

**AT&T Wireless
Business Solutions**

**Office Online
Technical White Paper
Security**



Table of Contents

1. INTRODUCTION.....	2
2. OFFICE ONLINE SECURITY FOR USERS.....	2
3. OFFICE ONLINE SECURITY IN THE CORPORATE NETWORK.....	5
4. SUMMARY.....	7

1. Introduction

As the 'wired' world of IP data networks increasingly loses its tethers and becomes mobile, a host of new challenges and rewards emerge. Security is the key to overcoming the challenges and reaping the rewards of data mobilization.

Office Online provides the security for key personal and enterprise data like e-mails, contact lists, and calendars. This service takes advantage of many aspects of existing, commercially available methods for securing data, so that offering mobile access to personal and corporate data is not a security risk. This paper briefly addresses the mechanisms used by Office Online to protect both the data and access to the data within the corporation.

2. Office Online Security for Users

Is Office Online Secure?

Office Online takes advantage of many aspects of existing, commercially available methods for securing data that travels the Internet so that mobile access to corporate data is not a security risk.

Can I use Office Online in my corporate workplace?

Yes. If you have corporate access and permission to download and install applications from the Internet, you can install the Office Assistant and use Office Online to access key e-mail, contacts, and calendar data from your Lotus Notes[®] and Microsoft Exchange[®] solutions via your mobile device.

Does Office Online ensure the safety of my key corporate data?

Your corporate-based e-mail, calendar and contacts are secure.

- All of the communication between the Office Assistant and the Office Online Server through the firewall is secure and encrypted.
- All of your e-mail, contact and calendar data accessed from a wireless device is transmitted using industry standard HTTPS or WTLS and wireless protocol encryption.
- All of your e-mail, contact and calendar data accessed from a PC-based Web interface is transmitted using industry standard HTTPS encryption.

- None of the corporate data you access via Office Online is ever stored outside of the corporate network and firewall. Any personal contact information you choose to import and store in Office Online is done in a secure manner within the highly protected Office Online network.
- Office Online login information (mobile number and PIN) is securely stored in the Office Online Server, never on the mobile device itself.
- Corporate network or mail server login information is never transmitted or stored outside the safety of your corporate network.

If I chose to delegate¹ my Office Assistant to a colleague acting on my behalf, is my e-mail, contact and calendar information protected so that my colleague can't view it?

Yes. Even when a colleague hosts the Office Assistant on your behalf your e-mail, contact, and calendar information remains private and protected for only you to see. You have the ability to disable a colleague's hosting capability at any time.

Is my Office Online user profile including mobile number and PIN safe?

Yes. All login information is securely stored and encrypted at the Office Online network. For additional security, none of your information is stored on your mobile device.

If I lose my mobile device is my network safe from being compromised?

Yes. Office Online does not require you to store your user name or passwords for your corporate network, mail server, or Office Online login on your device. If you lose your mobile device you can immediately end any possible third-party access to your Office Online account by changing your password and/or calling AT&T Wireless Customer Care to temporarily suspend your account. You can always log out from each Office Online session on your mobile device to prevent access in the event of loss.

¹ When you delegate your Office Assistant, a colleague provides a connection to your corporate mail server on your behalf so that you can continue to access your office e-mail, contacts and calendar even when your computer is offline. You should delegate to one or more colleagues to provide this back up connection if you are a mobile laptop user and/or periodically disconnect from the office network.

Now that we have outlined how Office Online protects every aspect of logon and transmission of your corporate e-mail, contact, and calendar data to your mobile device, let's take a closer look at some security aspects of Office Online.

