

INFRAGISTICS, INC.

SharePlus Enterprise: Security White Paper

Security Overview

Anand Raja, Gustavo Degeronimi

6/29/2012

SharePlus ensures Enterprise data security by implementing and interoperating with standard security measures.

Contents

| | |
|--|----|
| Introduction | 3 |
| Data Storage Security..... | 4 |
| iOS Data Protection..... | 5 |
| Secure Data Wipe..... | 5 |
| Secure Data Wipe Triggered by Failed Passcode Entry..... | 5 |
| Secure Data Wipe Triggered by “Authentication Time Bomb” | 5 |
| Channel (Communication Security) | 5 |
| Virtual Private Network (VPN) | 6 |
| Secure Sockets Layer (SSL) | 6 |
| Authentication | 6 |
| Windows Integrated Authentication | 6 |
| Form-Based Authentication | 6 |
| Office 365 Authentication..... | 6 |
| Web Login authentication..... | 7 |
| Claims-Based Authentication (CBA)..... | 7 |
| Multi-Factor Authentication | 7 |
| Application-Level Authentication | 7 |
| Passcode Lock | 7 |
| Authorization | 8 |
| Enforcing Business Security Rules by Restricting Specific Functionality..... | 9 |
| Feature Trimming..... | 9 |
| Editor White Listing..... | 10 |
| Trim Copy/Paste..... | 11 |
| Block Screenshot Capture (iOS feature) | 11 |
| Hide lists via Mobile Navigation Settings..... | 11 |
| Mobile Device Management (MDM) Integration | 12 |
| Good Technology MDM | 13 |

