Windows Phone

Windows Phone 8.1 Security Overview

Published April 2014

Overview

Organizations of all sizes are expanding their support for an increasingly mobile workforce, making privacy and security essential. Windows Phone is designed with security in mind for users and organizations. The result is a feature-rich, flexible smartphone that uses a holistic approach to security design—a breakthrough for enterprises that need smartphones capable of enterprise-level security, features, and management.

Smartphones help organizations be productive and competitive, but these mobile devices also require increased security vigilance. The pervasive threat of malicious software, or *malware,* and the need to prevent data leakage are two reasons why a thoughtful, comprehensive security design is essential.

Identity and access control are essential parts of any organization's security plan. Windows Phone 8.1 includes highly secure identity features, such as Multi-Factor Authentication (MFA) with virtual smart cards and PINs. These features help keep confidential information secure yet are easy for information workers to use.

Organizations want smartphones that protect data when it is stored and when it is communicated. Windows Phone 8.1 uses a defense-in-depth, multilayered approach that addresses organizational security requirements in numerous ways. Because Windows Phone 8.1 shares many of the same underlying components, including those related to security, as Windows 8.1 and Windows Server 2012 R2 operating systems, it offers predictability, reliability, and commonality in how it can be used and managed. The result is a platform this is unique in today's marketplace.

Note In this guide, *Windows Phone* refers to Windows Phone 8.1 unless explicitly specified otherwise.

Windows operating systems: One platform for security

Windows operating systems can be found on a variety of devices, including desktops, laptops, tablets, convertibles, and smartphones. All current Windows operating systems have a consistent look and feel. Regardless of whether you're using a 32-bit operating system, a 64-bit operating system, or an ARM-based operating system, the user experience is similar.

But the commonality goes much deeper than appearances and user experience. Windows-based devices share many security features that are not only identical in name but increasingly common at a code level. Table 1 lists some of the security features that are common across all current Windows operating systems.

Table 1. Common Security Features in Current Windows Operating Systems

Security feature	Description
Unified Extensible Firmware Interface (UEFI)	UEFI is a standard firmware interface for devices and designed to replace BIOS. For more information about UEFI, see the UEFI sections in the "Trustworthy hardware" and "Boot process" sections later in this guide.
Trusted Platform Module (TPM)	TPM is a standards-based crypto-processor designed to help secure data, enable authentication, and ensure device integrity. All current Windows operating systems support TPM. For more information about this technology, see the TPM section in "Trustworthy hardware" and "Certificate authentication" later in this guide.

Security feature	Description
Data Execution Prevention (DEP)	This defensive technology dramatically narrows the attack surface area for memory related exploits by preventing code from being executable in sections of memory that have specifically allocated for read only data. DEP support is a critically important defense when used in conjunction with Address Space Layout Randomization (ASLR).
ASLR	ASLR automatically protects the system and apps by moving executable images into random locations within system memory. This may prevent, or at least it extremely difficult, for an attacker to exploit vulnerabilities that may be discovered in applications or the platform itself.
Device encryption	All Windows Phone devices support device-level encryption based on BitLocker Drive Encryption technology for data stored on the device. For more information about device encryption, see the section “Internal storage encryption” later in this guide.
AppContainer sandbox	The Windows Phone 8 operating system introduced a sandboxing mechanism called an *AppContainer* that offers fine-grained security permissions and inherently blocks unauthorized access to the system, apps, and data. For more information about AppContainer, see the section “AppContainer” later in this guide.
SmartScreen Filter	The SmartScreen Filter in Windows Phone helps provide anti-phishing protection. If SmartScreen Filter detects malicious content on a site, it can block the site itself or in some cases just specific content on the page. For more information about the SmartScreen Filter, see the section “Internet Explorer” later in this guide.
Remote business data removal	Any organizational information and data can be removed from a device either by IT pros using a Mobile Device Management (MDM) system or by the user. Any personal data stored on the device is retained, such as music, photos, and personal email messages. All apps and data that your organization deployed are removed. For more information about this feature, see the “Device wipe management” section later in this guide.
Virtual smart cards	Virtual smart cards provide two-factor authentication (2FA), which provides stronger authentication than single-factor options like user names and passwords. For more information, see the “Virtual smart cards” section, later in this guide.
Information Rights Management	Information Rights Management (IRM) enables users to fully participate in IRM-protected email conversations and to access IRM-protected documents on their phones. Support for IRM in Windows Phone is based on Windows Rights Management Services (RMS). For more information, see the “Information Rights Management” section later in this guide.
App and programming architecture and model	The app architecture is similar in current Windows operating systems, which means that you developers can write their apps once using secured coding practices, and then use that same code across multiple devices.

A key advantage to these and other common security features in Windows operating systems is the predictability and uniformity of security configuration. You can use the same types of security policies and settings to enforce the same level of security, regardless of the device used.

The security capabilities of Windows operating systems provide an advantage over other operating system families, which often have different security implementations for desktops and laptops versus tablets and smartphones. Windows also offers a common operating system distribution for each hardware vendor and device, whereas competing operating systems may be fragmented into many variations. This lack of consistency in operating system distributions can result in security challenges that just aren't an issue on the Windows platform.

Windows Phone 8.1 security improvements

Windows Phone includes several security-related improvements over Windows Phone 8, as listed in Table 2. These improvements were added based on feedback from customers to make Windows Phone devices more secure, enterprise ready, and yet easy for users to operate.

Table 2. Security Improvements in Windows Phone 8.1

Security improvement	Description
Secured enrollment with MDM systems	Devices can be enrolled with your MDM system by using a simplified and more secure method than with Windows Phone 8. The MDM system and the organization can customize the new enrollment process and use the web authentication broker (WAB) to better secure user credentials. For more information about WAB, go to http://msdn.microsoft.com/en-us/library/windows/apps/hh750287.aspx.
Security policy management	Windows Phone 8.1 includes several new security policies that you can managed through your MDM system. These policy settings are discussed in the section "Security-related policy settings" later in this guide.
Encryption of apps and confidential organizational data on removable storage	Windows Phone 8.1 supports the ability to install apps on a secure digital (SD) card. The apps are stored on a hidden partition on the SD card that is specifically designated for this purpose. This partition is encrypted just like the internal storage and is enabled when the device encryption policy is provisioned to the device through EAS or an MDM. There is no need to explicitly set a policy to get this level of protection. This feature is discussed further in the section "Removable storage protection" later in this guide.
Lock down the phone to a specified set of applications and settings (Assigned Access)	The Assigned Access feature works like the same feature in Windows 8.1, allowing you to define a list of authorized and blocked apps for your devices. This feature is discussed further in the "Assigned Access" section later in this guide.

