you must first enroll at least one SMS device (cell phone) in a user profile and enable that device for access to your system in the Configure SMS page of your service. If you have done this and your mobile services provider supports SMS Short Codes, you can send text message commands to operate your security system remotely from the enrolled phone. Your system will respond with a confirmation message to the phone number of the enrolled SMS device that sent the command. The confirmation message includes the command and your system’s response to the command. Most of the time you will see confirmations telling you the command was successfully completed, but occasionally you may ask your system to do something it can’t (arm with a zone open, for example). If the command is not executed successfully and you want detailed information, you will see a short, general explanation of the reason that is consistent with the characteristics of SMS service. You may want to log into your eSecure service from a convenient PC and get the details.

Send Remote Command messages to the “Short Code” 2-5-2-7-6 [A-L-A-R-M on a telephone keypad]. You can store the short code in your phone’s Contacts (if it has this feature) so you don’t have to type it in each time. We DO NOT recommend storing draft or complete Remote Command messages in your phone, because they include your panel’s User Code. In the Syntax Table, Remote Commands are not case sensitive; commands are shown in upper case for clarity.

The Remote Command message format is:

[SMS system name] = This is the SMS system name name for your system, which you created in the Configure SMS page of your eSecure service. It can be as short as one digit and can contain letters and/or numbers but no spaces. We recommend you use something you can remember easily.

[Command] = The Command library includes the most common operations for your system. Commands are single letters, except Arm Stay which is two letters: Arm Away (A), Arm Stay (AS), Disarm (D), Bypass (B), Output (O), Status (S). (See the Syntax Table that follows).

[Code] = This is your four-digit User Code in your alarm panel (not your username or password for eSecure login). In the Syntax Table, the User Code is represented by cccc.

[Number Detail] = Some commands support detail like partition number or zone number. In the Remote Command syntax, the Number Detail is entered following your User Code (separated by a space). In the Syntax Table, Number Details are represented as follows:

zzz = Zone Number Detail. Zone Number Detail is required with the Bypass command. Zone Number Detail is entered as a three-digit number. Enter leading zeroes for one- or two-digit zone numbers (zone 1 is entered as 001).

p = Partition Number Detail. Partition Number is optional with Arm and Disarm commands. Partition Number Detail is entered as a single digit when necessary. Most systems do not operate in multiple partitions, so partition Number Detail is usually not necessary. Without Partition Number Detail, an Arm or Disarm command is applied to all partitions active in the system. For example, a basic Arm command without Partition Number Detail is interpreted as a command to Arm All.
**Output Number Detail** is required with the Output Control command. Output Number Detail is entered as a two-digit number. Enter leading zeroes for one-digit Outputs (Output 3 is entered as 03).

[Action Detail] = Remote Commands to operate Output devices in your system require Action Detail to tell the system what action you want the Output to take. In the Syntax Table, Action Detail is represented as **a**. Output Action Detail can be one of two words:

- **on** = Turn the Output ON.
- **off** = Turn the Output OFF.

Below are the text message command field definitions and their formats.

**A** = Arm Away
Syntax: [SMS system name] A cccc p
If successful, you will receive an Armed Away status message that is time and date stamped.
Examples:  
- **home a 5555**  
  Arm entire system (SMS system name home) to Away using code 5555
- **office a 5555 2**  
  Arm only Partition 2 of system (SMS system name office) to Away using code 5555

**AS** = Arm Stay
Syntax: [SMS system name] AS cccc p
If successful, you will receive an Armed Stay status message that is time and date stamped.
Examples:  
- **home as 5555**  
  Arm entire system (SMS system name home) to Stay using code 5555
- **office as 5555 1**  
  Arm only Partition 1 of system (SMS system name office) to Stay using code 5555

**B** = Bypass/Unbypass Zone
Syntax: [SMS system name] B cccc zzz
If successful, you will receive a Zone Bypassed status message that is time and date stamped, along with general system status.
Examples:  
- **home b 5555 006**  
  Bypass/unbypass zone 6 of system (SMS system name home) using code 5555
- **office b 5555 037**  
  Bypass/unbypass Zone 37 of system (SMS system name office) using code 5555

**D** = Disarm system
Syntax: [SMS system name] D cccc p
If successful, you will receive a Disarmed status message that is time and date stamped.
Examples:  
- **home d 5555**  
  Disarm entire system (SMS system name home) using code 5555
- **office d 5555 2**  
  Disarm only Partition 2 of system (SMS system name office) using code 5555
O = Turn programmed output on/off (letter O, not number zero)
Syntax:  [SMS system name] O cccc oo on / off
If successful, you will receive a Programmed Output status message that is time and date stamped.
Examples:  
  home o 5555 03 on
  Turn ON Output 3 in system (SMS system name home) using code 5555
  office o 5555 07 off
  Turn OFF Output 7 in system (SMS system name office) using code 5555

S = Status Request
Example:  [SMS system name] S cccc
If successful, you will receive a current System Status message. Status includes current Arm/Disarm state, faulted zones and troubles.
Example:  home s 5555
  Request status of system (SMS system name home) using code 5555

Help, H, Info, ?, I = Help Request
This command is a little different from the others because it doesn’t require an SMS system name or a user code – the command itself (Help, H, Info, I or ?) is all that’s necessary. The Help commands request information from the eSecure service instead of a security system. The reply from the service depends on whether the phone that sends the Help command is enrolled as an SMS device or not.

An enrolled and authorized phone will receive the following reply message:
SMS Remote Control Services, Powered by Honeywell Inc.
Key
a = System Abbreviation
p = optional partition #
cccc = user code
For details log onto your account at CMD

a A cccc p = Arm Away
a AS cccc p = Arm Stay
a B cccc xxx = Bypass zone xxx
a D cccc = Disarm
a O cccc xx On/Off = Turn output xx on or off
a S cccc = Get Status
For further details, e-mail us at CustomerService@ProtectionOne.com.

A non-enrolled or unauthorized phone will receive this reply message:
SMS Remote Control Service, Powered By Honeywell Inc.
Text the word “Stop” to opt out of SMS Remote Command service.

For further details, go to www.ProtectionOne.com and click on eSecure in the “Access Online Services” gateway box in upper-right area of the home page, or e-mail us at CustomerService@ProtectionOne.com.

1. A system that is engaged with a Remote Access application session is temporarily unavailable to SMS Remote Control.
2. SMS Remote Control service works properly only after the system has been accessed at least once by the Remote Access application. If changes have been made to the system’s programming or settings, or the system has lost and regained power or been reset, please be sure to access it using the browser Remote Access application before attempting SMS Remote Control.
3. Quick Secure systems do not include zone number in the SMS reply message to an SMS command.
4. Systems that operate on a pure wireless communicator require 2-3 minutes to reset the communicator between SMS commands.
5. From an enrolled and authorized phone, commands can be sent to “Opt Out” or un-enroll the phone from SMS Remote Control service. Opt Out commands are similar to Help commands – they are to the e-Secure service rather than to a particular security system. Stop, quit, cancel, unsubscribe, terminate, or end can be sent through SMS communication to opt out of the service and disable the phone from SMS Remote Command. The service sends a reply message stating that SMS Remote Control services for this cell phone have been terminated. We recommend using the Opt Out commands with caution because they can’t be recalled by the phone after they have been sent.