Personal notification using SMS and email

Introduction

The B5512/B4512/B3512 control panels v2.00 by Bosch introduced the ability for end users of the system to receive emails and text messages directly from the control panel. With enhancements made in firmware v2.01, the personal notification system becomes much more flexible and powerful, allowing security dealers to more effectively tap into this growing market. The B9512G/B8512G control panels fully support Personal Notifications and their enhancements.
This paper describes the configuration options and mechanisms to allow security dealers to understand and to properly select and configure personal notifications.

Technologies

B5512/B4512/B3512 v2.00 utilize a single hardware path for personal notification. The B44x Conettix Plug-in Communicators sends personal notifications via cellular Short Message Service (SMS). The destination of the message is a cellular telephone number or an email address. If using an email address, the SMS text message goes the cellular carrier's SMS-to-email bridge. This server converts the text message to an email and routes it accordingly.

B5512/B4512/B3512 v2.01 and B9512G/B8512G add a new dimension to personal notification. The control panel can directly communicate with the email server using the on-board wired Ethernet, or via a B44x Conettix Plug-in Cellular Communicator.

With the new flexibility comes additional configuration options. Understanding these is critical to finding the most cost-effective and reliable solution to meet your customers' needs.

Reliability

Cellular SMS is a very reliable mechanism in terms of ease of connectivity and uptime. The control panel and the cellular infrastructure have battery backups so personal notifications can be sent even during power outages.
Sending email over Cellular is nearly as reliable as sending an SMS. Note! Any time a 3rd party email server is used, you may experience downtime as a result of that server. Also, the required passwords and rules for sending emails may change, causing a permanent service interruption until the configuration is updated.

Sending email over on-board Ethernet adds another layer of complexity on top of that imposed by the email over cellular. The connection relies on the end users' network infrastructure. This might include low-end network equipment, which is not always protected by battery backup. Any power failure or equipment failure also temporarily affects the ability to send personal notifications. However, most end users rely heavily on their network connection, and are very satisfied with their uptime. Email over on-board Ethernet is reliable for the majority of personal notification needs.

Because on-board Ethernet does not require a Plug-in Cellular Communicator, or a monthly data plan, this is the lowest cost solution.

Side effects of spam

Unwanted spam emails had a huge and lasting effect on our personal notification infrastructure. Whenever an email server or domain (such as "aol.com") was determined to send too much spam, it would be "blacklisted" by other email servers. This meant that whenever somebody from that blacklisted domain or server tried to send emails, the email network outside their organization would discard the email. That resulted in other subscribers using the same internet service provider (ISP) as the spammer being blocked from sending emails.

When legitimate ISPs became blacklisted, they worked extremely hard and fast to stop the source of the spam within their network, and then petitioned to be removed from the blacklist.

In response, ISPs now consistently use security measures to prevent spam from originating within their networks. To use any commercial email system to send email, you must have a username and password, and might need an encrypted connection to the email server.

The configuration of these and the rules they impose may be an inconvenience up front, but once they are properly configured, the systems run reliably.

Mobile phone (cellular) destinations

The most common use of personal notifications is to send a text message to end users' mobile phone (cellular). These messages arrive as SMS text messages, but they do not necessarily originate that way. They might originate as SMS messages or as emails.

SMS to SMS

The control panel can send an SMS message to any mobile phone number, regardless of the cellular carrier. This option is the simplest to configure, and is the most reliable because it is immune to email server changes and spam filtering.

To configure SMS to SMS in Remote Programming Software (RPS), simply enter the mobile phone number as the SMS Phone #, and set the method to the appropriate "Cellular SMS" device.

Email to SMS

The control panel can send emails to customer cellular phones. All major cellular providers maintain an email-to-SMS bridge for this purpose. But the bridge only sends SMS message to the customers of their own network, so the security dealer must know the phone number and cellular carrier of the end customer to use this.

The following table provides the email to SMS configuration for the major US Cellular carriers.

Customer's cellular carrier	**Customer's phone number**	**Associated email**
Verizon	(555) 123-4567	5551234567@vtext.com
AT&T	(555) 123-4567	5551234567@txt.att.net
T-Mobile	(555) 123-4567	5551234567@tmomail.net
Sprint	(555) 123-4567	5551234567@messaging.sprintpcs.com

Most discount wireless providers that resell cellular service under a private label might not work with the above configuration. A quick web search can usually determine whether or not a particular discount cellular provider has an SMS-to-email bridge.

All SMS-to-email bridges use strict spam filtering and the requirements of these may change without notice. Test email to SMS should be offline before using this in control panel configuration.

To configure Email to SMS in RPS, simply enter the phone number as an email address using the table above, and set the method to be "Plug-In Cellular Email", "Bus Device Cellular Email" or "Onboard Ethernet Email". Be sure the email server configuration is correct, as described in the following Email Configuration section.

Email destinations

Some users, including smart phone users, might prefer to receive an email as their notification. These can originate as SMS messages or as emails.

SMS to email

The Bosch Cellular data plans include access to an SMS-to-email bridge. This allows the control panel to send text messages from a B44x Conettix Plug-in Communicator to be sent to end users' email accounts.

The advantage of this is the configuration is trivial on the control panel. To configure, simply insert the plug-in module and enter the email address as the destination. Set the method to SMS, **not** email.

Email to email

The supported control panels can directly email the end users' email addresses. This might be the most cost-effective way to enable personal notifications.