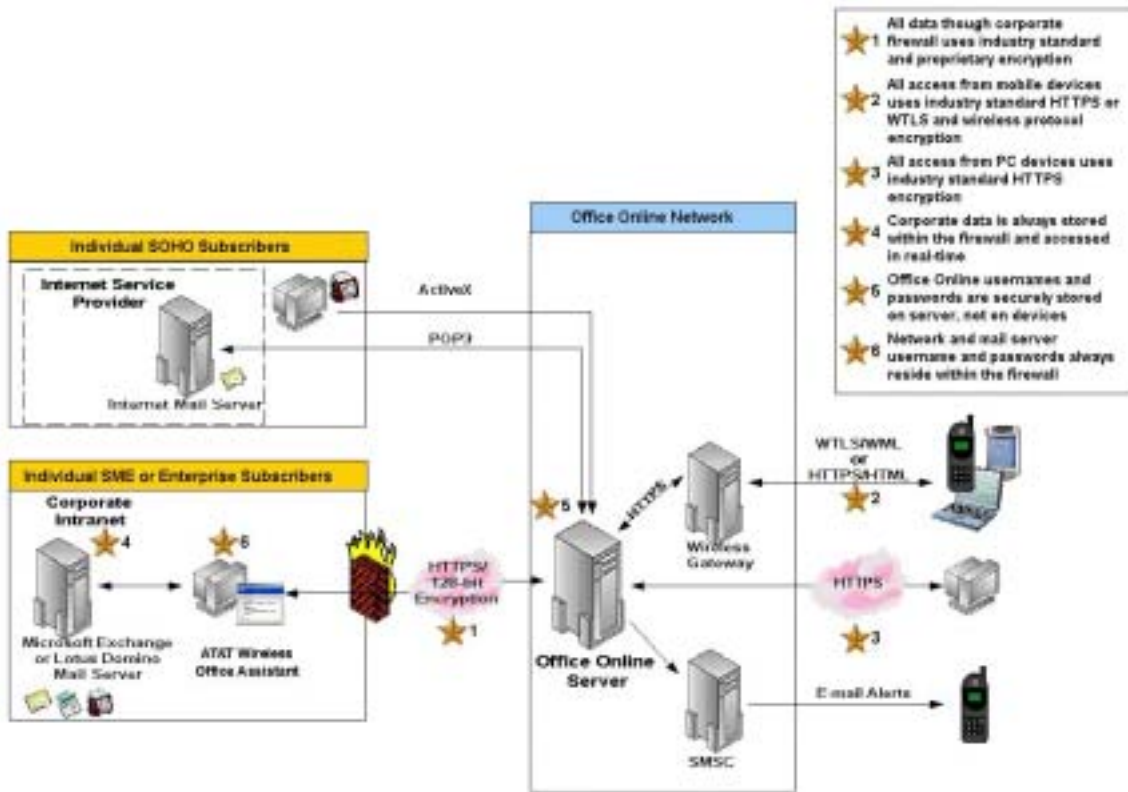


Figure 1

3. Office Online Security in the Corporate Network

At this point it is vital to answer a few more detailed questions about how Office Online fits in your corporate environment from an IT perspective. Unlike dedicated PDA-based solutions that use synchronization or mobile information redirection solutions, Office Online is designed to comply with and further protect an enterprise's data and corporate network integrity. With that in mind it is important to ask these additional questions:

Does Office Online protect my network security perimeter?

Yes. All Office Online data transfer remains secure through an enterprise's network and firewall by using 128-bit encryption through the network's standard outbound-only ports (Figure 1).

Is Office Online data transfer and communication secured?

Yes. Office Online traffic within the network and across the Internet is highly secure and is encrypted using 128-bit encrypted data transfer for all communication between the Office Assistant, the Office Online servers, and the gateway (Figure 1).

Is any of the information accessed by Office Online stored outside my corporate firewall?

No. Accessing corporate data is done in real-time using Office Online's Real-Time Service. It is never compromised by being stored outside an enterprise's firewall protected, private network. In addition, outbound e-mail messages will be routed via the Real-Time Service to the Office Assistant to be sent locally on the corporate local-area network.

After leaving my corporate network, is the data accessed by Office Online protected?

Yes. After the secured data reaches the Office Online network, all data is transferred using industry standard encryption (Figure 1).

After leaving the Office Online network is my corporate data transmitted securely?

Yes. All Office Online data transmission from the Office Online network to wireless devices leverages existing "over-the-air" GSM™ and WTLS Encryption (Figure 1).

Do my network user names or passwords stay within my network and firewall?

Yes. Network mail server logon user names and passwords are never stored or transmitted outside of the corporate network. Only the Office Assistant that is used and secured within the corporate network utilizes a user's credentials (Figure 2a).