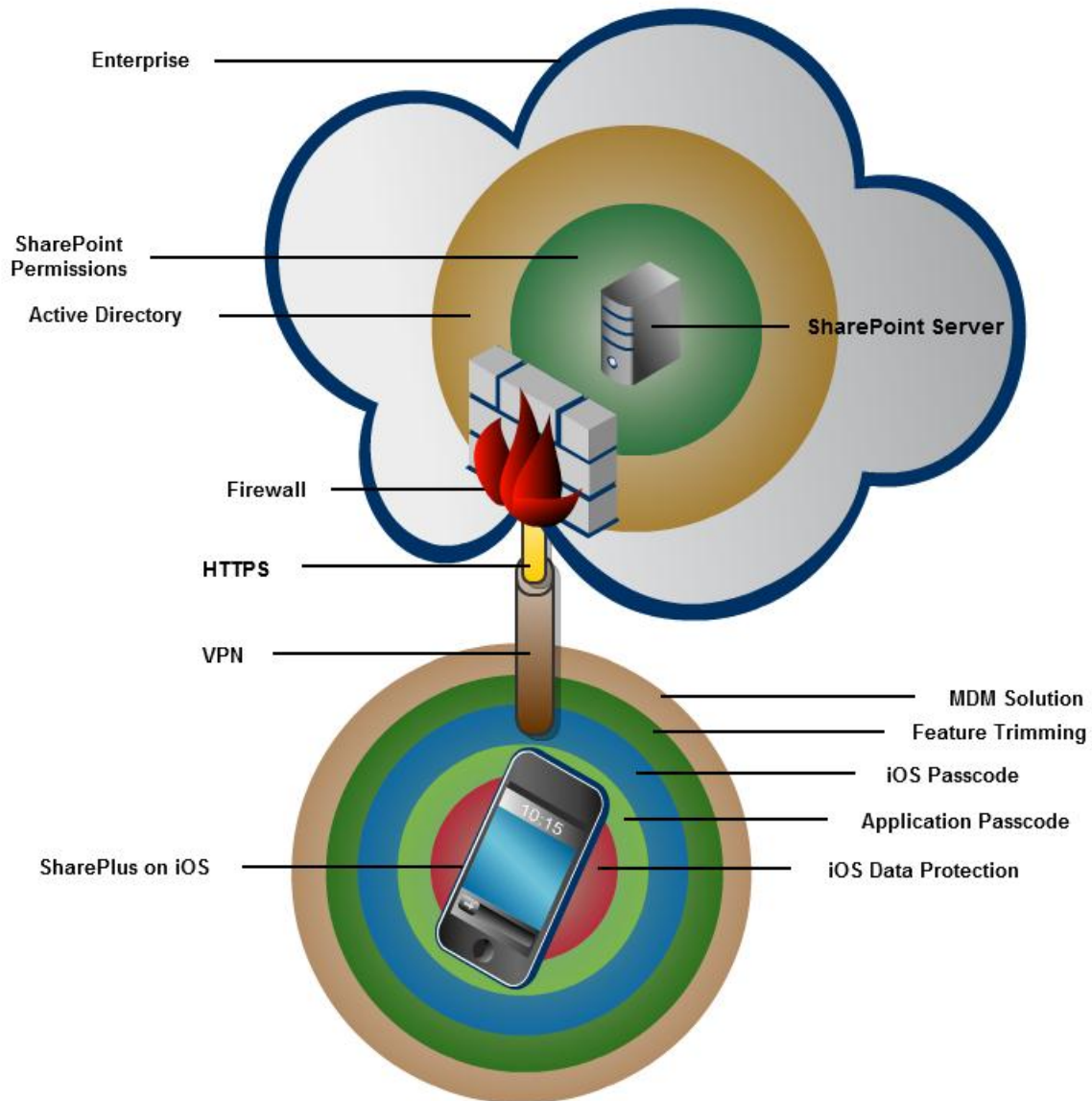
Introduction

SharePlus Enterprise provides secure access to SharePoint sites from mobile devices. Keeping enterprise data secure is the highest priority of SharePlus. To fortify enterprise data security, core security features have been built into the product at each layer.

The following is a list of security features that are included in SharePlus Enterprise for iOS devices. These features will be described in detail in subsequent sections of this document.

- ❖ Data Storage Security
 - iOS Data Protection
 - Data Wipe
- ❖ Channel (Communication) Security
 - VPN
 - SSL
- ❖ Authentication
 - Passcode Lock
 - Authentication Mechanisms
 - Client-side Certificates
 - Two-factor Authentication using one-time Passwords
- ❖ Authorization
 - SharePoint Permissions
- ❖ Enforcing Business Security Rules by Restricting Specific Functionality
 - Feature Trimming
 - Editor White Listing
 - Trim copy/paste (needs customization)
 - Block Screenshot Capture (iOS feature)
 - Hide Lists via Mobile Navigation
- ❖ MDM Integration
 - Standard MDM Solutions (Mobile Iron, etc.)
 - Good Technologies

Figure 1 Typical Enterprise Deployment



Data Storage Security

SharePlus offers two features to ensure that data is secure on a user's device:

- iOS Data Protection
- Secure Data Wipe

iOS Data Protection

SharePlus employs Apple's iOS *Data Protection* feature to keep application data secure. This native iOS feature enhances the built-in hardware AES 256-bit encryption by protecting the encryption keys with a user's passcode. This provides an additional layer of protection for application data such as cached documents and user configuration information.

The iOS Data Protection feature protects data at rest. This includes locking or powering down the device.

Secure Data Wipe

An administrator can configure a secure data wipe to activate upon failed passcode entry attempts or failed attempts to authenticate to the server. An administrator can also initiate the secure data wipe on-demand by issuing a remote wipe command from a Mobile Device Management (MDM) server. MDM integration will be discussed in a subsequent section of this document.

The iOS achieves the data wipe by securely discarding the block storage encryption key from iOS *Effaceable Storage*, which renders all data unreadable.

Secure Data Wipe Triggered by Failed Passcode Entry

SharePlus may be configured centrally to securely wipe all application data upon reaching a configurable amount of failed passcode entry attempts. This feature may be enforced centrally by using the Remote Configuration feature provided by SharePlus.