To configure email to email in RPS, simply enter the email address, and set the method to be "Plug-In Cellular Email", "Bus Device Cellular Email", or "Onboard Ethernet Email". Be sure the email server configuration is correct, as described in the *Email Configuration* section below.

Data charges

Sending email from on-board Ethernet

The on-board Ethernet is the most cost-effective way to send emails. There is no charge for sending each email. The only requirement is that the system is configured properly, and the control panel is able to contact the required server through the firewalls. The drawback is the requirement of configuring and maintaining the outbound email account as described in the following *Email Configuration* section.

Sending SMS text messages from the Plug-In Cellular Communicator

The control panels can directly send SMS text messages whenever a Plug-in Cellular Communicator is present and activated.

The Bosch data plans all support SMS service at à la carte rates. Frequent SMS users should choose a plan that includes a monthly bundle of SMS text messages. To prevent overages, please review the terms of the data plan, and configure the control panel to only report events to the end customer at a rate that is within the monthly allotment. Any time the personal notification method of SMS is chosen, SMS text message rates apply.

Sending email from the Plug-In Cellular Communicator

The Conettix Plug-in Cellular Communicator can be used to send emails. This uses the Ethernet data channel rather than the SMS text message. This does count towards your total monthly data byte count, but does not require an SMS text bundle option to be added to the plan.

The billing for sending the email is higher than the size of the received email. The total billing is for establishing a transport layer security (TLS) encrypted socket to an email server, authenticating, sending the email, and disconnecting. This is approximately 17 kilobytes per email, which is far less efficient than sending email as an SMS.

A 100 KB plan can only send 5 emails per month if it is used solely for email. A 2 MB plan can send 120 emails per month if it is used solely for email.

Email configuration

In order to send an email from the control panel (but not an SMS to Email), the email server must be properly configured. This requires only a few pieces of information: an email server name and port number, authentication mechanism, username, and password.

An important item is choosing an email provider that meets your needs. For large security dealers, the information technology department may create the entire infrastructure you require to do this and run a dedicated email server for this purpose. For other dealers it may make more sense to contract a 3rd party email service provider to maintain a dedicated email server. Other dealers may find that a free email may make the most sense. Alternately, you could rely on the end users' internet service providers.

The only requirement of the email server is that it be reachable by the control panel. If the control panel is on an internal corporate network with a strict firewall, the cellular communicator is the best option to reach the public internet. But the corporation may provide an internal email server that can be used directly.

For internally operated or contracted 3rd party email providers, you can get the required configuration directly from the server operators.

To use the end users' own internet service provider is a possibility, but might be a burden for some customers. The end user should contact his internet service provider to create a dedicated email account for his security panel. He must then provide the security dealer the SMTP server information along with the username and password.

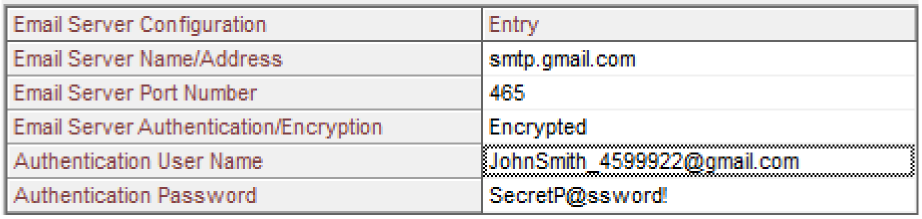
The end user can share his personal email account, without creating a separate one for the control panel; this works, if desired. He must provide his email address and email password to the dealer, and notify the dealer any time the password changes.

Another complication of using the end users' internet service provider is the provider may require inbound connections to originate within their network. Those providers work for on-board Ethernet, but not for cellular technologies. The cellular technologies will originate from an IP address within the cellular network and might be blocked by an email SMTP server that works fine for wired Ethernet.

For all public email providers, the SMTP server information is available on the web. Some sample common server configuration is in the table below.

Provider	SMTP Server URL	Port	Authentication / Encryption
Gmail	smtp.gmail.com	465	Encrypted
Yahoo (unencrypted)	smtp.mail.yahoo.com	25	Authenticate
Yahoo (encrypted)	smtp.mail.yahoo.com	465	Encrypted
Verizon	smtp.verizon.net	465	Encrypted
AT&T	outbound.att.net	465	Encrypted
Comcast	smtp.comcast.net	465	Encrypted
Time Warner	smtp-server.<region>.rr.com	25	Authenticate

For all commercial email providers the username includes the domain name, for example: "JohnSmith_4599922@gmail.com", and the password is the same password used to login and read email over the web. A sample RPS Email Server Configuration using Gmail might look like this:



Email Server Configuration	Entry
Email Server Name/Address	smtp.gmail.com
Email Server Port Number	465
Email Server Authentication/Encryption	Encrypted
Authentication User Name	JohnSmith_4599922@gmail.com
Authentication Password	SecretP@ssword!

For some providers it is okay to share a single account with multiple panels. So you can create a single account alarms_by_joe@freemailsystem.com and configure all control panels to use the same credentials.

For other email providers, including Gmail, there are restrictions to prevent sharing accounts. Each time a new login is detected the user must login to the web and authorize the new access. Once Gmail has detected too many users are actively using the same account at the same time, the entire account may be locked-out for all users. Gmail will work if each control panel has its own Gmail account.