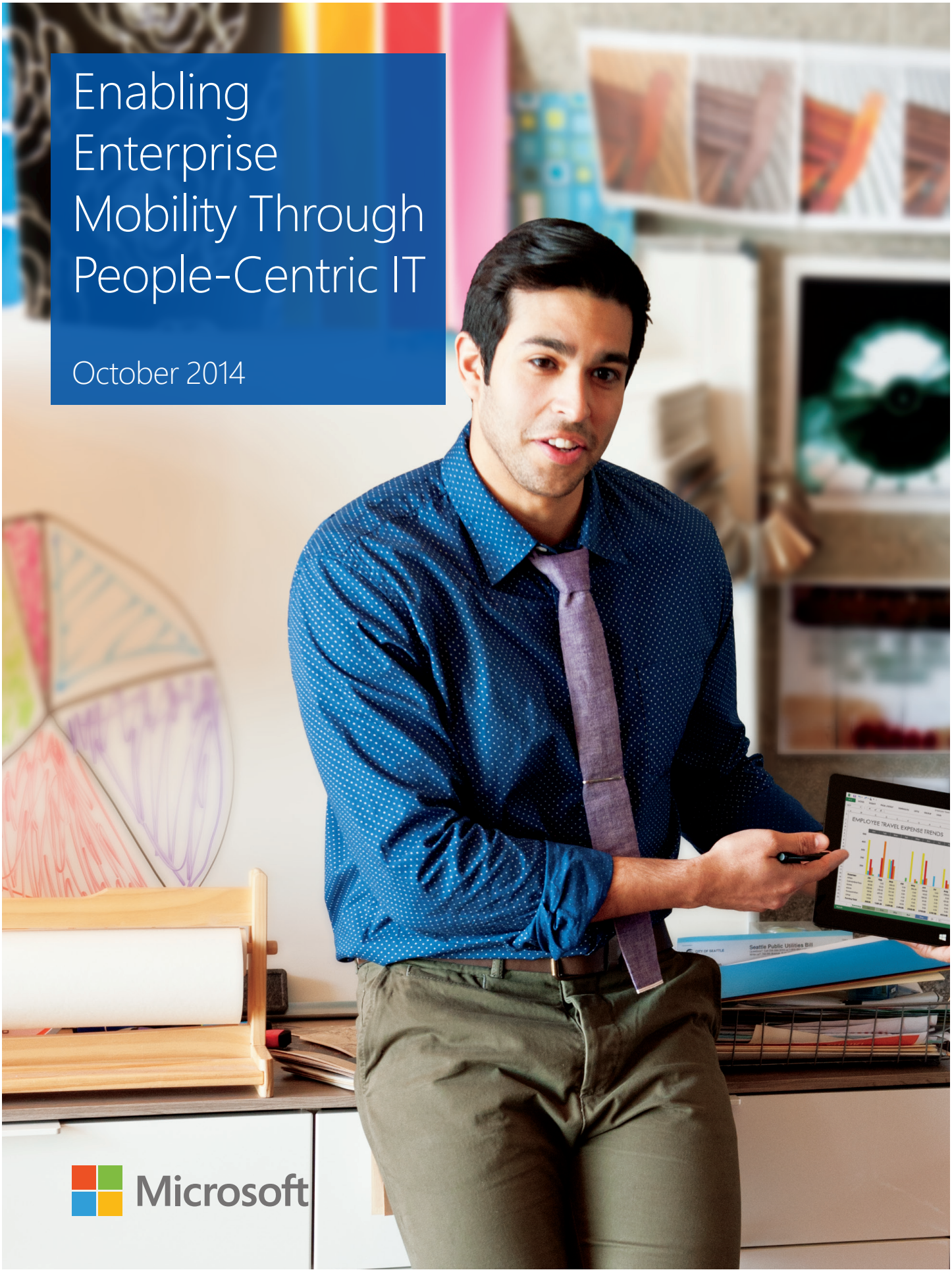
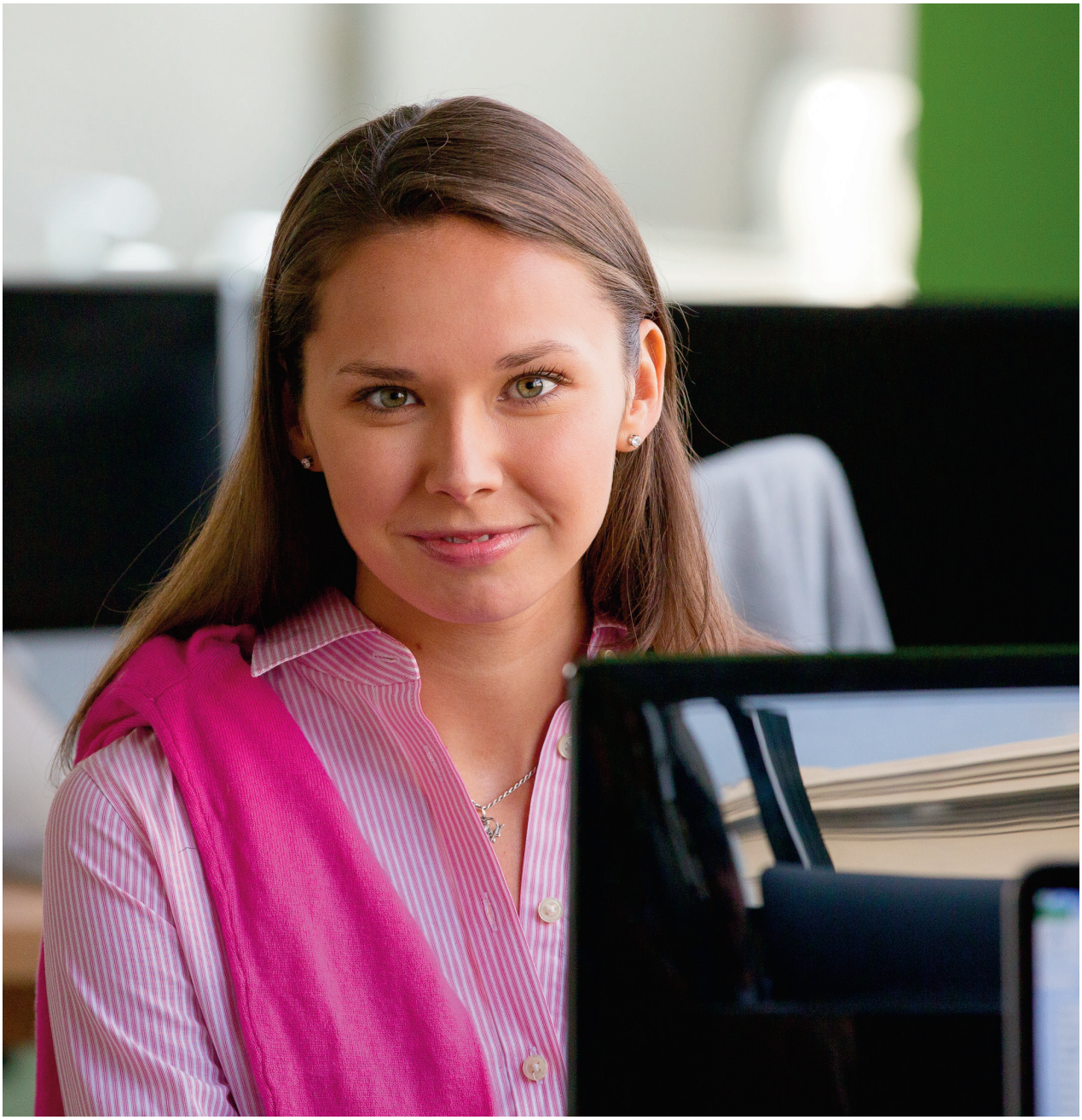
Enabling Enterprise Mobility Through People-Centric IT

