



# Microsoft Intune privacy and data protection overview

March 2018

## Privacy and data protection overview

The Microsoft Intune service can help organizations manage and secure mobile devices, applications, and PCs across Windows, Windows Phone, Apple iOS and MacOS, and Google Android platforms. Because it is cloud-based and hosted in Microsoft's data centers, Intune requires no additional infrastructure, but organizations can use the service to extend existing management infrastructure into the cloud. In addition to enhancing device security by providing update and policy management, Intune can help organizations give employees access on their own devices to the apps and resources they need, making Bring Your Own Device (BYOD) programs a reality.

Relying on Microsoft Intune to manage organizations' devices requires trust, but before customers give that trust, they want to know the answer to questions like:

- Who can access their data and how it is it used?
- Where does Microsoft store their data?
- How is their data secured in the data center and on the move?
- Is the privacy of their data assured, and who owns the data?
- What organizations have independently verified Microsoft Intune?

Microsoft takes its responsibility to protect customers' data seriously, and we are committed to providing the answers you need to trust Intune. We have applied our many years of cloud and on-premises experience with security and privacy to our management of Intune.

This white paper offers an overview of how we help secure your data and protect its privacy. Of course, the technical details in this white paper are subject to change, but our commitment to the protection of your data and devices will not waver.

## Physical security

Security for the service starts in the data center. The Microsoft Cloud Infrastructure and Operations Group (MCIO) delivers the core infrastructure and foundational technologies for Microsoft's more than 200 online businesses, including Bing, Hotmail, MSN, Microsoft Office 365, Xbox Live, and the Microsoft Azure platform. MCIO hosts Microsoft Intune in its data centers, which are strategically located around the world. It brings all of this experience to Intune.

# Microsoft Intune

MCIO controls personnel physical access to data centers by using two-tier authentication, including proxy card access readers and biometric readers. On a quarterly basis, a Microsoft security officer sends reports to personnel with authority to approve data center access. Authorized personnel regularly review the list to verify that all people on that list still require access and have the least privileged access level necessary to perform their job functions.

Respected non-Microsoft registrars and accreditation organizations regularly audit MCIO data centers in support of multiple industry and regulatory certifications. The complete list is located on the Microsoft Trust Center website, categorized by service offering.

Microsoft recognizes that security is an ongoing process, not a steady state. Therefore, experienced and trained personnel constantly maintain, enhance and verify our infrastructure. We use up-to-date software, hardware technologies, and processes for designing, building, operating, and supporting our services. To learn more about MCIO, visit <http://www.microsoft.com/datacenters>.



## Personnel security

Security starts with people, and Intune is no exception. Beginning with the hiring process, all Microsoft employees and contingent staff with access to customer data go through standard background checks as permitted by law. For U.S.-based personnel, this includes a review of candidates' education, employment, and criminal history. In addition to standard background checks for all new personnel, personnel must undergo additional background checks if they are to have access to customer data or manage key

physical or logical access controls. Background checks are re-performed on a regular cadence for any employees or contingent staff with access to customer data. To protect the privacy of its employees and subcontractors, Microsoft does not share the results of background checks with customers.

Security awareness, data protection, and privacy are key topics of this training. Microsoft also requires that all personnel complete business conduct training each year.

We follow principles of segregation of duties and least privilege. Although physical access to data centers is

# Microsoft Intune

generally limited to MCIO staff, select Microsoft Intune personnel have logical access to the Microsoft Intune service and data hosted in the data centers. Employees are accountable for their handling of customer data. Microsoft enforces this accountability through a process that includes system controls, such as the use of unique user names, role-based access, and multi-factor authentication. As with physical access to the data centers, we review logical access periodically to help ensure that only appropriate access is granted to relevant customer data, such as contact information, machine details, and user information.

## Architecture security

The following sections offer an overview of security for architectural components, including:

- Client installation and enrollment on PCs
- Mobile devices, such as smart phones and tablets
- Account, Administrator, and Company Portals

- Identity and authentication
- Microsoft System Center Configuration Manager

### Client installation and enrollment on mobile devices and PCs

Each mobile platform uses their own proprietary processes and security models to help secure client installation on mobile devices. For example, the security measures of the Windows Store, Google Play, and Apple App Store contribute to the security of the client software. Microsoft follows the rules each store has set up for publishing our Company Portal apps into them.

