

## Product Overview

janusGATE Mobile filters e-mail between the corporate mail server and smartphones to prevent the delivery of sensitive information to mobile devices.

Enterprises responsible for private and confidential information immediately gain direct control over the risk of information spillage via their mobile phone fleet.

### Highlights

- janusGATE Mobile allows enterprises to provide a secure mobile e-mail solution for its employees.
- Enterprises can implement an effective policy to restrict the flow of sensitive information from the LAN e-mail network to the mobile e-mail network.
- Enterprises are not locked into the use of a specific smartphone device, and can even offer a choice of devices to staff.
- janusGATE Mobile can be easily deployed to existing and new mobile e-mail solutions. It operates independently of smartphone device and network configuration.

### Comply with corporate security policy

janusGATE Mobile operates as a security enforcement point, and segregates the e-mail that is retained within the enterprise's secure local area network from that which is synchronised with its less secure smartphone fleet. janusGATE Mobile can distinguish between devices, users and content to ensure that only appropriate messages are delivered to smartphones.

### Keep communication flowing

If janusGATE Mobile detects that an e-mail containing sensitive information is being delivered to a smartphone, janusGATE Mobile can notify the recipient that the original message is not accessible on the smartphone (Figure 1) and inform the recipient of how to access the original message. Alternatively, if personal or confidential information is detected in a message, such as a credit card number, a tax file number, a social security number or a keyword, that portion of the message can be replaced (Figure 2).

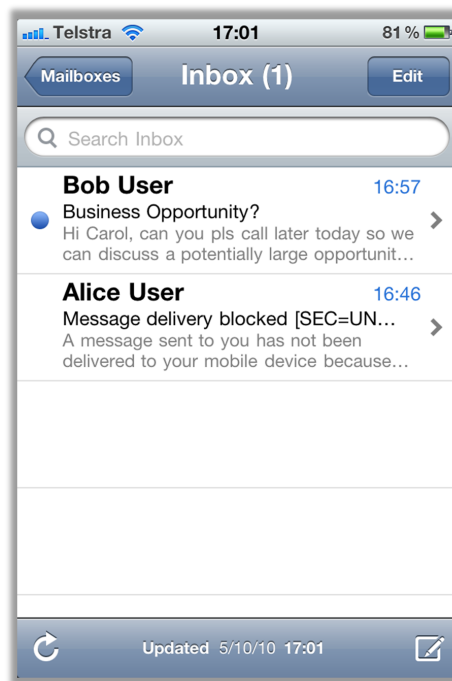


Figure 1: janusGATE Mobile message replacement, as shown on in the iPhone inbox

### Measure risk

Use janusGATE Mobile to measure the amount of sensitive information stored on smartphones. Used in this fashion, janusGATE Mobile does not impact the flow of information delivered to smartphones, but allows assessment and approval of the impact of a mobile e-mail enforcement policy by board and senior executive prior to its introduction.

### Manage Risk

janusGATE Mobile can minimise the risk of leakage by replacing sensitive information prior to its delivery to a smartphone. Messages which are too sensitive to deliver to smart phones can be substituted with notification messages. These messages can be used to notify the recipient that the original message is available (Figure 1). If a credit card number or similar is detected, janusGATE Mobile can replace the number with predefined character (Figure 2).

### Greater employee flexibility

Traditionally, enterprises provide only a single type of smartphone for their employees. As these devices have had to meet minimum security requirements to store sensitive information, the solutions have not been scalable to provide mobile email access for a large number of enterprise users.

janusGATE Mobile allows for a variety of smartphones to be connected to the Exchange Server. A blanket policy can be used for all smart phone types. janusGATE Mobile's rich policy set also allows the policy to be specialised for different devices. For example, if one device type was deemed to be more secure than another, then it would be possible to allow more sensitive information onto that phone.