October 2014



Microsoft

Table of Contents



Enable Enterprise Mobility Through People-Centric IT

Windows Server 2012 R2, Microsoft System Center 2012 R2 Configuration Manager, Microsoft Intune, and Microsoft Azure enable the consumerization of IT without compromising compliance

Overview

The proliferation of consumer devices and ubiquitous information access is driving the enterprise away from a device-centric model, centered on corporate-owned and provisioned devices to a bring-your-own-device (BYOD) and bring-your-own-cloud (BYOC) model in which employees use their own devices to access corporate applications and data and use personal cloud storage for data and services. When they're working, people expect consistent access to corporate tools and data regardless of the type of device they're using. They also want their corporate-issued technology and resources to look and behave like their personal technology—always on and always available from any device, from virtually anywhere.

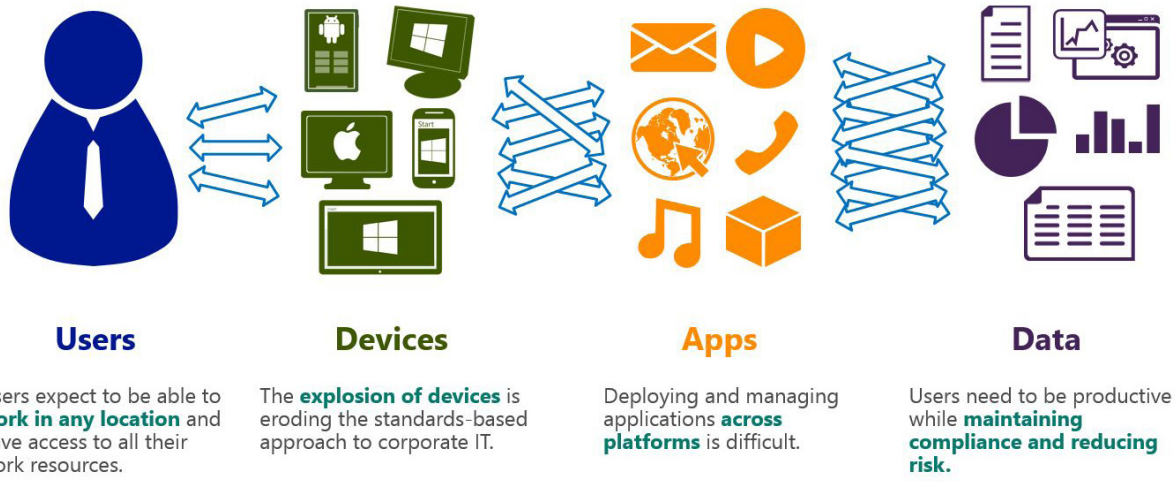
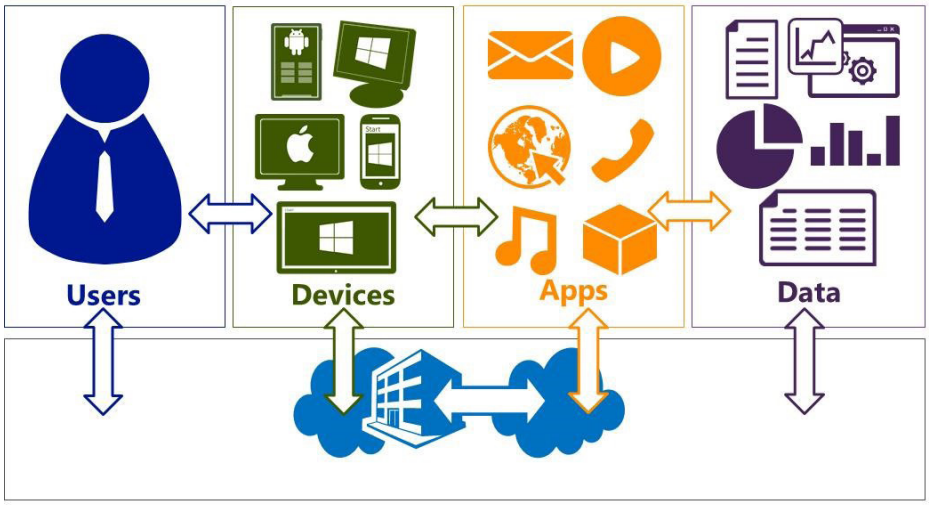


Figure 1 Today's challenges

The trend toward BYOD and BYOC—and with it, the move toward the consumerization of IT—presents an opportunity for IT to help increase user productivity and satisfaction. But this trend also brings numerous management and security challenges to IT organizations, which must see that enterprise infrastructure and corporate data are protected from malicious intent, while ensuring that these resources can be accessed in compliance with corporate policies regardless of device type or location.