Security improvement	Description
Support for Secure/Multipurpose Internet Mail Extensions (S/MIME) signing and encryption	Users can now sign and encrypt email messages by using S/MIME signing and encryption support. You can manage the certificate used for S/MIME signing and encryption through your MDM system. This feature is discussed further in the “S/MIME singing and encryption” section later in this guide.
Support for enterprise Wi-Fi connectivity	In addition to the Wi-Fi connections in previous versions, Windows Phone 8.1 supports Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) and EAP-Tunneled Transport Layer Security (TTLS) wireless, certificate-based authentication. This is a stronger authentication than using preshared keys (PSKs) or other Wi-Fi authentication methods. This feature is discussed further in the “Wi-Fi identity and access” section later in this guide.
Support for virtual smart cards	Windows Phone 8.1 supports the use of virtual smart cards to provide 2FA, which provides stronger authentication than single-factor options like user names and passwords. For more information, see the “Virtual smart cards” section later in this guide.
Support for new virtual private network (VPN) tunnel types	In addition to support for the VPN connections in Windows Phone 8, Windows Phone 8.1 introduces support for Internet Key Exchange Protocol version 2 (IKEv2), IP security (IPsec), and Secure Sockets Layer (SSL) VPN connections (the SSL VPN connections require a downloadable plug-in from the VPN server vendor). This feature is discussed further in the “VPN identity and access” section later in this guide.
Automatically initiate VPN connections (auto-triggered VPN)	You can configure Windows Phone to automatically initiate VPN connections when a specific app runs or when a specific domain name is referenced. This feature is discussed further in the “VPN identity and access” section later in this guide.
Remote Assistance	The Remote Assistance feature is designed to help resolve issues that users might encounter even when support personnel don’t have physical access to the device. This feature includes the ability to remotely lock a device, remotely ring the device, and remotely reset the user password (PIN). This feature is discussed further in the “Device access” and “Remote assistance management” sections later in this guide.
Remote business data removal	Any organizational information and data can be removed from a device either by IT pros using an MDM system or by the user. Any personal data stored on the device is retained, such as music, photos, and personal email messages. All apps and data that the organization deployed are removed. For more information about this feature, see the “Device wipe management” section later in this guide.

Each new feature listed in Table 2 helps ensure that Windows Phone devices are deployed secure and stay secure. They help devices stay secure throughout the entire life cycle, as well—from device enrollment to device retirement and all life-cycle phases in between.

Trustworthy hardware

Operating system security in the modern world requires capability that is derived from security-related hardware, and Windows Phone is no exception to that rule. Windows Phone takes advantage of the latest standards-based security hardware components to help protect devices and the information stored on them.

UEFI

UEFI is a modern, standards-based replacement for the traditional BIOS found in most devices. UEFI provides the same functionality as BIOS while adding security features and other advanced capabilities. Like BIOS, UEFI initializes hardware devices, and then starts the Windows Phone boot loader, but unlike BIOS, UEFI ensures that the operating system loader is secure, tamper free, and prevents jailbreaking which can enable an attacker, or even a user, to tamper with the system and install unauthorized apps.

Current implementations of UEFI run internal integrity checks that verify the firmware's digital signature before running it. These checks also extend to any optional ROM components on the device. Because only the hardware manufacturer of the device has access to the digital certificate required to create a valid firmware signature, UEFI has protection from firmware and master boot record rootkits (or *bootkits*). From a security perspective, UEFI enables the chain of trust to transition from the hardware to the software itself (i.e.: Windows Phone platform).

UEFI is required for Trusted Boot, which is described in the section "Trusted Boot" later in this guide.

TPM

A *TPM* is a tamper-resistant security processor capable of creating and protecting cryptographic keys and hashes. In addition, a TPM can digitally sign data using a private key that software cannot access. Essentially, a TPM is a crypto-processor and secure storage place that both UEFI and the operating system can use to store integrity data, meaning *hashes* (which verify that firmware and critical files have not been changed) and *keys* (which verify that a digital signature is genuine).

Among other functions, Windows Phone uses the TPM for cryptographic calculations and to protect the keys for BitLocker storage encryption, virtual smart cards, and certificates. All Windows Phone 8.1 devices include a TPM.

Summary

The modern threats that organizations face require more than software solutions. Trust and security must be anchored in standards-based security hardware. Windows Phone is built on top of just such a foundation, which enables the protection of the Windows Phone operating system, the apps, and the data stored on the device. The trustworthy hardware components that Windows Phone supports include:

- **UEFI.** Help protect your devices from firmware master boot record rootkits (or *bootkits*) by using UEFI. This replacement for a traditional BIOS helps ensure that only trusted software is booted on the device and prevents malware from being booted on the device.

- **TPM.** Perform cryptographic calculations and help protect the public key certificates by using this security processor. You can use the TPM to enhance authentication and identity control by using TPM with virtual smart cards for MFA.

Malware resistance

It is imperative that all devices be resistant to malware, but it's even more important for mobile devices like smartphones. Windows Phone devices are frequently used in public, unsecured places, and thieves and security attackers look at smartphones as easy prey. Windows Phone includes features that help make these devices highly resistant to malware. Each is discussed in later sections.

Boot process

Windows Phone uses some of the same technologies that Windows 8.1 uses to secure the boot process—specifically, UEFI and its Secure Boot component. *Secure Boot* is a feature of UEFI that helps protect devices against malware or other tampering during the boot process.

When a Windows Phone device starts, the firmware starts the boot loader only if the boot loader's digital signature has maintained integrity and the boot loader is signed by a trusted authority that is registered in the UEFI database. In the case of all Windows Phone devices, the Windows Phone boot loader signature is trusted.

For Windows 8.1 operating systems, you can disable Secure Boot. Windows Phone and Windows RT devices are designed to run only their respective operating systems, so Secure Boot cannot be turned off and users cannot load a different operating system.

Trusted Boot

As mentioned in the UEFI section above, UEFI Secure Boot verifies that the boot loader is trusted, and then *Trusted Boot* protects the rest of the startup process by verifying that all Windows boot components have integrity and can be trusted. The boot loader verifies the digital signature of the Windows Phone kernel before loading it. The Windows Phone kernel, in turn, verifies every other component of the Windows startup process, including the boot drivers and startup files.

If a file has been modified (for example, if malware has modified the file to launch malicious code), Trusted Boot protects all of the Windows components and prevents any components that have been tampered with from starting.

System and app integrity

After Trusted Boot has completed the startup process, Windows Phone loads the system components and any apps that are loaded automatically at startup. The system components and apps must be properly signed before Windows Phone will load and start them. If a malicious user or code has tampered with the system component or app files, the corresponding component or app will not be loaded and started.

Unsigned apps are unable to run on Windows Phone, because an app must be signed to be in the Windows Store or be signed with the organization's enterprise development signature. Because all system components and apps must be signed, it is extremely difficult for attackers to run malicious code on a device.

Microsoft security development life cycle

Windows Phone 8.1 is the culmination of many years of effort from Microsoft. With each release, Windows operating systems improve their defense-in-depth implementation for security. The strategy is derived from the Microsoft Security Development Lifecycle (SDL), which ensures that our research and

development teams create software that is secure by design and can eliminate or at least mitigate potential security risks. The use of the SDL has paid big dividends in the case of Windows Phone and has created an environment that contains far less malware than peers such as Apple iOS and Google Android.

