



iPhone and IMAP



IMAP or POP-enabled mail solutions

iPhone supports industry-standard IMAP4- and POP3-enabled mail solutions on a range of server platforms, including Windows, UNIX, Linux, and Mac OS X.

Additional information regarding the IMAP4rev1 standard can be found at www.imap.org.

With support for the IMAP mail protocol, iPhone can integrate with just about any mail server environment. If the server supports IMAP and is configured to require user authentication and SSL, iPhone provides a highly secure, standards-based approach to email deployment. In a typical deployment, iPhone establishes direct access to an IMAP-enabled server over port 993 and access to SMTP servers over port 587. These servers can be located within a DMZ subnetwork, behind a corporate firewall, or both. With SSL, iPhone supports 128-bit encryption and X.509 root certificates issued by the major certificate authorities. iPhone also supports strong authentication methods, including industry-standard MD5 Challenge-Response and NTLMv2.

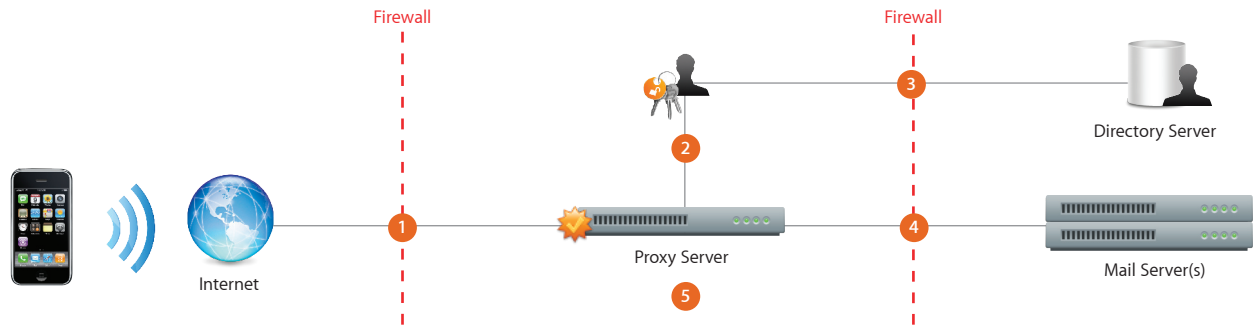
IMAP Network Setup

The IT or network administrator will need to complete these key steps to enable direct access from iPhone to an IMAP-enabled mail solution:

- Open port 993 to allow email to be received through the firewall. The proxy server must be set to IMAP over SSL. SSL ensures that mail is securely encrypted during wireless transmission.
- As a best practice and for additional security protection, install a digital certificate on the server from a trusted certificate authority (CA) such as VeriSign. Installing a certificate from a CA is an important step in ensuring that your proxy server is a trusted entity within your corporate infrastructure.
- Port 587, 465, or 25 must be opened to allow email to be sent from iPhone. iPhone automatically checks for port 587, then 465, and then 25. Port 587 is the most reliable, secure port, because it requires user authentication. Port 25 is considered the least secure because it's been around the longest and is subject to more attacks by hackers. It's also the port that some ISPs block by default to prevent spam.

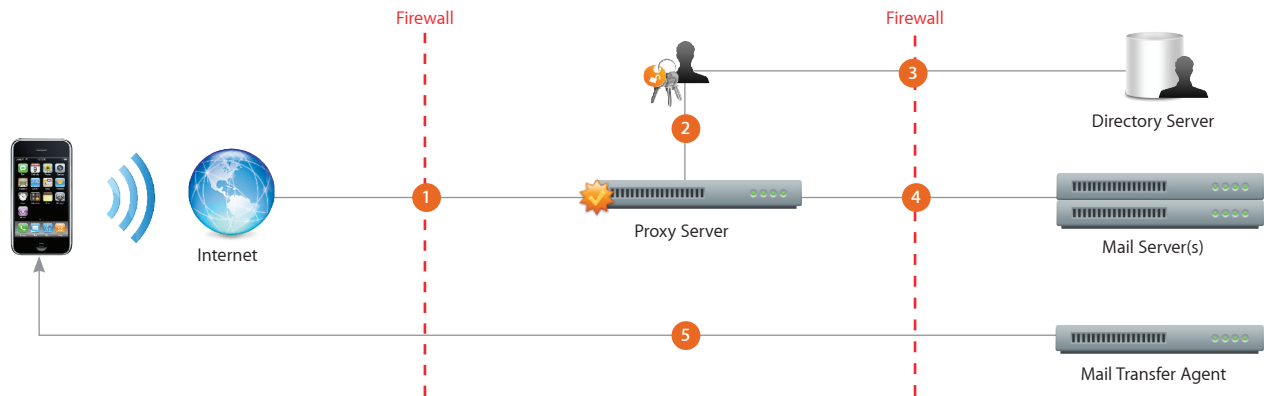
IMAP Deployment Scenario

Receiving email



- 1 iPhone requests access to email over port 993 (IMAP/SSL).
- 2 Next, the iPhone user must be authenticated by the corporate network. This is handled by the proxy server, which functions as a secure gateway.
- 3 The proxy server verifies account information using the directory service.
- 4 Once the user is authenticated, the proxy server routes the request to the mail server.
- 5 Messages and updates are retrieved and sent back through port 993. What the user sees are new messages and inbox updates on iPhone.

Sending email



- 1 Sent email is routed through port 587 (SSL/TLS).
- 2 Send mail requests are then routed through the proxy server.
- 3 The proxy server initiates the authentication process with the directory service.
- 4 Once the user is authenticated, the message is routed through the mail server and a copy is placed in the user's Sent folder.
- 5 The message then goes through the mail transfer agent and is sent through port 587 to the external recipient via SMTP (SSL/TLS).