An enterprise model that supports the use of consumer devices and cloud storage in the workplace and the ability to work from virtually anywhere and anytime must move from a device-centric view of IT management to one that's people-centric.

Enable Enterprise Mobility Through People-Centric IT



Enable users

Allow users to work on the devices of their choice and provide consistent access to corporate resources.

Protect your data

Help protect corporate information and manage risk.

Unify your environment

Deliver a unified application and device management on-premises and in the cloud.

Figure 2 People-centric IT

Microsoft assists IT in supporting the consumerization of IT and in retaining effective management, security, and compliance capabilities. The enterprise tools and technologies that Microsoft provides can help with key enterprise tasks—such as identifying non-corporate devices, delivering applications and data to those devices with the best possible user experience, and establishing and enforcing policies on devices based on the user's role. Microsoft enterprise tools and technologies can help IT maintain security across all device types, regardless of whether the devices are corporate or personal assets, and establish security measures that protect their organizations' systems, data, and networks.

With Windows Server 2012 R2, Microsoft System Center 2012 R2 Configuration Manager, Microsoft Intune, and Microsoft Azure, Microsoft builds on a comprehensive, people-centric solution that empowers user productivity while supporting IT's management needs.

For enterprises, Microsoft solutions enable users' mobile productivity and provide:

Simplified registration and enrollment for BYOD. Users can register their devices for access to corporate resources and enroll in the Microsoft Intune management service to manage their devices and install corporate apps through a consistent company portal.

Consistent access to company resources across devices. Users can use the device of their choice to access corporate resources regardless of location.

Support for modern work styles with Desktop Virtualization. The Microsoft Desktop Virtualization solution helps IT enable users to access corporate resources from virtually anywhere, on a variety of devices, and maintain data compliance. Desktops and applications are streamed but never stored on user devices, reducing the risk of losing data on stolen, compromised, or lost devices.

Automatic connection to internal resources when needed. Users can access corporate resources automatically when IT enables support for single sign-on and other automatic authentication mechanisms.

Business applications delivered from Microsoft Azure. Azure RemoteApp brings scale, agility, and global access to business applications. With Azure RemoteApp, company applications run on Windows Server in the Azure cloud, where they're easier to scale. This helps users to stay productive on the go, and lets IT scale up or down with no large capital expenditure while protecting sensitive corporate applications on the reliable Azure platform. (Note that Azure RemoteApp is currently in preview.)

Cross-platform access to remote desktops and applications. Microsoft Remote Desktop apps provide easy access to a variety of devices and platforms, including Windows, Windows RT, Windows Phone, iOS, OS X, and Android. Microsoft's Desktop Virtualization solution provides flexibility to both users and IT by providing access to users' PCs (through RD Gateway), personal or pooled virtual machine (VM)–based desktops, session-based desktops, and RemoteApp programs, all from a single app. Users can get the Microsoft Remote Desktop app by accessing the application store for their devices.

A single user identity for each user. Increase user productivity by providing users with a single identity to use no matter what they're accessing and whether they're working in the office, working remotely, or connecting to a cloud-based Software as a Service (SaaS) application. Having a single username and password to remember makes for happy users.

For IT professionals, Microsoft solutions unify the environment and provide:

Mobile device management of on-premises and cloud-based mobile devices. IT can manage mobile devices completely through the cloud with Microsoft Intune or extend its System Center Configuration Manager infrastructure with Microsoft Intune to manage their devices (PCs, Macs, or servers) and publish corporate apps and services, regardless of whether they're corporate-connected or cloud-based.

Simplified, user-centric application management across devices. IT gains efficiency with a single management console, where policies can be applied across group and device types.

Comprehensive settings management across platforms, including certificates, virtual private networks (VPNs), and wireless network and email profiles. Policies can be applied across various devices and operating systems to meet compliance requirements, and IT can provision certificates, VPNs, and Wi-Fi and email profiles on personal devices from within a single management console.

Microsoft solutions help protect corporate data by providing:

The ability to protect corporate information by selectively wiping apps and data. IT can access managed mobile devices to remove (or render inaccessible) corporate data and applications in the event that the device is lost, stolen, or retired from use.

Policy-based access control to corporate applications and data. IT can set policy-based access control for compliance and data protection.

A common identity for accessing resources on-premises and in the cloud. IT can better protect corporate information and mitigate risk by being able to restrict access to corporate resources based on user, device, and location.

Identification of compromised mobile devices. Jailbreak and root detection enables IT to determine which devices accessing corporate resources are at-risk, so that IT can choose to take appropriate action on those devices, including removing them from the management system and selectively wiping the devices.

Protect information anywhere. Protecting information at rest and in transit requires authentication and preventing alteration, both key requirements for protecting sensitive corporate information.

This guide provides an overview of the Microsoft solution that can help enterprises transition from a device-centric to a people-centric, consumerized IT environment without compromising compliance. It also provides details about how Microsoft solutions and products can help IT organizations use a people-centric approach to client management.

Microsoft's solution optimizes the application infrastructure, provides unified management, and supports the latest security and access models.

Simplify acquisition of the complete solution:

The Enterprise Mobility Suite is the comprehensive cloud solution that enables people centric-IT. The Enterprise Mobility Suite is also the most cost-effective way to acquire the included cloud services:

- Microsoft Azure Active Directory Premium for hybrid identity management
- Microsoft Intune for mobile device and application management
- Microsoft Azure Rights Management Services for information protection

Now, with these three cloud services brought together in the Enterprise Mobility Suite (EMS), Microsoft makes it easy and cost-effective for IT to acquire the full set of capabilities necessary to manage enterprise mobility challenges.

The Enterprise Mobility Suite delivers greater capacity for enabling BYO and SaaS than anyone in the market, and at a fraction of the cost charged by others in the industry.

To learn more about the Enterprise Mobility Suite, visit http://aka.ms/EnterpriseMobilitySuite.