Apps

Securing the Windows Phone operating system core is the first step in providing a defense-in-depth approach to securing Windows Phone devices. Securing the apps running on the device is equally important, because attackers could potentially use apps to compromise Windows Phone operating system security and the confidentiality of the information stored on the device.

Windows Phone can mitigate these risks by providing a secured and controlled mechanism for users to acquire trustworthy apps. In addition, the Windows Phone Store app architecture isolates (or *sandboxes*) one app from another, preventing a malicious app from affecting another app running on the device. Also, the Windows Phone Store app architecture prevents apps from directly accessing critical operating system resources, which helps prevent the installation of malware on devices.

Windows Phone Store

Downloading and running apps that contain malware is a common concern for all organizations. One of the most common methods that enables malware to make its way onto devices is by users downloading and running apps that are unsupported or unauthorized by the organization.

Downloading and using apps published in the Windows Phone Store dramatically reduce the likelihood that a user can download an app that contains malware. All Windows Phone Store apps go through a careful screening process and scanning for malware and viruses before being made available in the store. The certification process checks Windows Phone Store apps for inappropriate content, store policies, and security issues. Finally, all apps must be signed during the certification process before they can be installed and run on Windows Phone devices. In the event that a malicious app makes it's way through the process and is later detected, the Windows Phone Store can revoked access to the app on any devices that have installed it.

In the end, the Windows Store app-distribution process and the app sandboxing capabilities of Windows Phone 8.1 will dramatically reduce the likelihood that users will encounter malicious apps on the system.

Note Windows Phone Store apps built by organizations (also known as *line-of-business [LOB] apps*) that are distributed through sideloading processes need to be reviewed internally to help ensure they meet organizational security requirements. For more information, see the "Line-of-business apps" section later in this guide.

You can manage Windows Phone Store apps by using policies that are supported for Windows Phone. These policies allow you to completely disable access to the Windows Phone Store, disable app sideloading, allow or block apps, and other security settings. For more information about these policies, see the "Windows Phone Store and app management" and "Security-related policy settings" sections later in this guide.

Many Windows Phone Store apps require sensitive information from users or may want to access confidential information stored on the device, such as user credentials or the user's physical location. To pass certification, apps obtained from the Windows Phone Store must notify users when such sensitive information or device resources are requested. This notification helps users know when they are granting access to this information.

AppContainer

The Windows Phone security model is based on the principle of *least privilege* and uses isolation to achieve it. Every app and even large portions of the operating system itself run inside their own isolated sandbox called an *AppContainer.*

An *AppContainer* is a secured isolation boundary that an app and its process can run within. Each AppContainer is defined and implemented using a security policy. The security policy of a specific AppContainer defines the operating system capabilities to which the processes have access within the AppContainer. A *capability* is a Windows Phone device resource such as geographical location information, camera, microphone, networking, or sensors.

By default, a basic set of permissions is granted to all AppContainers, including access its own isolated storage location. In addition, access to other capabilities can be declared within the app code itself. Access to additional capabilities and privileges cannot be requested at runtime, as can be done with traditional desktop applications.

The AppContainer concept is advantageous for the following reasons:

- **Attack surface reduction.** Apps get access only to capabilities that are declared in the application code and are needed to perform their functions.
- **User consent and control.** Capabilities that apps use are automatically published to the app details page in the Windows Phone Store. Access to capabilities that may expose sensitive information, such as geographic location, automatically prompt the user to acknowledge and provide consent.
- **Isolation.** Unlike desktop style apps, which have unlimited access to other apps, communication between Windows Phone apps is tightly controlled. Apps are isolated from one another and can only communicate using predefined communications channels and data types.

Like the Windows Store security model, all Windows Store apps follow the security principal of *least privilege.* Apps receive the minimal privileges they need to perform their legitimate tasks only, so even if an attacker exploits an app, the damage the exploit can do is severely limited and should be contained within the sandbox. The Windows Phone Store displays the exact permissions that the app requires along with the app's age rating and publisher.

Operating system app protection

Although applications built for Windows Phone are designed to be secure and free of defects, the reality is that as long as human beings are writing code, vulnerabilities will always be discovered. When identified, malicious users and software may attempt to exploit the vulnerability in the hopes of a successful exploit.

To mitigate these risks, Windows Phone includes core improvements to make it more difficult for malware to perform buffer overflow, heap spraying, and other low-level attacks.. For example, Windows Phone includes ASLR and DEP, which dramatically reduce the likelihood that newly discovered vulnerabilities will result in a successful exploit. Technologies like ASLR and DEP act as another level in the defense-in-depth strategy for Window Phone.

- **Address space layout randomization.** One of the most common techniques for gaining access to a system is to find a vulnerability in a privileged process that is already running, or guess or find a location in memory where important system code and data have been placed, and then overwrite that information with a malicious payload. In the early days of operating systems, any malware that could write directly to system memory could pull off such an exploit: The malware would simply overwrite system memory within well-known and predictable locations.

Because all Windows Phone Store apps run in an AppContainer and with fewest necessary privileges, most apps are unable to perform this type of attack outside of one app. It is conceivable that an app from the Window Phone Store might be malicious, but the AppContainer severely limits any damage that the malicious app might do, as apps are also unable to access critical operating system components. The level of protection AppContainers provide is one of the reasons that their functionality was brought into Windows 8.1 client operating systems. However, ASLR provides an additional defense in-depth to help further secure apps and the core operating system.

- **Data execution prevention.** Malware depends on its ability to put a malicious payload into memory with the hope that it will be executed later. ASLR makes that much more difficult, but wouldn't it be great if Windows Phone could prevent that malware from running if it writes to an area that has been allocated solely for the storage of information?

  DEP does exactly that by substantially reducing the range of memory that malicious code can use for its benefit. DEP uses the eXecute Never (XN) bit on the ARM processors in Windows Phone devices to mark blocks of memory as data that should never be executed as code. Therefore, even if an attacker succeeds in loading the malware code into memory, to the malware code will not execute. DEP is automatically active in Windows Phone because all devices have ARM processors that support the XN bit.

Line-of-business apps

With Windows Phone, organizations can register with Microsoft to obtain the tools to privately sign and distribute custom LOB apps directly to their users. This means that organizations are not required to submit business apps to the Windows Phone Store before deploying them. After registration, organizations (or contracted vendors) can use a validated process to privately develop, package, sign, and distribute apps.

These LOB apps are identical in architecture to apps obtained from the Windows Phone Store. The only difference is the method that is used to deploy these apps and that they are for private rather than public consumption.

Management of these LOB apps is identical to managing Windows Phone Store apps and can be done by using Windows Phone policies. For more information about these policies, see the "Windows Phone Store and app management" and "Security-related policy settings" sections later in this guide.

Potentially, a user could sideload apps onto their device by using a development environment. To disable this ability, use the **Disable development unlock (side loading)** policy in your MDM system.

Company portal

Many MDM systems, such as Microsoft System Center 2012 R2 Configuration Manager and Windows Intune, have a company portal app that allows users to install LOB and Window's Phone Store apps. A company portal app coupled with a properly designed MDM system can help reduce the likelihood of users downloading apps that have malware, because the company portal list only those apps that the organization trusts and has approved.