Secure Data Wipe Triggered by "Authentication Time Bomb"

The *Authentication Time Bomb* feature allows administrators to set a limit on the number of days that a user can use the application without re-authenticating against the server.

This feature is most relevant when users are using offline functionality. In the offline mode, it is possible to work with SharePoint data cached on the device after the user authenticates with the server. The *Authentication Time Bomb* allows an administrator to limit the number of days that the application may be used without re-authenticating to the server. All SharePlus application data will be securely wiped from the device if a user reaches the configurable threshold for failed authentication attempts.

Channel (Communication Security)

SharePlus communicates with SharePoint Server by accessing the out-of-the-box SharePoint Web Services over the network.

Channel security may be enhanced by employing a *Virtual Private Network (VPN)* and/or by using Secure Sockets Layer (SSL) .

Virtual Private Network (VPN)

Organizations often employ Virtual Private Networks (VPN) to enable secure communication over a public network. VPNs enhance communication security by encrypting the data passing through its channel.

SharePlus supports the built-in iOS VPN client. This native client supports the following VPN Tunneling protocols:

- Layer 2 Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)
- Internet Protocol Security (IPsec)

Once the VPN iOS feature has been turned on and a connection is established, SharePlus will utilize the tunnel for server communication. Additionally, the VPN can be set to automatically establish a connection when a SharePlus user attempts to connect to the server. This eliminates the need for the end user to connect to the VPN prior to using the application.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is a cryptographic protocol used to facilitate secure communication over the Internet. SharePlus supports SSL, access to certificate enabled repositories, and *Self-Signed Certificates*.

In the case where an Enterprise site uses legacy encryption methods, SharePlus may be configured to set a matching certificate version.

Authentication

SharePlus supports the following authentication mechanisms:

Windows Integrated Authentication

This authentication mechanism uses Active Directory (AD) credentials to authenticate against the SharePoint site. User credentials are transmitted to the server where they are authenticated against an Active Directory Server.

Form-Based Authentication

In this method of authentication, the user's credentials are passed to the server over HTTP as *Form* data.

Office 365 Authentication

This mechanism is used with SharePoint Servers hosted by Office 365 on the cloud.

When this mechanism is employed, SharePlus renders a browser-like window displaying the Office 365 logon screen. These credentials are then passed to the server for validation.

Web Login authentication

This mechanism has been implemented to support customized online authentication mechanisms such as Forefront UAG and ISA Server. This authentication method behaves in the same manner as Office 365 authentication. SharePlus presents the user with a browser-like window to enter credentials. The credentials are then authenticated by Office 365 services.

Claims-Based Authentication (CBA)

Versions of SharePoint 2010 or higher support this method of authentication. Claims-based authentication is based on concept of an “identity” that works with any Identity System. An Identity is represented by a security token. When a user attempts to obtain access to an application, the user’s security token is passed to the application. CBA provides a trust-based system between applications and a centralized provider that issued the token.

SharePlus versions 3.2 and higher support CBA.

For additional information regarding CBA, please refer to the following White paper:

<http://technet.microsoft.com/en-us/library/hh487289.aspx>

Multi-Factor Authentication

Multi-Factor Authentication methods such as the use of an RSA token is also supported by SharePlus.

Application-Level Authentication

Passcode Lock

SharePlus provides an optional Passcode lock. When enabled, a user will be prompted for a four digit pin upon opening the application. This lock may also be set to activate upon a configurable amount of inactivity. The lock settings may be centrally enforced by an Administrator using global configuration.

Figure 2 SharePlus Passcode Lock



Authorization

User access to SharePoint resources such as lists and documents is granted in SharePoint Server using *permissions*. Since SharePlus authenticates with SharePoint Server's web services using the end user's credentials, server-defined authorization rules apply. Therefore, the level of resource access (read/write, etc.) will mirror that which has been set up on the server.

For additional information regarding setting up permissions in SharePoint Server, please refer to the following article:

<http://office.microsoft.com/en-us/windows-sharepoint-services-help/permission-levels-and-permissions-HA010100149.aspx> .