Enable Users

Enable people to use their chosen devices at work and provide consistent access to corporate resources

Overview

Today's users want to access corporate applications and data from anywhere and from any device (smartphones, tablets, and PCs), and they want a streamlined way to provision a new device for corporate information access. Then, after their devices are provisioned, they want a consistent way to access corporate applications and data from their devices, including a simplified sign-on process and easy access to tools virtually anytime and from virtually anywhere.

Challenges

Users want to **use the device of their choice** and have access to both their personal and work-related applications, data, and resources.

Users want an easy way to be able to **access their corporate applications** from anywhere.

IT departments want to enable users to work this way, but they also need to **control access to sensitive information** and remain in compliance with regulatory policies.

Solutions

Users can **register their devices,** which makes them known to IT, who can then use device authentication as part of providing **access to corporate resources**.

Users can **enroll their devices,** which provides them with the company portal for **consistent access to applications** and data, and to manage their devices.

IT can **publish access to corporate resources** with conditional access based on the user's identity, the device they are using, and their location.

Figure 3 People-centric IT enables users to use the devices of their choice

IT must find ways to accommodate the proliferation of consumer devices and support access to corporate resources from locations outside the tightly controlled corporate network setting. IT needs a management infrastructure that's efficient, cost-effective, and secure. Finally, it's important to have enterprise management tools that make it easy to set up and manage devices, and solutions that provide access to corporate applications and data from locations within and outside the corporate network.

The following sections outline key capabilities and present sample business scenarios that show how Microsoft enables users by empowering people-centric IT.

Simplify BYOD Registration and Enrollment

Until a few years ago, most IT organizations discouraged or explicitly prevented employees from using personal devices for business-related data. It simply wasn't necessary to support users' personal devices.

However, employees often have or want more up-to-date devices than those IT has provided, leading people to demand that they be able to use their own technology at work. This requires IT to support a growing number and wider range of device types in their enterprise infrastructure, as well as to manage the frequent replacement of devices and regular introductions of new technology. This drives the need for flexibility—IT must be able to support and manage the current generation of devices as well as those two or three (or more) generations out. And this support must extend not only to corporate assets, but also to employee-owned devices.

Business Requirements

Scenario: Joan from finance just purchased a new tablet for her personal use. At first, she carries both her personal tablet and her corporate laptop with her, but she quickly finds that carrying two devices is inconvenient. She asks the IT department if she can give back her corporate laptop and access the corporate apps she needs through her personal tablet, which is newer and faster than her work device.

Joan needs an easy way to configure her personal devices for use at work. IT needs a way to support the use of employee-owned devices in the workplace, enabling Joan to access the applications she needs, while controlling what the information that devices can access.

The People-Centric IT Solution

In the past, the answer to this scenario would have been "No." But because Joan's company has implemented Microsoft's solutions for BYOD scenarios, Joan can work on her personal tablet, while IT retains the control they require to remain compliant with corporate policies.

Supporting BYOD in the workplace requires a simple way for users to register their devices for use and ways for IT to take the device registration into account as part of the authorization for access to corporate resources. Workplace Join in Windows Server 2012 R2 enables users to register their devices in Active Directory, and IT can require multi-factor authentication as part of this registration process. Additionally, users can enroll their devices for management, which connects the devices to Microsoft Intune and allows the installation of the company portal. This enables users to access their applications and data, and to self-manage their enrolled devices.

For example, when Joan registers her device, she makes it "known" to IT; IT can then configure conditional access policies that take into account not only Joan's identity, but also the device she's using. After Joan enrolls her device, she can access her applications and manage her own device through the company portal that's installed. System Center 2012 R2 Configuration Manager and Microsoft Intune together gather information about the user and device and allow IT to manage the device.

Windows Server 2012 R2

- Users can register their devices, which makes the device "known" to IT, which can then use device authentication as part of providing access to corporate resources. Device registration is a "give-and-get" scenario. The user "gives" by registering the device, and in turn "gets" access to resources. From an IT perspective, after the device is registered, it becomes a record in Active Directory, so it can be used as a part of the authentication and authorization policies.
- Registering a device enables single sign-on and access to corporate data through Workplace Join. Registration makes the device "known" to IT and enables IT to provide access to applications and data that otherwise wouldn't be available.

System Center 2012 R2 Configuration Manager and Microsoft Intune

- An easy way for users to access all their corporate applications from one place is by enrolling their devices for access to the company portal. Enrollment adds the device to the unified device management solution and allows the installation of the company portal. IT can populate the company portal with internal line-of-business (LOB) applications, as well as with links to web applications and applications available in the public application stores (Microsoft Windows Store, Windows Phone Store, Apple App Store, and Google Play). From within the company portal, users can manage their devices and perform various actions, such as wiping a lost or replaced device.

Supporting Features

Features	Description	Product
Web Application Proxy	Allows the publishing of corporate resources to external users and devices as well as enabling Workplace Join to be completed from external locations.	Windows Server 2012 R2
Active Directory Federation Services (ADFS)	Provides the Workplace Join feature, including support for multi-factor authentication and the enforcement of conditional access policies when users connect to resources.	Windows Server 2012 R2
Device Management	Provides comprehensive management services for devices based in the cloud and on-premises, enabling users to install offered applications onto their devices.	System Center 2012 R2 Configuration Manager and Microsoft Intune

Conclusion

Microsoft makes it easier for organizations to allow people to use the devices they choose by enabling those devices to be integrated into the security and management models IT may already have in place.

Enable Consistent Access to Corporate Resources

The prevalence, speed, and availability of affordable high-speed broadband and Wi-Fi networks means that people can expect to get their work done even when they're mobile. They expect to access corporate resources in a consistent way across devices, and they expect that the technology provided will be available on their schedule and from wherever they happen to be. This work-from-anywhere paradigm requires IT to change the way people access resources such as company tools, apps, data, and services.

Business Requirements

Scenario: Paul from Human Resources considers himself a savvy consumer of technology. As an early adopter of new mobile technology, Paul now finds that his personal device has outpaced the device provided for him at work. Paul wants to be able to use his more flexible and powerful personal device from home to review the résumés of applicants prior to their job interviews.