For more information about app deployment by using an MDM system and a company portal, see the "Windows Phone Store and app management" section later in this guide.

Internet Explorer

Windows Phone includes Internet Explorer 11 for Windows Phone. Internet Explorer helps to protect the user because it runs in an isolated AppContainer and prevents web apps from accessing the system and other app resources. In addition, Internet Explorer on Windows Phone supports a browser model

without plug-ins, so plug-ins that compromise the user experience or perform malicious actions cannot be installed (just like the Windows Store version of Internet Explorer in Windows 8.1).

The SmartScreen URL Reputation filter is also available in Internet Explorer for Windows Phone. This technology blocks or warns users of websites that are known to be malicious or are suspicious.

Internet Explorer on Windows Phone can also use SSL to encrypt communication, just as in other Windows operating systems. This is discussed in more detail in the "Communication encryption" section later in this guide.

Summary

Malware resistance is a cornerstone to a security strategy, and Windows Phone devices are designed from the ground up to mitigate or in some cases even eliminate the potential for the most common malware threats. Windows Phone includes the following malware-resistance features:

- **UEFI and Secure Boot.** Rest easy that malware cannot be introduced during the boot process (bootkits or rootkits). Only trusted, signed software is started and loaded during the startup process. Coupled with UEFI, your devices will be less vulnerable to bootkits and rootkits.
- **Trusted Boot.** When the boot process is secure, this feature helps ensure that all operating system components and drivers are unmodified and free of malware. Any components that have been tampered with will be unable to start on the device.
- **System and app integrity.** This feature builds on Trusted Boot process security by ensuring that all system software (such as Windows services) and apps on Windows Phone are signed and tamper free.
- **Windows Phone Store apps.** Regardless of whether you use apps from the Windows Phone Store or custom LOB apps, Windows Phone helps ensure that these apps are secure. All Windows Phone Store apps are scanned for malware prior to being published in the store.

  Internally developed LOB apps must be signed with the organization's developer certificate, ensuring that no malware can be introduced through unauthorized apps. You can even restrict the apps that are available to users for installation from the Windows Phone Store or completely disable access to the Windows Phone Store, if required by organizational or regulatory agency guidelines.

- **AppContainer.** All apps, and even some system components, on Windows Phone run in an isolated sandbox called an *AppContainer*. Apps running within an AppContainer run with least privilege and can only gain access to resources in a predefined, declarative manner. Apps running in the AppContainer have limited to no access to the system, other apps, or data.
- **Vulnerability mitigations.** Technologies like ASLR and DEP help ensure that malware cannot be injected onto your devices through vulnerabilities that may be discovered later.
- **Internet Explorer.** Browsers are one of the most targeted and common ways to spread malware. Internet Explorer on Windows Phone helps protect the organization's apps and data from attack by using technologies such as AppContainers and SmartScreen.

Information protection

Although it is extremely important to protect the Windows Phone operating system and the apps running on the device, it is even more important to protect the information that these apps access. Windows Phone supports several technologies that help protect this information.

Internal storage encryption

Windows Phone 8.1 performs device encryption, which is based on BitLocker technology, to encrypt the internal storage of devices with Advanced Encryption Standard (AES) 128-bit encryption. This helps ensure that data is always protected from unauthorized users, even when they have physical possession of the phone.

The encryption key is protected by the TPM to ensure that the data cannot be accessed by unauthorized users, even if the internal storage media is physically removed from the device. With both PIN-lock and device encryption enabled, the combination of data encryption and device lock would make it extremely difficult for an attacker to recover sensitive information from a device.

The **Require Device Encryption** policy prevents users from disabling device encryption and forces encryption of internal storage. Additional security can be included when the **Device wipe threshold** policy has been implemented to wipe the device when a brute-force attack on the PIN lock is detected. For more information about this policy, see "Security-related policy settings" later in this guide.

Removable storage protection

Many Windows Phone devices have an SD card slot that allows users to store apps and data on an SD card (the installation of apps on an SD card is a new feature in Windows Phone 8.1). Windows Phone stores the apps on an encrypted SD card partition that is specifically designated for apps. This feature is always enabled, so there is no need to explicitly set a policy to have this level of protection.

The **Disable removable storage card** policy prevents users from using SD cards altogether, but the primary advantage to the new SD card app partition encryption feature is that you can give users the flexibility to use an SD card while still protecting the confidential apps and data on the SD card.

Note Windows Phone stores personal content (like photos and videos) on the SD card in an unencrypted partition so that the user can access the SD card on other devices and share content with others.

If SD card use is enabled, users can sideload apps and upload data from the card. They can use this functionality to install apps that might be accessible by your MDM system, as well, but any apps installed from the SD card must be signed by the Windows Phone Store or your organization's certificate.

Note To sideload an app from an SD card, the device must be unlocked, which you can prevent by setting the **Disable development unlock (side loading)** policy.

For more information about the **Disable removable storage card** policy, see "Security-related policy settings" later in this guide.

Information Rights Management

Windows Phone is one of the few smartphones that offers native support for IRM, enabling users to fully participate in IRM-protected email conversations and to access IRM-protected documents on their devices. Support for IRM in Windows Phone is based on Windows RMS. When IRM is employed, the data in rights-protected documents or email messages is encrypted, and only authorized users can view it. IRM can also be used to limit other rights to a document or message, such as limiting access to Read-only content, preventing anyone from copying content in the document or message, preventing email form being forwarded, or preventing the document or message from being printed.

IRM relies on Windows RMS, a Windows Server–based technology that IT administrators can configure to manage the encryption keys for rights-protected documents. In addition, Windows RMS can be applied to email so that messages can circulate in a protected environment but not be forwarded

outside the organization. Windows RMS can also be applied to documents that are attached to email or stored on Microsoft SharePoint servers, limiting distribution and editing capabilities and helping to prevent information from being leaked to unauthorized personnel.

Organizations can use IRM in conjunction with Microsoft Office 365 services, such as SharePoint Online and Exchange Online. You can enable Windows Azure Active Directory Rights Management for your organization in Office 365 and use IRM just as you would if you had installed Windows RMS on your intranet.

IT can configure IRM by using the **Allow IRM over EAS** policy in your MDM system or Microsoft Exchange Server. For more information about this policy, see the "Security-related policy settings" section later in this guide.

For more information about IRM, see the "Information Rights Management" topic on TechNet at http://technet.microsoft.com/dd638140.aspx.

S/MIME signing and encryption

New in Windows Phone 8.1 is S/MIME support, which allows you to digitally sign or encrypt email messages. The digital signature helps recipients know the authenticity of the sender and that the email message actually originated from the sender. Digital encryption encrypts the content of the email message and can be unencrypted by the authorized recipients only.

Use the following policies in your MDM system or Exchange Server infrastructure to configure S/MIME support in Windows Phone:

- Require signed S/MIME messages
- Require encrypted S/MIME messages
- Require signed S/MIME algorithm
- Require encrypted S/MIME algorithm
- Allow S/MIME encrypted algorithm negotiation
- Allow S/MIME SoftCerts

For more information about this policy, see the "Security-related policy settings" section later in this guide.