For Android, iOS mobile devices and Windows Phone, Microsoft uses Secure Sockets Layer (SSL) to help secure communication between each device and the Intune service. Intune communicates with iOS devices by using the Apple Notification Service. Intune uses a certificate, which the administrator must download

from the Apple Push Certificates Portal, to talk to the Apple Mobile Device Management service. For current versions of Windows Phone, the Windows 10 Push Notification Service is used and for Android devices, Google Cloud Messaging is used. For more information about planning and setting up management of mobile devices, see the following article: <https://docs.microsoft.com/intune/device-enrollment>.

The PC enrollment process is documented in the article "Manage computers with Microsoft Intune" at <https://docs.microsoft.com/en-us/intune-classic/deploy-use/manage-windows-pcs-with-microsoft-intune>.

Only a customer's Intune administrator can use the Administrator portal to download client software. End users with existing Intune accounts can download and install client software from the Company Portal after they



Client installation on PCs



Mobile devices



Account Administrator, Company Portals



Identity, authentication



System Center Configuration Manager

complete the self-enrollment process.

Client installation requires elevated permissions, which helps protect the PC from malicious installation. (You can deploy the client software to standard users by using Group Policy or an electronic software distribution [ESD] system like System Center Configuration Manager.) If organizations choose to distribute the client software by using a file share or an ESD system, they should take steps to prevent unauthorized access to it (for example, use access control lists to secure it).

## Mobile Application Management

Microsoft Intune allows you, as the IT admin, to manage the mobile apps that your company's workforce uses. This functionality allows Admins to perform a variety of App management capabilities, including protecting company data in Apps with App protection policies. To learn more about App-based conditional access with Intune, see the following article:

<https://docs.microsoft.com/intune/app-based-conditional-access-intune>

## Account, Administrator, and Company Portals

Intune provides the following portals:

**Azure Management portal** This portal provides the service and user account management interface to the Intune online service. The account Administrator uses this portal to manage user accounts, user groups, domain names, passwords, if configured, and subscriptions for the Intune service. The Admin can also set policies and enrollment rules.

Learn more about Microsoft Intune in the Azure portal in the following articles:

<https://docs.microsoft.com/intune/what-is-intune>

<https://docs.microsoft.com/intune/ui-changes>

**Company portal** Users can see machine status, download software, and contact their company's IT support through the web-based Company Portal. To access the Company Portal, a user must be granted access by the administrator and enroll their device.

Additionally, a Silverlight console application/portal exists to support legacy Windows PC client management capabilities.

All three portals use SSL to secure communication with the web browser. Sessions have

an inactivity timeout—that is, after a period of no activity, the user's session is ended, and the user must sign into the portal again.

**NOTE** Organizations can configure the Remember Me option in Active Directory Federation Services (AD FS) to automatically sign users in for a specific time frame. This configuration supersedes the total timeout in Intune.

## Identity and authentication

Intune uses Azure Active Directory (Azure AD) as its authentication platform. To provide users with a single sign-on (SSO) experience, businesses can connect their on-premises directories with Azure AD. The Intune administrator then adds users to the Intune user group, giving them seamless access to Intune when they sign into the corporate network. There are two options for authentication when connected to Azure AD: Federation with AD FS and Password Sync. With AD FS, users' credentials never leave the domain network while with Password Sync the hash of users' passwords is synchronized to the cloud. the domain network while with Password Sync the hash of users' passwords is synchronized to the cloud.

# Microsoft Intune

**Use the latest directory integration tools from Microsoft** in order to configure single sign for Intune. For more information about connecting on-premises directories to the cloud, see the article at <https://docs.microsoft.com/azure/active-directory/connect/active-directory-aadconnect>.

**For organizations that do not want single sign on**, they can create cloud only users and administrators in Azure AD.

## System Center Configuration Manager

Organizations can integrate Intune with System Center Configuration Manager. This combination helps provide a unified device management solution that focuses on users and the variety of devices they employ to get their work done.