Paul needs an easy way to access corporate apps and data from any device he chooses to use. IT needs an efficient way to provide Paul with consistent access to corporate resources from his personal devices.

The People-Centric IT Solution

While the IT department at Paul's company has previously forbidden the use of personal devices, IT has recently worked with Microsoft to implement the people-centric IT solution, which enables streamlined device management and provides access while protecting corporate resources.

When users enroll a device for management, they can access the company portal from their device. This company portal is consistent across devices, and it makes the latest corporate applications available. Work Folders, new in Windows Server 2012 R2, enable users to store the data they need for work in one place and make it easy for users to sync this data with the corporate datacenter and across devices.

System Center 2012 R2 Configuration Manager and Microsoft Intune

- Users can self-provision applications through a company portal that shows the applications they have permissions to install. Users can view, install, and run corporate applications across devices, including corporate-owned LOB applications, web applications, and links to IT-recommended applications available from public application stores (Windows Store, Windows Phone Store, Apple App Store, and Google Play).
- IT can specify which applications users can see in the company portal based on a variety of criteria, such as a defined user role (for example, finance managers or group managers) or groups within Active Directory.
- Using the company portal, people can view all their managed devices and take action, such as selectively wiping corporate applications and data from their devices or removing a device from the management system and corporate access.

Windows Server 2012 R2

- Using Work Folders, users can sync files stored in their personal Sync Share on a corporate file server with their devices. IT can integrate this share with Dynamic Access Control for automated classification and protection of documents based on their content, and these changes will then be replicated to the users' devices.
- IT controls external access through Web Application Proxy, which publishes resources with multi-factor authentication and conditional-access policies.

Supporting Features

Features	Description	Product
Company Portal	A self-service portal that runs natively on each device and that enables users to install applications on their devices. Users can view and remove their managed devices and set up synchronization of their work data.	System Center 2012 R2 Configuration Manager and Microsoft Intune
Work Folders	A centralized location on a file server in the corporate environment that's configured to allow the synchronization of files to users' devices. Work Folders can be published directly through a reverse proxy or via the Web Application Proxy for conditional access policy enforcement.	Windows Server 2012 R2
Web Application Proxy	Allows the publishing of corporate resources to external users and devices, including Work Folders, in straight reverse proxy pass-through authentication or integrated with ADFS for conditional policy-based access.	Windows Server 2012 R2

Conclusion

Microsoft enables IT to make corporate resources available to people on the devices of their choice from virtually anywhere, while enforcing security policies and retaining control for corporate compliance.

Deliver Windows Desktops and Applications with Microsoft Desktop Virtualization

As the enterprise adapts to more personally owned devices, IT needs a way to offer a consistent, managed enterprise desktop to employees. Microsoft Remote Desktop Services/Virtual Desktop Infrastructure (VDI) enables IT to deliver corporate desktops and applications that employees can access from their personal or corporate devices, from both internal and external locations. Centralized desktops and apps hosted in the datacenter or cloud can be managed easily, and apps and data can be secured.

Business Requirements

Scenario: Adam is the desktop manager for his company's IT department. In the past, PCs were all corporate-owned, and Adam deployed a standard desktop image to the machines that included a standard set of policies and applications. As more people move to using their own PCs, laptops, and tablets, often from non-corporate networks, Adam needs a way to enforce the same security policies to protect data, while enabling access to applications on devices that his company no longer directly manages.

IT needs a way deploy a standard desktop solution that can be housed centrally in the datacenter. Users can access these virtual desktops and applications from a variety of devices and locations, while IT protects the data, including limiting the ability to store the data on any unmanaged devices.

The People-Centric IT Solution

Windows Server 2012 R2 provides a desktop virtualization solution that's easy to deploy and configure, and it delivers a rich user experience. With the Microsoft people-centric IT solution, IT has the freedom to choose personal and pooled virtual machine (VM)–based desktops as well as session-based desktops and RemoteApp programs hosted on-premises or in the cloud with Microsoft Azure RemoteApp. The Microsoft solution also offers IT several storage options.

Enable Users

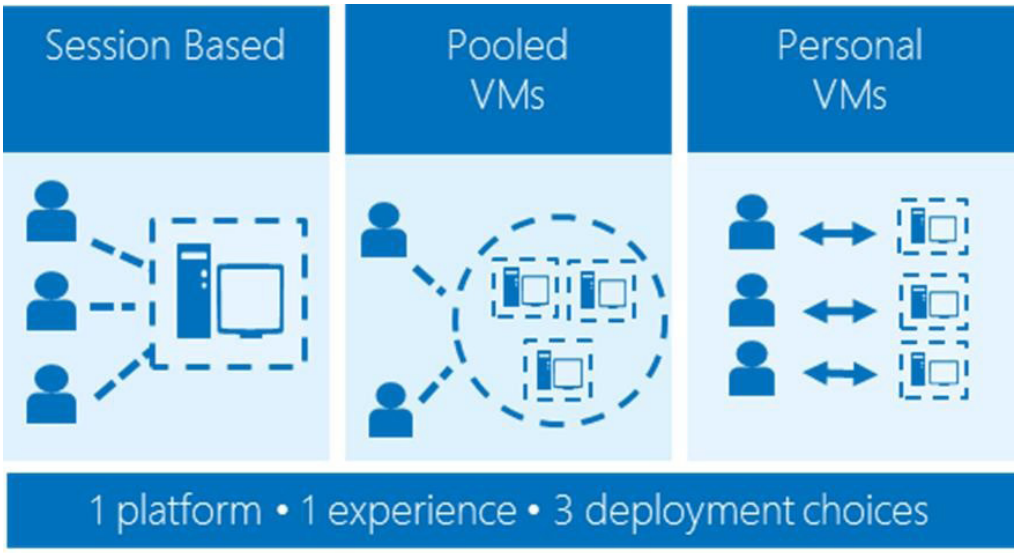


Figure 4 Single management console provides a unified experience and multiple deployment choices

Windows Server 2012 delivered significant enhancements that simplify the deployment and management of a VDI environment as well as improve the user experience. Windows Server 2012 R2, Microsoft Remote Desktop apps, and Azure RemoteApp continue to improve the user experience and management capabilities with key new features.