S/MIME uses certificates that your MDM system manages or even virtual smart cards to perform encryption and signing. For more information, see "Management" later in this guide.

Communication encryption

Attackers commonly gain unauthorized access to information by viewing unencrypted data sent between devices and the services users access. Windows Phone provides a number of encryption methods for protecting the communication between the device and the services that manage your data, including:

- **Transport Layer Security (TLS) and Secure Sockets Layer (SSL).** Most web-based services use TLS or SSL for secure communication. Windows Phone supports TLS 1.0 – 1.2 and SSL 3.0 to help ensure that all communication is adequately protected.

  Windows Phone ships with several trusted root certificates that can be used with TLS and SSL, and you can easily add new trusted root certificates manually or through your MDM system.

- **VPN.** In some instances, users require access to information that resides on servers on your organization's private intranet. VPN connections are a common method for providing this type of secured access. You can require VPN connection encryption by configuring the VPN servers in your

organization to it. Windows Phone includes support for a number of VPN vendors in addition to Microsoft VPN connections. Windows Phone 8.1 introduces support for IKEv2, IPsec, and SSL VPN connection (the SSL VPN connections require a downloadable plug-in from the VPN server vendor).

VPNs also require user (and optionally device) authentication to help further protect the VPN connection. For more information about using VPNs for identity and access control, see the "VPN identity and access" section later in this guide.

Summary

Protecting confidential information on mobile devices is challenging. Your security plan must account for all possible risks for information loss. Windows Phone has a comprehensive set of information protection technologies that can help protect your information, including the following:

- **Internal storage encryption.** Confidential information in internal storage is encrypted by industry-proven BitLocker encryption. Even if the device is lost or stolen and unauthorized users have physical access, BitLocker helps keep your confidential information confidential.
- **Removable storage protection.** Removable SD cards represent a potential risk for unauthorized information disclosure. You can encrypt a partition on SD cards that contains your organization's apps and data. If the user loses the card or gives the card to an authorized user, the unauthorized user cannot access the data on the encrypted partition. Need more protection? You can completely disable the SD card usage to provide additional protection.
- **Information Rights Management.** Limits data access within documents and email messages to only authorized users within and outside of the organization. This feature brings the same security strength of information protection as the full Windows 8.1 operating system but on a smartphone.
- **S/MIME signing and encryption.** Ensure that the user identity for email messages is secure for messages sent within and outside the organization. Further protect email messages by encrypting the message body and content so that only the designated recipients can read the message's contents. Managing the certificates used in S/MIME signing and encryption is easy through your MDM system.
- **Communication encryption.** Information sent between Windows Phone devices and your services is protected through SSL or VPN connections. These technologies help ensure that snooping or eavesdropping on network connections results in frustrated attackers and no information loss.

Identity and access control

Smartphones are pervasive in most organizations, regardless of whether they are organization-owned or personally owned devices. Most devices have some mechanism for helping to ensure that only an authorized user can unlock and use the device, but this is just the beginning. The apps running on the device need to ensure user identity before they allow access to confidential information. Therefore, identity and access control are of paramount importance for comprehensive security.

Device access

One of the differences between Windows Phone 8.1 and the Windows 8.1 operating system for desktop, laptop, and tablet devices is device access. Windows 8.1 operating systems support multiple user profiles and require that users log on with a managed user identity. Windows Phone 8.1 uses a password (PIN) to access the device and the information on it.

You can use MDM and Microsoft Exchange ActiveSync (EAS) policies to require users to set PINs or passwords and also to configure additional password policies to manage password length, complexity, and other parameters along with additional security functionality.

Windows Phone also supports the following methods of controlling access to devices:

- **Remote wipe.** Support personnel can initiate a remote wipe of the device by using their MDM system or the Exchange Server Management Console. Users can initiate a remote wipe of the device by using Microsoft Outlook Web Access (OWA).

  Note: The remote wipe features listed above are in addition to the ability to perform a software or hardware reset of the device, which wipes the apps and information from it.

- **Remote device retirement.** Support personnel can remotely retire a device. When a Windows Phone device is managed by an MDM system, it enrolls with that system. When the device is retired, all the corporate information, email accounts, VPN connections, Wi-Fi connections, policy settings, apps, and data that the apps deployed are removed by the MDM system.

  Any personal apps or data on the device that the user installed are retained, so device retirement performs a "partial wipe" of the device, leaving only the user data and apps. Users can also retire (un-enroll) their device from the MDM system locally, which has the same effect.

- **Remote lock.** Support personnel can remotely lock a device, which can help in scenarios such as when a user loses the phone and can retrieve it but not immediately (such as leaving the phone at a customer site).

- **Remote password (PIN) reset.** Support personnel can remotely reset the password (PIN) used to unlock the device. This functionality can help when the user forgets their PIN and is unable to access their device. None of the corporate or user data is lost, and the user is able to quickly gain access to their device.

- **Remote ring.** Support personnel can remotely make the device ring, which can help a user locate a misplaced device. In conjunction with the Remote Lock feature, remote ring helps ensure that unauthorized users are unable to access the device if they should find the device.

  After registering their phone at http://www.windowsphone.com, users can map the location of their phone, make it ring, and wipe its data, if necessary.

Windows Phone devices can also be wiped if an unauthorized user attempts to use an incorrect password above a specified threshold. You can specify this threshold by using the **Device wipe threshold** policy in your MDM system or EAS. For more information about device wipe management, see the "Device wipe management" section later in this guide.

Assigned Access

The Assigned Access feature in Windows Phone allows you to control the user experience on a device. Assigned Access allows you to enable a set of specific apps and settings for users, preventing access to all other functionality. You can use this feature to create a single app experience on a device, such as a single app for check-in agents at an airline or a set of apps for retail customer service agents.

You can also control the built-in apps (e.g., phone, text messaging, email, calendaring) so that you can provide only the features you want to be available to the user, helping to ensure that people use the device for its intended experience and purpose. Assigned Access helps secure the device by preventing users from running apps that can be used to share confidential information with unauthorized users. It can also help control access to specific device hardware resources, allowing you to disable specific features on a device that require access to the hardware features that are disabled.

App Allow and Deny Lists

Windows Phone allows you to create a list of approved and blocked apps by using the App Allow and Deny Lists feature. Configure that list through the MDM system by using the **App Allow/Deny list** policy. With this feature, you can control the availability of Windows Phone Store or LOB apps on devices.

Use the App Allow and Deny Lists feature in conjunction with the Assigned Access feature to provide even tighter control of apps. For example, you could use the App Allow and Deny Lists feature to select which apps are available from the company portal in your MDM system. Then, you could use the Assigned Access feature to hide the built-in Windows Phone Store app, thereby forcing users to go through your company portal instead of the built-in Windows Phone Store app.

It is also possible to create a configuration conflict by using both the Assigned Access and App Allow and Deny Lists features. For example, you could allow an app in the Assigned Access feature, and then block the same app by using the App Allow and Deny Lists feature.