Enforcing Business Security Rules by Restricting Specific Functionality

Enterprises commonly have a need to adjust application functionality based on security rules. These rules may mandate the restriction of application functionality such as saving a SharePoint document locally or sharing files via the *WiFi Share* feature. SharePlus natively supports this administrative effort through mechanisms that will be discussed in this section.

Feature Trimming

Feature Trimming allows Enterprise administrators to disable and adjust SharePlus features on a global level. This is facilitated by modifying the SharePlus global remote configuration file. This Enterprise-owned and hosted file is used to set application configuration at a global level. When this file is modified to disable a feature, the change will be affected for all Enterprise SharePlus users.

The following list includes, but is not limited to all functional aspects of the application that may be disabled via the *Feature Trimming* mechanism:

- ❖ Site Administration
 - Adding Sites
 - Deleting Connections
 - Updates to Connections
 - Credential Storage
 - Remembering Last User Name
 - My Site Support
 - My Profile support
- ❖ Local Files
 - Copy to Local Files
 - File browser
 - Emailing Documents
 - Swiping Documents
 - Tabbed Previewing of Documents
- ❖ List Management
 - Advanced Search
 - Offline Mode
 - Favorites
 - Displaying Items Count
- ❖ Items Management
 - Add
 - Edit

- Delete
- CheckOut
- Approve/Reject
- Copy URL
- Email URL
- ❖ WiFi Sharing
 - Allow WiFi Sharing
 - Uploading Documents
 - Downloading Documents
- ❖ Open In Functionality
 - Allow
 - Restrict specific third-party application use
- ❖ Printing
 - Allow Printing
- ❖ Enterprise Search
 - Allow Enterprise Search
 - Include Search Scopes
 - Exclude Search Scopes
- ❖ Global Settings
 - Preview Documents On Tap
 - Remove Local Files After Upload
 - Help URL
 - Enable Logging
 - Disable Auto Lock on Preview
 - Disable Device's Auto Lock on Sync
 - Connection Timeout
 - Sync Idle Time
 - User Agent
 - SSL Level
- ❖ Location Services
 - Enable Location Services
 - Auto Start

For additional information on remote configuration, please refer to:

http://blogs.infragistics.com/blogs/anand_raja/archive/2012/05/01/shareplus-enterprise-configuration-overview.aspx.

Editor White Listing

Administrators can restrict third-party editors using *Editor White Listing*. This feature allows administrators to control which third-party editors can be used when editing documents from within SharePlus.

Trim Copy/Paste

Infragistics can implement custom functionality to restrict copy and paste functionality prior to application deployment.

Block Screenshot Capture (iOS feature)

An administrator can modify user profile settings within the device to disable the iOS screen shot feature.

Hide lists via Mobile Navigation Settings

Administrators can hide specific lists by using the *Mobile Navigation* feature of SharePlus. This feature allows administrators to modify the manner in which SharePlus works with a list. These list settings can be set via the custom SharePoint list named "MobileNavigation," which is depicted in the illustration below.