Windows Server 2012 R2

- Windows Server 2012 provided a single console for deploying, configuring, and managing a VDI deployment. Windows Server 2012 R2 brings Session Shadowing to the management console, enabling helpdesk or IT staff to view and remotely control a user's session.
- Windows Server 2012 supported SMB 3 and Storage Spaces for VDI storage, providing a high-performance storage alternative to expensive storage area network (SAN) storage. Windows Server 2012 R2 further expands on this by supporting online disk deduplication, which reduces the amount of space on disk that's consumed by personal VMs. It also provides support for storage tiering, enabling IT to use a mix of solid state and spinning disks to create a storage volume that automatically optimizes locations of data across the disks so that the most accessed data blocks are on the highest-performing disks.

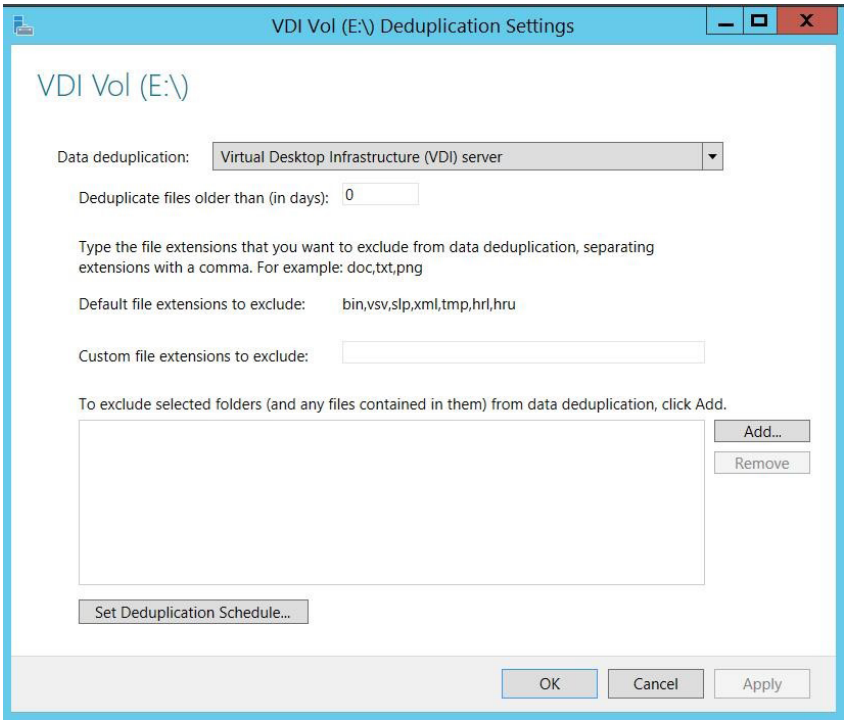


Figure 5 Windows Server 2012 R2 provides deduplication on your schedule

- Windows Server 2012 delivered several enhancements to the Remote Desktop Protocol (RDP) that improves the performance of remote desktops over WAN connections. This is accomplished by enhancing the appearance of RemoteApp programs so that they behave graphically more like locally executed apps. There are also improvements to the codecs and display handling. Disconnected sessions reconnect much faster than in the past—reconnect times may be reduced from over 70 seconds to less than 10.
- Remote Desktop Gateway (RD Gateway) in Windows Server 2012 includes support for pluggable authentication, so providers can write a plug-in to support one-time password (OTP) or RSA SecureID authentication to the RD Gateway.

Supporting Features

Feature	Description	Product
Session Shadowing	Allows administrators to view and remotely control active user sessions on RD Session Host servers.	Windows Server 2012 R2
Deduplication Storage	Enables storage volumes containing virtual hard disk (VHD) files for a VDI collection to automatically identify redundant blocks on the storage and remove duplicate data to reduce the storage consumed.	Windows Server 2012 R2

Storage Tiering	Enables storage volumes that are a mix of multiple disks of different speeds. The operating system automatically optimizes the location of data in the volume so that the most frequently accessed data is on the fastest disks.	Windows Server 2012 R2
RemoteApp	Displays the correct thumbnail on the task bar instead of using generic icons. Moving a window drags the whole window, not just a wireframe. Transparent sections of RemoteApp windows render correctly.	Windows Server 2012 R2
Quick Reconnect	Reconnects disconnected sessions much faster than in earlier versions.	Windows Server 2012 R2
Dynamic Resolution Change	Enables full-screen remote desktop sessions to automatically resize to account for resolution changes on the endpoint without requiring the user to disconnect and reconnect.	Windows Server 2012 R2
Codec and Display Improvements	Delivers the best possible user experience under varying network conditions, trading off resolution of experience with bandwidth available.	Windows Server 2012 R2

Easy Access from Bring-Your-Own Devices with the Microsoft Remote Desktop App

With the release of Windows Server 2012 R2, Microsoft also introduces Microsoft Remote Desktop app, which provides easy access to a variety of devices and platforms, including Windows, Windows Phone 8.1, Windows RT, iOS, OS X, and Android. Microsoft VDI provides flexibility to both users and IT by providing access to users' PCs (for Windows Pro and above, through RD Gateway), personal or pooled virtual machine (VM)–based desktops, session-based desktops, and RemoteApp programs, all from a single app. Users can get the Microsoft Remote Desktop app by visiting the application store on their devices.