For more information about the management of the:

- Assigned Access feature, see the "Assigned Access" section later in this guide
- **App Allow/Deny list** policy, see the "Security-related policy settings" section later in this guide

Virtual smart cards

An important security improvement in Windows Phone 8.1 is the support for virtual smart cards, which are based on the industry-standard smart card solution. Virtual smart cards emulate the functionality of traditional smart cards but use the TPM processor on devices rather than requiring the use of a separate physical smart card and reader.

Virtual smart cards enable users to provide two-factor authentication ("2FA") when accessing resources and work just like their physical smart card counterparts. In many instances, users can use the same virtual smart card on Windows Phone as they are already using for other Windows devices. Users can use virtual smart cards for secure browsing and also for S/MIME signing and encrypting of email messages.

For more information about virtual smart cards, see the "Understanding and Evaluating Virtual Smart Cards" document, available for download at http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=29076.

Certificate authentication

Many apps and remote connectivity solutions use certificates as an additional authentication factor and for signing. Windows Phone supports the use of certificate authentication for:

- **Wi-Fi connections.** Windows Phone supports EAP-TLS and EAP-TTLS authentication for Wi-Fi connections. For more information about Wi-Fi connections in Windows Phone, see the "Wi-Fi identity and access" section later in this guide.
- **Virtual smart cards.** Windows Phone supports the use of virtual smart cards for more secure browsing and also for S/MIME signing and encrypting of email messages.
- **S/MIME signing.** S/MIME signing requires a certificate or virtual smart card that is used to create the digital signature for email messages. For more information about S/MIME signing, see "S/MIME signing and encryption" earlier in this guide.

Windows Phone protects certificates and keys by using the TPM that is built into each device. The TPM can release keys automatically, on demand, or based on a secondary authentication factor (such as a PIN in the use of virtual smart cards).

Most MDM systems allow you to manage certificates throughout their life cycle, including certificate enrollment, renewal, and revocation. Windows Phone uses the Simple Certificate Enrollment Protocol (SCEP) to perform certificate management. SCEP allows you to use the certification authority (CA) of your choice (or as required by the MDM system).

VPN identity and access

Many organizations use VPNs to provide access for remote users. Windows Phone includes built-in support for a number of VPN providers in addition to Microsoft, including Check Point, F5, Juniper, and SonicWall.

Windows Phone includes support for IKEv2, IPsec, and SSL VPN connections, but the SSL VPN connections require a downloadable plug-in from the VPN server vendor. Windows Phone also includes auto-triggered VPN support (similar to the auto-triggered VPN support [see http://blogs.technet.com/b/networking/archive/2013/10/03/automatically-triggering-vpn-connections-and-vpn-diagnostics-enhancements-in-windows-8-1.aspx] in Windows 8.1), and unique VPN connections can be defined on a per-app basis. When the user switches between apps, Windows Phone automatically establishes the VPN connection for that app.

Your MDM system can deploy (push) VPN connection profiles to users, which helps ensure that VPN connections have the appropriate security settings.

For more information about:

- The use of certificates for VPN authentication, see the "Certificate authentication" section earlier in this guide
- Managing VPN connection profiles in you MDM system, see the "VPN management" section in the *Windows Phone 8.1 Mobile Device Management Overview* at http://go.microsoft.com/fwlink/?LinkId=394987.

Wi-Fi identity and access

Users use Wi-Fi connections almost as much as they use their cellular data connections. And with regard to the sheer volume of data, Wi-Fi connections are used to transfer the largest amounts of data more often. Many apps that users run require secured, persistent, high-speed connections to resources, and although cellular data connections continue to improve, they cannot keep pace with Wi-Fi connection speeds. This means that users will prefer to use Wi-Fi connections regardless of whether they are at the office, at home, or in public areas.

Windows Phone 8 can encrypt Wi-Fi connections using Wi-Fi Protected Access (WPA and WPA2) and Wired Equivalent Privacy (WEP). Both of these methods are still available in Windows Phone 8.1, but Windows Phone 8.1 now includes support for Wi-Fi authentication using EAP-TLS and EAP-TTLS, which provide enterprise-class Wi-Fi features.

EAP-TLS and EAP-TTLS require devices to have a client certificate installed on the device. This certificate is used to authenticate the device for wireless connectivity and is typically issued by a CA within your organization. The wireless access points in your organization will deny access to devices that don't have the correct certificates.

The use of client-side certificates dramatically increases the authentication and identity strength for Wi-Fi connections. WPA, WPA2, and WEP are significantly more open to security attacks than Wi-Fi networks that require EAP-TLS or EAP-TTLS authentication.

Of course, the downside to client-side certificates is the management of those certificates. Fortunately, you can manage client-side certificates through your MDM system. A properly designed MDM system can deploy the certificates to devices.

In addition to managing certificates for EAP-TLS and EAP-TTLS authentication, you can use your MDM system to perform the following Wi-Fi–related management tasks:

- Provision Wi-Fi profiles, which include the service set identifier (SSID), even if it's hidden, and any PSKs.
- Prevent a device from being used as a Wi-Fi hotspot.
- Prevent users from manually adding Wi-Fi profiles and connecting to untrusted hotspots.
- Prevent users from routing traffic through Wi-Fi connections (*Wi-Fi offloading*).

You can control all of these tasks by using security policies configured in you MDM system, and then applied to your Windows Phone devices. For more information about Wi-Fi–related security policies, see the "Security-related policy settings" section later in this guide.

Summary

Verifying user identity is essential to security. In fact, without properly identifying users, all other parts of security become ineffectual. When the user's identity has been established, you want to ensure the user has access only to the apps and services that you specify. With Windows Phone, you can accurately identify users and then control their access to apps and services by using the following technologies:

- **Device access.** Ensure that only authorized users have access to your devices. In the event that a device is lost or stolen, support personnel or the user can remotely wipe the device. And, notwithstanding those levels of protection, if an unauthorized user enters the wrong password over a specified number of time, the device automatically performs a wipe.
- **Assigned Access.** One of the primary problems facing organizations is how to ensure users are only using devices for intended purposes. With Assigned Access, you can help ensure that users can only run the apps you desire.
- **Virtual smart cards.** Multi-factor authentication ("MFA") helps strengthen any identity authentication system. Virtual smart cards provide users with 2FA that helps prevent unauthorized users from compromising your identity and authentication systems.
- **Certificate authentication.** Certificates have long been used as a method for providing MFA for devices, especially for Wi-Fi connections. With Windows Phone and your MDM system, you can automatically manage the certificates used for client authentication with minimal effort. This extra level of security helps ensure that only authorized devices can access your Wi-Fi networks.
- **VPN identity and access.** Users are able to seamlessly and securely access resources on your organization's private intranet with no user interaction by using auto-triggered VPNs.
- **Wi-Fi identity and access.** Minimize concerns about unauthorized Wi-Fi access within your organization's private intranet by using EAP-TLS and EAP-TTLS authentication for Windows Phone devices. These certificate-based authentication protocols help ensure that only authorized Windows Phone devices can access your organization's internal wireless networks.