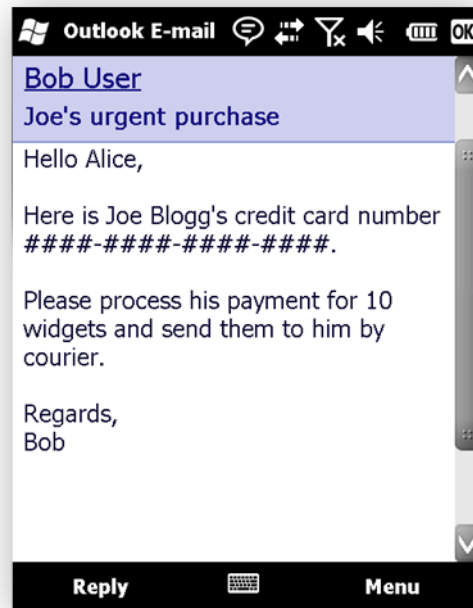


Figure 2: janusGATE Mobile text redaction as shown on a Windows Mobile Pocket Outlook message.

### Maximise usage of existing infrastructure

Enterprises can take advantage of the pool of existing e-mail ready smartphone fleet. janusGATE Mobile allows enterprises to utilise the latent capabilities of these phones, and can boost productivity by simply allowing staff to synchronise contacts, calendar and low sensitivity e-mail between the corporate mail system and their smartphones.

### Advanced detection and processing

janusGATE Mobile can detect and process:

- security classifications in subject lines or in the body of a message
- numeric sequences such a credit card numbers, social security numbers and taxation file numbers
- keywords
- attachment name and extensions

### Easy deployment

janusGATE Mobile is quickly deployed to the Exchange ActiveSync Client Access Server (Figure 3).

The operation of janusGATE Mobile does not affect remaining system configuration. There are no changes to existing firewall rules, nor to smartphone configuration. iPhones, Windows Mobile, Android and Symbian phones operate in their native mode. No additional software is required on these phones. No additional hardware is required. A basic installation can be completed in less than 1 hour.

Installation at the ActiveSync Client Access Server allows for smart phone connection via an external wireless telephone network (for example, 3G or GSM), or via the enterprise's local wireless network (WLAN). In either case janusGATE Mobile intercepts traffic being synchronised to smart phones, and inspects the e-mail traffic.