In this hybrid configuration, the Configuration Manager site initiates all communication with Intune to push or pull data to the service. For example,

Intune queues messages for System Center Configuration Manager, and the site uploads or downloads them. Intune does not initiate communications with System Center Configuration Manager. All communications are over SSL. An Intune certificate is installed with the Intune Connector role and the site uses that certificate to authenticate and communicate with the connector. Intune client software is not aware that Intune is using a hybrid configuration. The data flow is the same whether the client software is installed on a PC or a mobile device, but the data being distributed to the device depends on the feature being used (e.g., software distribution versus policy enforcement).

## Privacy

Customer Data is defined as "all data, including all text, sound, video or image files, and software that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service." For example, this includes inventory information from managed devices or apps which have been installed through Intune. Customers can access their own Customer Data at any at any time and for any reason without assistance from Microsoft. Microsoft will not

## Data flow between the on-premises site and Microsoft Intune

**From Microsoft Intune to the System Center Configuration Manager site** Data that Intune delivers to System Center Configuration Manager includes detailed inventory information that devices report, such as installed apps and hardware characteristics. Intune packages and forwards this information to the System Center Configuration Manager site. System Center Configuration Manager maintains the detailed information about organizations' devices and users in the customer's own data centers.

**From the System Center Configuration Manager site to Microsoft Intune** The System Center Configuration Manager site uses the Intune Connector to upload relevant data and policies to the Intune service.

When necessary, Intune caches data for optimal transport (for example, caching data for mobile devices when using metered connections). The service flushes data from the cache after a set period.

# Microsoft Intune

use Customer Data or derive information from it for advertising. We will use Customer Data only to provide the service or for purposes compatible with providing the service.

It is ultimately up to our customers to evaluate our offerings against their own requirements, so they can determine if our services satisfy their regulatory needs. We are committed to providing our customers detailed information about our cloud services to help them make their own regulatory assessments.

Microsoft does not create customer accounts; the customer creates the accounts either directly in Intune Administrator Console, or in their local Active Directory,

where the accounts can then be synchronized into Azure Active Directory. For this reason, the customer remains responsible for the accuracy of the user accounts they created.

Microsoft provides a coherent, robust, and transparent privacy policy that emphasizes customer data ownership. The Microsoft Online Services Privacy Statement tells you how we handle and use data gathered in your company's interactions with the Intune service. You can view this Privacy Statement at <http://go.microsoft.com/fwlink/?LinkId=512132>.

The following list summarizes Microsoft's position on customers' privacy:

**Control:** We will put you in control of your privacy with

easy-to-use tools and clear choices.

**Transparency:** We will be transparent about data collection and use so you can make informed decisions

**Security:** We will protect the data you entrust to us through strong security and encryption.

**Strong legal protections:** We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.

**No content-based targeting:** We will not use your email, chat, files or other personal content to target ads to you.

**Benefits to you:** When we do collect data, we will use it to benefit you and to make your experiences better.

Intune enables customers to publish company privacy statements to their end users.

For more information about customizing company privacy statements, see the article "Start using Microsoft Intune" at <https://docs.microsoft.com/intune/company-portal-app#company-contact-information-and-privacy-statement>.



# Microsoft Intune

Additionally, Intune meets the EU-U.S. Privacy Shield standard, which is an agreement between the United States and the European Union that enables organizations to self-certify compliance with data protection requirements regarding the collection, use and retention of data to allow legal data transfer from the EU to the U.S. In addition to being certified under EU-U.S. Privacy Shield, Microsoft offers Intune customers EU "Model Clauses" which are standardized contractual clauses that provide contractual guarantees around transfers of personal data leaving the European Economic Area (EEA).

## Data protection

Intune collects customer data only to provide and troubleshoot the service. Data the Intune service collects includes:

- Device names and inventory data used to provide the service.
- Administrator data, including the name, address, phone number, and email address of the account owner and IT administrators (Microsoft uses this data to provide the Online Service, complete transactions, administer the account and detect and prevent fraud.)