Management

Deploying any device in a secured configuration is relatively easy. Keeping the device secure throughout the balance of the device's life cycle is much more difficult. Windows Phone provides extensive security-management features that allow you to manage the key security aspect of devices centrally while allowing users to be productive and access the apps and information they need.

Software updates

If your organization doesn't use an MDM system, you can use the Windows Phone Update service to deliver Windows Phone updates to users. Microsoft manages and distributes feature updates and improvements that are developed by hardware manufacturers, mobile operators, and the Windows Phone engineering team. These updates include software updates for the Windows Phone operating system and for the apps on the device (such as Microsoft Office apps).

Assigned Access management

Assigned Access allows you to enable a specific set of apps and settings for users, preventing access to all other functionality. You can use this feature to create a single app experience on a device, such as a single app for airline check-in agents at an airline or a set of apps for retail customer service agents.

App Allow and Deny Lists management

To manage this feature, define a list of authorized and blocked apps for your devices by using the **App Allow/Deny list** policy. Windows Phone uses these lists to determine which apps it allows to run and which it does not. You can authorize or block apps based on:

- **The app publisher name only.** Authorize or block all apps from a specific app publisher.
- **The app product ID only.** Authorize or block a specific app by the app product ID, which is a globally unique identifier assigned to the app.
- **A combination of app publisher name and product ID.** Authorize or block a specific app by the app product ID for a specific publisher name.

Note There is one list that includes the apps that are allowed and another, separate list for apps that are blocked.

Each of these lists is sent in XML format to Windows Phone devices and contains an XML element for:

- Each publisher name that is authorized or blocked
- Each product ID that is authorized or blocked
- A product ID within a publisher element that is authorized or blocked for a specific publisher

Device wipe management

A *device wipe* removes all the apps and information on a device and returns the device to factory settings. A device wipe can be initiated:

- **Remotely by supported personnel.** Support personnel can use an MDM system or the Exchange Server Management Console to remotely initiate a wipe of a managed device that is lost or stolen.
- **Remotely by a user.** Users can remotely wipe their device by using OWA for devices that EAS manages or by using self-service portals on the MDM system. Users can also remotely wipe devices that EAS does not manage by going to windowsphone.com.
- **Locally by a user.** Users can perform a hardware reset of their device, which will wipe it.
- **Automatically when someone enters the wrong password too many times.** If an unauthorized user enters the wrong password too many times, an automatic wipe of the device is initiated. You can set the threshold for the number of wrong password attempts allowed by configuring the **Device wipe threshold** policy.

When a device has been enrolled in an MDM system, you can retire the device, which removes all information, email accounts, VPN connections, Wi-Fi connections, policy settings, apps, and data used by the apps that the MDM system has deployed. Retiring a device does not automatically wipe the entire device: Any personal apps or data (such as photos or music) and email accounts that the user

created are retained on the device. So, device retirement performs a “partial wipe” of the device, leaving only the user data and apps.

Policies available for managing device retirement include:

- Disable MDM un-enrollment
- Disable MDM software and hardware factory reset

For more information about the policies used to manage device retirement (un-enrollment) in Windows Phone, see http://go.microsoft.com/fwlink/?LinkId=394996.

Remote assistance management

When users encounter problems, it is rarely in the office. Most of the time, they experience problems when they are in remote locations. A comprehensive security management system needs to help provide remote user support.

Windows Phone includes the following remote management features that can help keep devices and information secure:

- **Remote lock.** Support personnel can remotely lock a device. This ability can help when a user loses the phone and can retrieve it but not immediately (such as leaving the phone at a customer site).
- **Remote password (PIN) reset.** Support personnel can remotely reset the password (PIN) to unlock the device, which helps when users forget their PIN and are unable to access their device. None of the corporate or user data is lost, and the user is able to gain access to their device quickly.
- **Remote ring.** Support personnel can remotely make the device ring. This ability can help a user locate a misplaced device and, in conjunction with the Remote lock feature, help ensure that unauthorized users are unable to access the device if they find the device.

These remote management features can be performed by using your MDM system management console or the Exchange Server Management Console.

Windows Phone Store and app management

Management of access to the Windows Phone Store and apps on Windows Phone is essential to securing devices. Without this management, users could download any number of apps from the Windows Phone Store or sideload any app they desired. Most organizations want to manage the apps that are in use on devices, especially for organization-owned devices.

You can use any of the following methods to manage Windows Phone Store access and apps that run on devices:

- **Disable access to the Windows Phone Store.** You can entirely disable access to the Windows Phone Store by using the **Disable Microsoft Store** policy. Set this policy in your MDM system. If your MDM system has a company portal app or you use your MDM system to publish all your apps, consider setting this policy.
- **Publish apps through an MDM system.** Sometimes, more is not necessarily better. Most organizations have a set of approved apps that they want to allow on devices, especially for organization-owned devices.

You can limit the apps available to users through your MDM system. Most MDM systems have a company portal app that allows you to present users with a list of apps that are available for installation. Also, most MDM systems allow you to make apps mandatory.

- **Restrict which apps users can install and run on devices.** The App Allow and Deny Lists feature in Windows Phone allows you to define a list of apps that are allowed or blocked on a device. The Assigned Access feature allows you to also restrict the apps that are able to run to a specific list. For more information about these features, see the "Assigned Access" and "App Allow and Deny Lists" sections earlier in this guide.
- **Disable Internet Explorer.** If users should not have browser access, you can disable Internet Explorer by using the **Disable Internet Explorer** policy. Set this policy in your MDM system.

For more information about the:

- Policy settings for managing Windows Phone Store access and restricting apps, see the "Security-related policy settings" section later in this guide
- Management of the Windows Phone Store and apps by using an MDM system, see the *Windows Phone 8.1 Mobile Device Management Overview* at http://go.microsoft.com/?linkid=9845666

Security-related policy settings

Windows Phone provides policy settings that you can use to configure security (shown in Table 3). Configure these policy settings by using your MDM system or the Exchange Server Management Console and EAS. Some policy settings you can use both MDM and EAS to configure; other settings you can configure only by using an MDM system. Yet another subset of the settings only EAS can configure.

Note To provide comprehensive management of Windows Phone, ensure that your Windows Phone management solution supports the management of MDM and EAS policies.

Table 3 lists the security policies that MDM and EAS support.