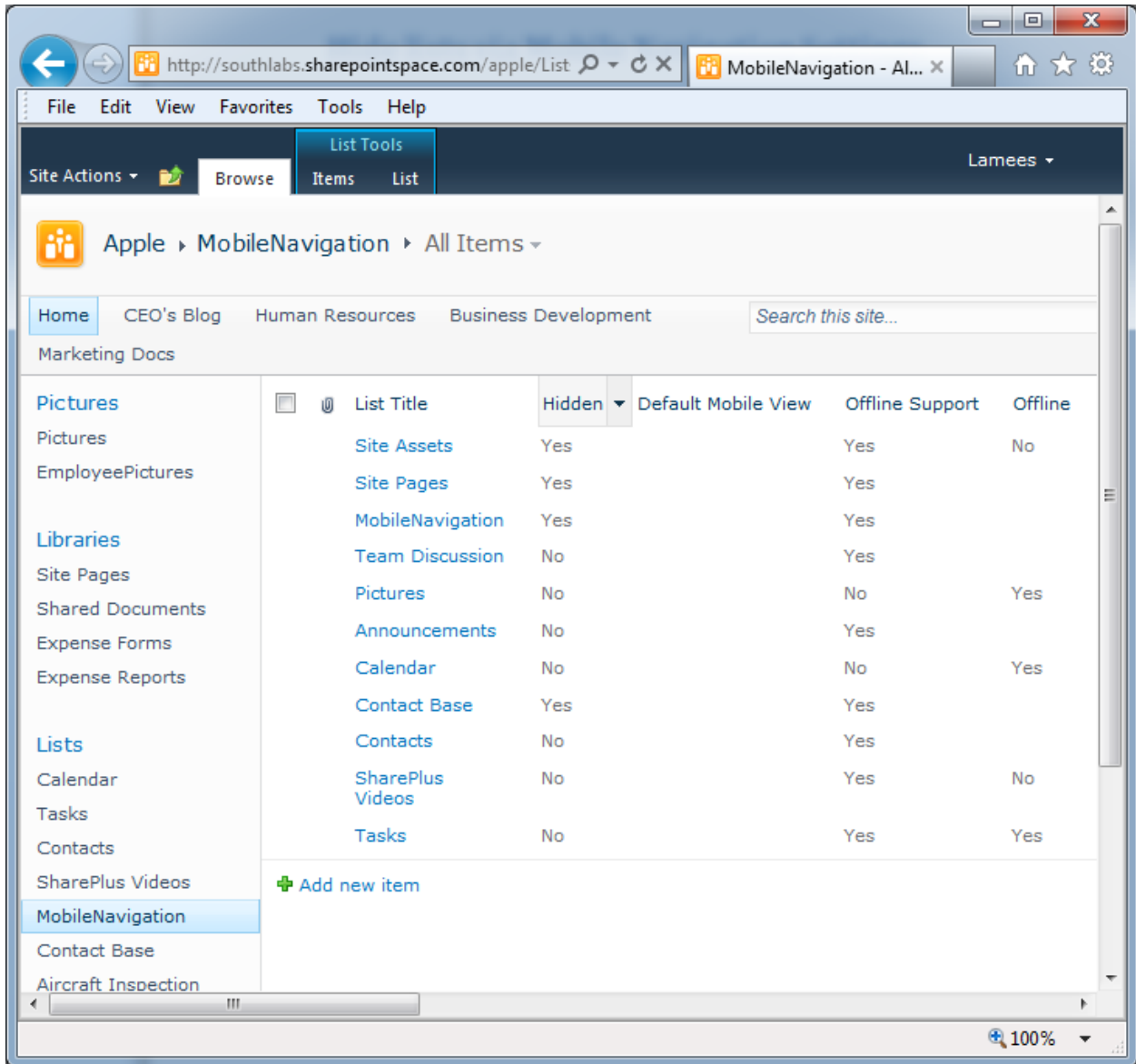


Figure 3

Mobile Device Management (MDM) Integration

Mobile Device Management solutions (MDM) allow the Enterprise to secure, monitor, and manage mobile devices. For additional information regarding Mobile Device Management, please refer to the following article: <http://www.apple.com/ipad/business/integration/mdm/>.

SharePlus integrates with all MDM solutions that implement the device management protocol known as *OMA Device Management*. The Open Mobile Alliance organization has specified this open standard. MDM solutions such as *MobileIron* and *MaaS360* adhere to this protocol.

The following SharePlus-related tasks may be performed by an MDM solution:

- Deployment
- Configuration Broadcast
- Secure Data Wipe

Good Technology MDM

SharePlus also offers advanced integration with the Good Technology MDM solution. In addition to standard MDM integration, the following functionality is available:

- Transmit email using Good Mobile Messaging
- Receive files from Good Native Apps

For additional information regarding Good Technology, please refer to:

<http://www1.good.com/mobility-management-solutions/mobile-device-management>.