There are three types of data collected from mobile devices managed by Intune:

### 1. Hardware inventory

This information is provided by the mobile device operating system (Windows, iOS, and Android) and may be different based on each OS. This information could include, but is not limited to:

- Name
- Manufacturer
- Model
- Operating system
- Processor
- Serial number
- OS version
- Cellular technology
- Jailbreak status
- Free/Total space
- Exchange Device ID
- Wi-Fi MAC address
- Ethernet MAC address
- Device encryption status

### 2. App inventory

There are two types of apps which can be installed on a mobile device. Corporate apps are installed through Intune's Company Portal and are offered or required by your company's Intune administrator. Personal apps are those which the user installs on their own from the Windows Store, Apple App Store, or Google Play. App Inventory includes:

- Name
- Version
- ID
- Installation location
- Size

There are a few factors which affect which apps are inventoried.

### Personal or corporate-owned devices

Whether you're using Intune or Intune connected to System Center Configuration Manager to manage devices, the administrator can identify specific devices as corporate-owned. By default, on personal devices, only those apps which are installed via Intune and the Company Portal are inventoried, whereas on corporate devices, all apps are inventoried. One exception is Mac OS, where all applications are inventoried regardless of ownership designation.

### Compliant and non-compliant apps

When the administrator defines compliant and noncompliant apps to define which apps are allowed on a device in order to be considered "compliant" with corporate policies, it is necessary to inventory all apps, even on a personal device, to compare against the policies. **These personal apps are listed in reports available to the Intune administrators.**



# Microsoft Intune

## 3. Policies and configurations

Device or application management settings, certificates, VPN and Wi-Fi profiles are all examples of policies and configurations which an Intune administrator can define and deploy. This content, as well as the resulting compliance information from each managed device, is also stored by Intune

Intune does not collect information specific to user activities, including:

- Phone logs
- Contacts, email, calendar information
- Documents
- Text (SMS) messages
- Video/photos
- GPS information
- Web browsing history

Additionally, Intune provides robust device restriction capabilities including encryption for Android, iOS and Windows Platforms. To learn more about these features, see the following article: <https://docs.microsoft.com/intune/device-restrictions-configure>.

## Data locality

Microsoft has a regionalized data center strategy. The

administrator inputs during initial setup of the services, determines the primary storage location for that customer's data. For example, if a customer in the United Kingdom creates an Intune subscription, their subscription will be created and customer data stored in a Microsoft data center located in a European Union (EU) country. To help ensure service availability, Intune follows a business continuity methodology that enables data center fail over within a given region.

## Primary data centers

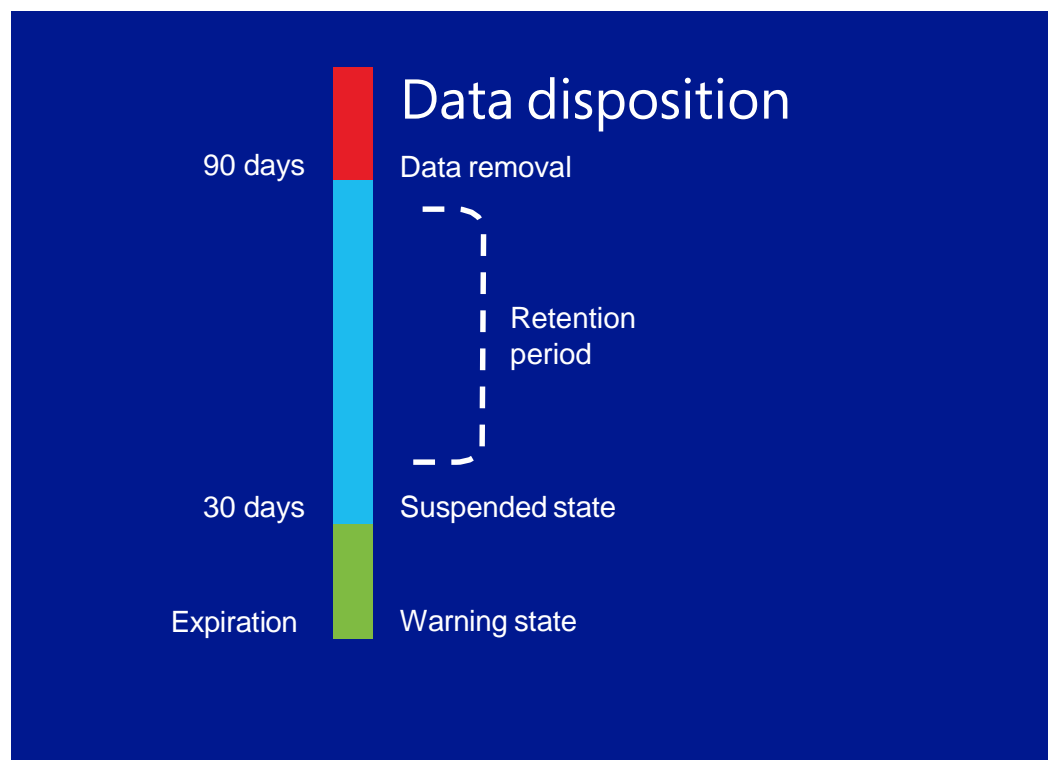
Intune's global data center strategy can be found here: <http://intunedatacentermap.azurewebsites.net/>