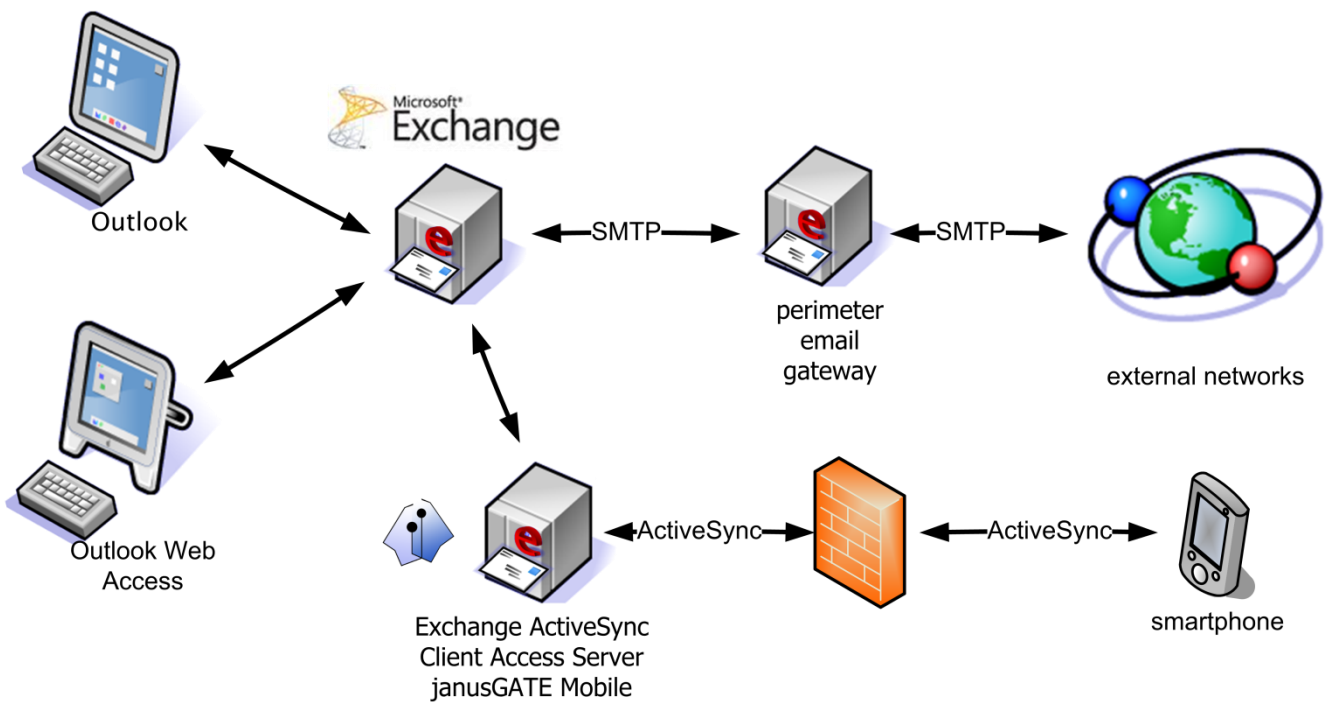


Figure 3: janusGATE Mobile is deployed to the Exchange ActiveSync Client Access Server

## Features and Benefits

Feature	Benefit
Smartphone independent	<p>The enterprise is not restricted to a specific smartphone for its mobile e-mail solution.</p> <p>Diverse smartphone platforms can operate simultaneously. Policies can be specialised to the needs of different groups within the enterprise and to the smartphone platform.</p>
No additional smartphone software	<p>No changes are required on the device.</p> <p>janusGATE Mobile allows for the operation of the native e-mail client on iPhone, Windows Mobile, Android and Symbian smart phones. An Exchange e-mail client is required for Blackberry.</p>
Minimal impact on useability	<p>Users have no loss of expected functionality using the native e-mail client.</p> <p>The majority of messages delivered to phones will be unaffected and operation is transparent.</p>
No changes to smartphone configuration	<p>All janusGATE configuration is managed at the ActiveSync Client Access Server.</p> <p>The enterprise does not need to change configuration in phones that already have ActiveSync e-mail, and does not need to change the connection process for new phones.</p>
Transparent to smartphone network connection	<p>janusGATE Mobile does not interfere with the mechanism used to connect the smartphone to MS Exchange Server. The enterprise can use well known and established security methods such as TLS or IPSec for channel authentication and encryption.</p>
Rich set of conditions and processes	<p>Allows the enterprise to implement a mobile e-mail policy to suit its requirements.</p>

## Evaluate

To evaluate, go to janusNET's evaluation page: [www.janusnet.com/evaluate](http://www.janusnet.com/evaluate), or send an email to [mobile@janusnet.com](mailto:mobile@janusnet.com).

## More Information

web	<a href="http://www.janusnet.com/janusGATE/Mobile">www.janusnet.com/janusGATE/Mobile</a>
e-mail	<a href="mailto:mobile@janusnet.com">mobile@janusnet.com</a>
call	Australia: 1300-795-078 International: +61 2 9962 8141
Head office	75 Miller St, North Sydney, NSW 2060 Australia

## About janusNET

janusNET was founded in 2004 following 11 years of research, development and innovative thinking around security for electronic information.

janusNET develop solutions and manufacture products for companies to enforce security classification policies.

janusNET solutions are deployed globally to both government and private enterprise.

janusNET also support a wide range of desktop productivity tools, with the ability to integrate into other information systems.