Table 3. MDM and EAS Security Policies

Policy	MDM	EAS
Simple password	X	X
Alphanumeric password	X	X
Minimum password length	X	X
Minimum password complex characters	X	X
Password expiration	X	X
Password history	X	X
Device wipe threshold	X	X
Inactivity timeout	X	X
Device encryption	X	X
Disable removable storage card	X	X
Disable Camera	X	X
Disable Bluetooth	X	X

Disable Wi-Fi	X	X
Disable Location	X	
Disable NFC	X	
Disable Microsoft Account	X	
Disable roaming between Windows devices	X	
Disable custom email accounts	X	
Disable screen capture	X	
Disable share and save as	X	
App Allow / Deny list	X	
Disable Microsoft Store	X	
Disable development unlock (side loading)	X	
Disable Internet Explorer	X	
Disable Internet Sharing over Wi-Fi	X	
Disable Wi-Fi Off loading	X	
Disable Manual Configuration of Wi-Fi Profiles	X	
Disable Wi-Fi Hotspot reporting	X	
Disable mdm un-enrollment and soft factory reset	X	
Disable Wi-Fi credential sharing	X	
Lock screen notification controls	X	
Disable telemetry data submission	X	
Email body truncation size		X
HTML email body truncation size		X
Require signed S/MIME messages		X
Require encrypted S/MIME messages		X
Require signed S/MIME algorithm		X
Require encrypted S/MIME algorithm		X
Allow S/MIME encrypted algorithm negotiation		X
Allow S/MIME SoftCerts		X

For more information about each of these security policy settings, see http://go.microsoft.com/fwlink/?LinkId=394987.

Direct Push firewall configuration

For Direct Push to work through a network firewall, TCP port 443, which is required for SSL, must be open between the Internet and the Client Access server. As part of the firewall configuration, the network idle connection timeout must be set. (The network idle connection time-out value indicates how long a connection is permitted to persist without traffic after a TCP connection has been fully established.)

The firewall session interval must be set to allow the heartbeat interval and enterprise session interval to communicate effectively. If the firewall closes the session, mail would be undelivered until the client reconnects, and the user could be unsynchronized for an extended period of time. By setting the firewall session timeout to a value that is equal to or greater than the idle timeout value on the mobile operator's network, the firewall will not close the session.

Microsoft recommends setting the idle connection timeouts for the firewall as follows:

- Mobile operators should set the idle connection timeout values on outgoing firewalls to 30 minutes.
- Organizations should set timeout values on their incoming firewalls to 30 minutes.

Web servers, network security appliances, and system network stacks have several time-based thresholds that are intended to insulate them from insufficiently tested or malicious clients. You should be able to safely increase the idle connection time-out value setting without compromising the security of the network.

Exchange secure mail and authentication configuration

To help protect outgoing and incoming data, deploy SSL to encrypt all Exchange Server traffic. You can configure SSL security features on an Exchange Server instance to help prevent Internet-based server spoofing and other types of attacks. Exchange Server, like any web server, requires a valid server certificate to establish SSL communications.

By default, when the Client Access Server role is installed, EAS is configured to use either Basic authentication or Certificate-Based authentication with SSL. EAS runs on an Exchange Server instance on which the Client Access Server role is installed. This server role is installed with a default self-signed digital certificate. Although the self-signed certificate is supported for EAS, it isn't the most secure method of authentication. For additional security, consider deploying a trusted certificate from a third-party commercial CA or a trusted Windows Public Key Infrastructure CA.

You can save a digital certificate to a file and install the certificate on a Windows Phone device. You might need to install a digital certificate on the Windows Phone device if EAS is required to use SSL and your organization uses a certificate that isn't from a trusted commercial CA.

For more information about using SSL for server authentication, see the "Configuring SSL and Exchange ActiveSync" topic on TechNet at http://technet.microsoft.com/en-us/bb430752(v=exchg.141).aspx.

Summary

Keeping Windows Phone devices and apps secure is an important part of an overall security strategy. Windows Phone has extensive security-related management features that help reduce the effort to secure your devices. These security management features include:

- **Software updates.** You can rest assured that your devices and apps are always current with the latest software updates.
- **Assigned access management.** You can control which apps users can run on their devices, down to a specific app publisher, a specific app, or a specific app for a specific publisher.

- **Device wipe management.** In the event that a device is lost or stolen, you can remotely wipe devices to help ensure that unauthorized users are unable to access your confidential data.
- **Remote assistance management.** Users will always receive the help they need in locating a lost device, wiping a device (if they are unable to locate it), or resetting their password (PIN) no matter where they are located.
- **Windows Phone Store and app management.** Users will only be able to download and install the apps that you want to run. You can even limit or disable user access to the Windows Phone store.
- **Security-related policy settings.** Feature-rich policies help ensure that you can configure your Windows Phone devices and apps to comply with security policies established by your organizations and any regulatory agencies. All of these policy settings can be centrally configured so that you have total consistency of security policies and settings across all Windows Phone devices.
- **Direct Push firewall configuration.** Ensure your firewalls protect your digital assets while ensuring that you can push updates directly to Windows Phone devices.
- **Exchange secure mail and authentication configuration.** Protect more than just the phone and the apps. Protect the network traffic between your devices and your Exchange Server infrastructure. SSL encryption helps ensure that all your confidential information sent by email stays confidential.

Conclusion

Microsoft organized its efforts for Windows Phone security around three simple areas: protecting the device against threats, protecting data, and securing access to resources. With Windows Phone 8.1, Microsoft decided to make an unprecedented level of investment across each of these areas so that we could address the threats of today and tomorrow.

With those investments, Microsoft has been able to deliver malware resistance capacities that literally start from the moment users turn on their Windows Phone devices and continue to help protect the device and software until they retire the device. Microsoft requires all certified devices to support new hardware-based security technologies like UEFI to help maintain device integrity and TPM to protect data and secrets on the device. With these investments and Windows technologies such as Trusted Boot, Windows Phone has made it possible to significantly reduce the possibility of bootkits and rootkits from starting. Improvements to the Windows Phone core, application model, and Internet Explorer reduce the risk of a variety of attacks that malware has used to gain elevated privileges and attack the system and data. It's now much more difficult to exploit and compromise Windows Phone devices, which is proof that Windows Phone is an industry leader in malware resistance.

Windows Phone offers several critical improvements to storage protection. In addition to being able to encrypt internal storage, Windows Phone 8.1 now enables the encryption of corporate apps and data that are storage removable SD cards. Users can further protect information sent in emails by using S/MIME signing and encryption. IRM allows organizations to restrict access to confidential information, even when unauthorized users have access to the physical file.

Extensive improvements in identity and access control help ensure that only authorized users can access devices and the information the device manages. Virtual smart cards and client-side certificates add string or even Multi-Factor authentication, which strengthens authentication for a number of scenarios. And now, devices can authenticate with Wi-Fi connections by using EAP-TLS and EAP-TTLS.

Finally, Windows Phone supports an extensive set of policies that help ensure that a device deployed in a secure configuration stays secure. You can centrally manage these policy settings by using an MDM system. Improved remote management allows organizations to remotely wipe information from the device in the event the device is lost or stolen, and Windows Phone is an excellent choice for Bring Your

Own Device initiatives, as it can manage your organization's apps and data separately from the user's apps and data. You decide how best to manage devices, given the usage scenarios and your organization's security requirements.

All of these reasons make Windows Phone 8.1 a superior choice for secured smartphone devices. To check out the depth and breadth of Windows Phone 8.1 devices, visit http://www.windowsphone.com. Evaluate using an MDM system to manage Windows Phone by downloading a free trial of System Center 2012 R2 Configuration Manager or subscribing to a free trial of Windows Intune. See how you and your mobile users can spend more time being productive and less time worrying about security problems.