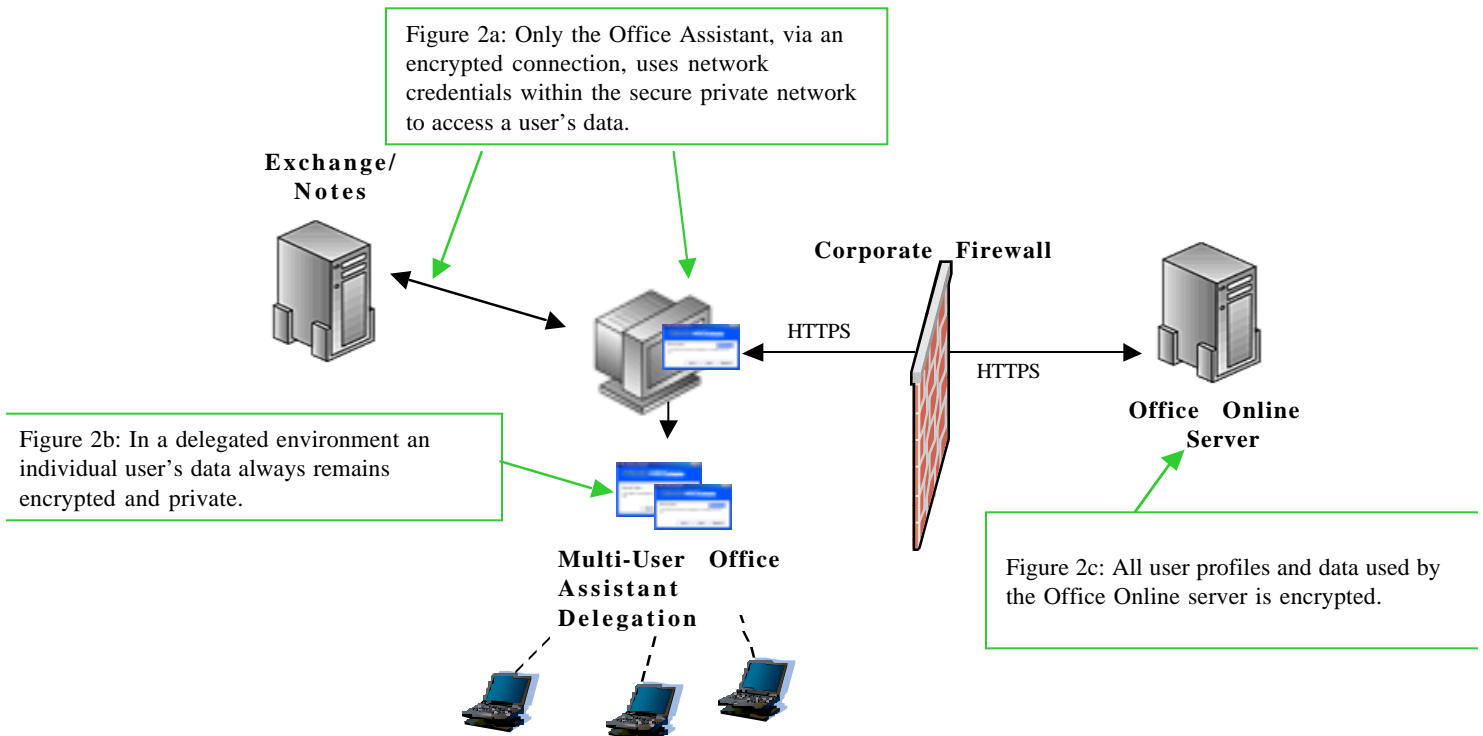
When the Office Assistant is delegated from one of my users to my colleague, is my information protected from being viewed by my colleague?

Yes. In a multi-user Office Assistant environment where other colleagues act as a delegate on your behalf, access to your corporate e-mail, calendar, contacts, user names and passwords remain highly secure and encrypted (Figure 2b).

Are Office Online passwords protected by the Office Online Server?

Yes. Office Online passwords are stored using secure encryption algorithms (Figure 2c).

Figure 2



Does Office Online require storage of critical user information on the mobile devices?

No. Critical information, like login information, is never stored on the mobile device or PC-based Web interface.

If my network users subscribing to Office Online lose their mobile device, is my network security safe?

Yes. There are no significant risks to network or user data from the loss of a device:

- All Office Online user profiles and usernames are stored securely within the Office Online server and not on the device itself so no network access via the Office Online connection can be established.
- Even if your network user didn't log out of the service before losing the device, they can simply change their password via the PC-based Web-UI and/or have the carrier suspend their service.

4. Summary

Office Online provides the security features to safely allow user access to corporate e-mail, contact, and calendar data via mobile devices.

Office Online encrypts data communication, passing it safely through the corporate firewall, across the Internet and through the over-the-air security of the AT&T Wireless network, using SSL and 128-bit encryption.

The protection of all user and network information within the corporate network and within Office Online itself, allows you to maintain the privacy of your critical personal and corporate data. Clearly, Office Online powerfully answers the security requirements for mobile device access to corporate data.