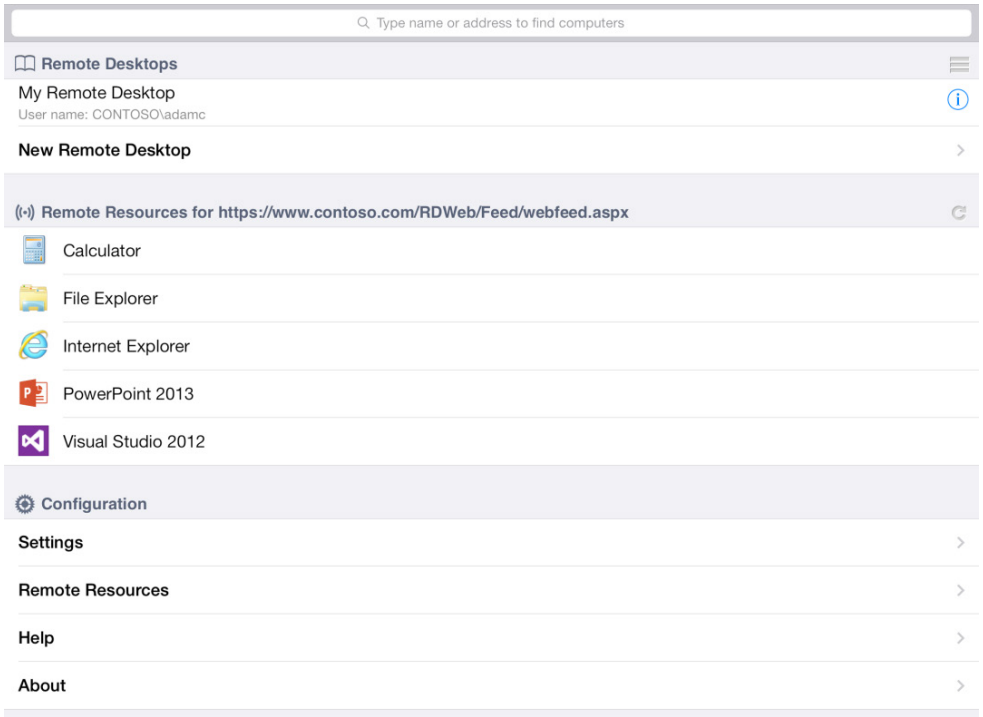


Figure 6 Microsoft Remote Desktop app for iOS – Connection Manager

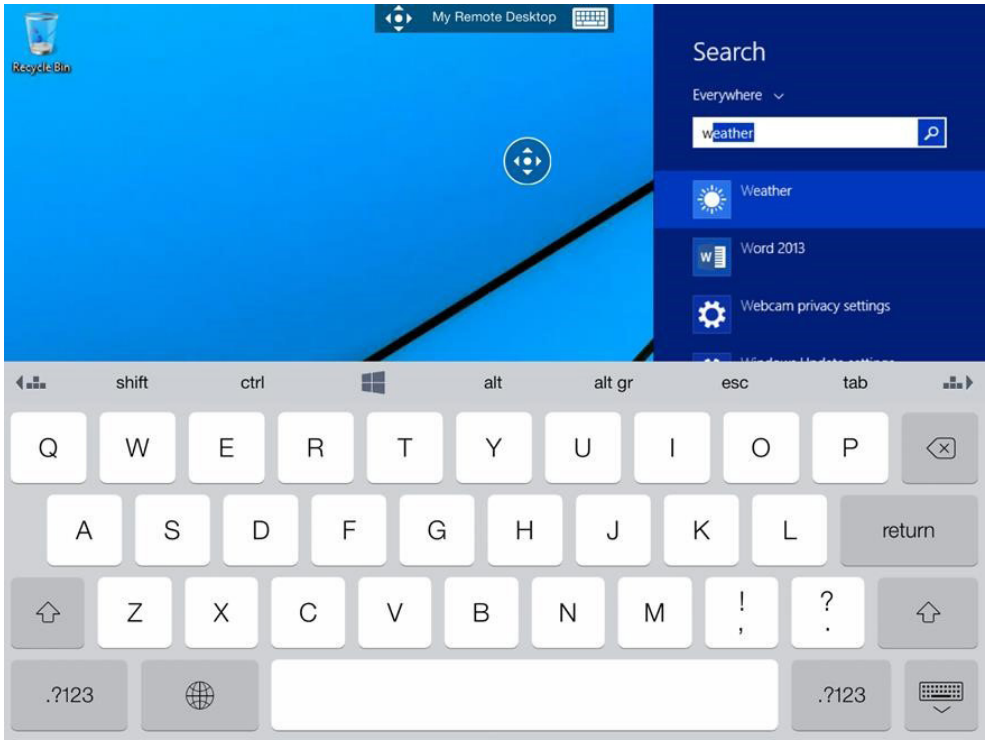


Figure 7 Microsoft Remote Desktop app for iOS – on-screen keyboard for Search

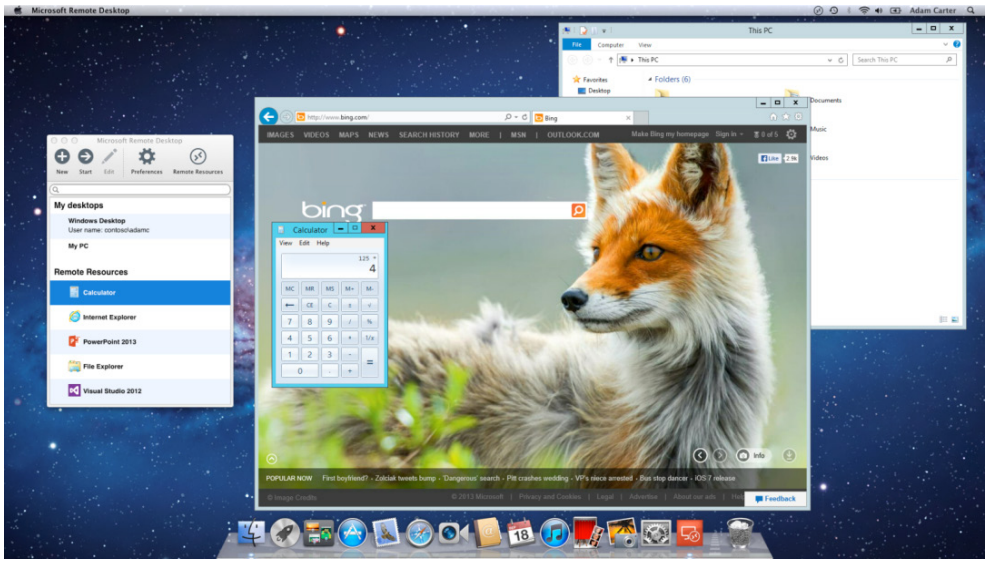


Figure 8 Microsoft Remote Desktop app for OS X

Supporting Features

Feature	Description	Product
Microsoft Remote Desktop App	Provides easy access to a variety of devices and platforms, including Windows, Windows Phone 8.1, Windows RT, iOS, OS X, and Android.	Windows Server 2012 R2 Azure RemoteApp

Microsoft Azure RemoteApp

Business requirements are changing as organizations strive to stay competitive and maintain operational efficiency while they support a variety of different devices that people choose to use. To meet these ever-changing business needs with limited resources, IT needs a flexible service that can scale up or down without large capital expenditure. Microsoft Azure RemoteApp was designed to overcome this challenge and provide scale, agility, and flexibility. Azure RemoteApp brings together rich Windows applications and Microsoft's years of experience in powerful Remote Desktop Services, on the trusted and reliable Azure platform.