## Data disposition

Microsoft believes that customers own their own data. When customers do not renew their Microsoft Intune subscriptions (i.e., they terminate or allow their subscriptions to expire), their subscriptions move through the following states:

### Warning state

Their subscriptions initially go into a warning state during which they can continue to use the service and their Customer Data is available. They have 30 days to renew their subscriptions, and during this time they will receive notifications.



## Suspended state

If after 30 days customers do not renew their subscription, they go into the suspended state. They still have rights to their Customer Data and can continue accessing the service, but they cannot enroll any new devices into the service.

## Retention period

At the end of the Suspended state, customers can continue accessing their Customer Data for 90 days in a limited function. If after 90 days customers do not renew their subscription, Customer Data is removed within 30 days of the end of the retention period.

Customers who actively cancel their subscription may choose to disable their accounts and request deletion of their subscriber data by contacting our Customer Support team. If they do not provide specific instructions to delete their data, we follow the 90 day retention period. There is no 30 day suspend state or warning. At the end of the 90 day retention period, Intune removes Customers Data within 30 days of the end of the retention period.

## Independent verification

Intune is compliant with many world-class industry standards,

and it is verified by third parties. Independent The complete list of Intune compliance offerings is available here: <https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings>. In the **Filter By** bar, select **Intune** as the **Product of Service**.

Intune customers throughout the world are subject to many different laws and regulations. Legal requirements in one country or industry may be inconsistent with legal requirements applicable elsewhere. As a provider of global cloud services, Microsoft runs its services with common operational practices and features across multiple jurisdictions.

To help customers comply with their own requirements, Microsoft builds its services with common privacy and security requirements in mind, and our built-in capabilities help customers comply with a wide range of regulations. It is ultimately up to customers to evaluate our offerings against their own requirements, so they can determine whether Intune satisfies their legal and regulatory needs.

## Conclusion

Intune can help any business reduce the cost and complexity of managing PCs, mobile devices, and applications. It can even help businesses adapt to entirely new scenarios, such as BYOD. But no business can move management into a cloud-based service without understanding its security practices and technologies.

To that end, Microsoft built Intune to meet the high bar required to gain business' confidence and trust. Microsoft built the service leveraging its years of experience providing sophisticated cloud and on-premises solutions. Intune makes it easy for businesses to access and use its services while helping keep their data private and secure in its data centers. To learn more about Intune, visit <http://www.microsoft.com/intune>

## Additional resources

To learn more about Intune security in the data center, see:

- Microsoft Intune Trust Center  
Frequently Asked Questions  
<https://www.microsoft.com/TrustCenter/CloudServices/Intune>
- Microsoft MCIO  
<https://azure.microsoft.com/global-infrastructure/>
- Microsoft Trustworthy Computing  
<https://azure.microsoft.com/overview/trusted-cloud/>

# Microsoft Intune

© 2015 Microsoft Corporation. All rights reserved.

This document is for informational purposes only and is provided "as is." Views expressed in this document, including URL and any other Internet Web site references, may change without notice. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.