Azure RemoteApp provides an effective solution for application delivery to a variety of users. Company applications run on Windows Server in the Azure cloud, where they're easier to scale and update. Employees install Microsoft Remote Desktop clients on their Internet-connected laptops, tablets, or phones—and can then access applications via Microsoft's Remote Desktop Protocol (RDP). While appearing to run on the users' local device, the applications are centralized on the reliable Azure platform. Software updates are no longer time-consuming, because they need to be updated only in Azure.

Azure RemoteApp provides a scalable platform for delivering corporate applications without large capital expenditure. Azure RemoteApp can help IT meet the elastic needs of the business, easing the challenges of the on-premises infrastructure and simplifying application delivery issues for a wide range of users, such as:

- Road warriors and mobile workers.
- Temporary/seasonal workers or vendors.
- Students.
- New employees joining the organizations during a merger and acquisition (M&A).

IT can choose between cloud deployment and hybrid deployment options, and decide whether to integrate the service with the company's on-premises infrastructure or deploy it as a standalone cloud service.

To build Azure RemoteApp on existing infrastructure, IT can use their own session host to deliver access to the applications, including LOB applications. IT can integrate Active Directory Domain Services with Azure Active Directory so that users can access the service by using their corporate credentials.

With a cloud deployment option, IT can quickly provision access using the pre-built app collections in Azure RemoteApp. Users can access their corporate resources by using their corporate credentials or with their Microsoft accounts (for example, outlook.com).

Supporting Features

Feature	Description	Product
Cloud-Based RemoteApps	Windows Server–based applications delivered from Microsoft Azure.	Azure RemoteApp

Conclusion

Microsoft Desktop Virtualization enables IT to deliver desktops and apps to users on a range of devices without compromising compliance. The integrity of the data is always maintained, and the risk of losing data on stolen, compromised, or lost devices is reduced. Desktop Virtualization also provides business continuity by making desktops and applications available from virtually anywhere and on a variety of devices.

Automate How Users Connect to Internal Resources

Balancing the needs of users, who want to access corporate resources from multiple device types and locations, with IT's need to protect corporate networks and data from malicious intent makes user authentication complex. Users have difficulty keeping track of multiple layers of credentials, and when those credentials vary depending on location, device type, or application, each potentially with a different sign-on, it can affect user productivity and result in less-secure access as users try to simplify sign-on information themselves.

Stymied by a difficult sign-on process, users may call helpdesk, which can increase overall support costs.

Business Requirements

Scenario: Mary works on site as a project planner three days a week. When she's on site, Mary signs on once to the corporate network, and then she can open any files she needs without supplying any other password authentication, regardless of the location of those files on the internal network. Twice a week, when Mary works from home on her laptop, accessing the files she needs requires multiple layers of authentication. She must sign on to the corporate network through a virtual private network (VPN), and then sign on again for the corporate tools she uses. This multi-layer authentication creates a potentially unsecure situation, because Mary has all her sign-on information written down on a sticky note next to her computer.

Mary needs an easier way to sign on to corporate resources, and IT needs a way to support this while maintaining the security of corporate resources.

The People-Centric IT Solution

Using a personal device shouldn't change a person's ability to access corporate resources, but, at the same time, IT must protect the security of corporate applications and data.

Microsoft provides connectivity features that help automate user access to resources in four ways:

- DirectAccess provides an "always on" connection for domain-joined Windows clients.
- The Remote Access role in Windows Server provides traditional VPN connections from user devices to corporate resources.
- Web Application Proxy, a feature in Windows Server 2012 R2, enables IT to publish access to corporate resources.
- A new feature in Windows 8.1 enables applications to trigger the VPN on the user's behalf as applications are launched.

System Center 2012 R2 Configuration Manager and Microsoft Intune

IT can define which applications automatically trigger a VPN connection to a corporate resource, and then can deploy the configuration details for applications and the Wi-Fi/VPN profiles to users' devices.

Windows Server 2012 R2

IT can tightly control access to corporate resources. The Web Application Proxy, when integrated with ADFS, enables IT security administrators to provide secure conditional access, based on the user, device, location, and application, by selectively publishing corporate resources to remote users using managed and unmanaged devices.

Supporting Features

Feature	Description	Product
Web Application Proxy	Enables IT to publish corporate resources to external users and devices. When integrated with ADFS, can also enforce multi-factor authentication and conditional access polices when users connect to resources.	Windows Server 2012 R2
Support for VPN, Email, and Wi-Fi Profiles	Deploys the policies and configuration for VPN, email, and Wi-Fi profiles.	System Center 2012 R2 Configuration Manager and Microsoft Intune

Use a Single User Identity for Each User

With the proliferation of consumer devices in the corporate world and the ease of adoption that cloud-based SaaS applications offer, maintaining control of users' access to applications across both internal datacenters and cloud platforms has become a significant challenge.

Business Requirements

Scenario: Robert is a sales manager who meets with customers around the world. While he's on the move, he needs to be as self-sufficient as possible; he has more than enough things that he has to manage and remember, and he doesn't have time to rely on others to manage his devices or daily tasks. Having to remember multiple sign-ons and profiles is cumbersome and slows him down. He needs features that streamline processes and enable him to manage most tasks, such as accessing apps, setting up group collaboration, or resetting his password, on his own.

Robert needs a streamlined way to sign on to multiple resources, including cloud resources, and manage common tasks on the corporate network and in the cloud. IT needs a way to control access to applications and information, on both the corporate network and in the cloud.

The People-Centric IT Solution

Users can be more productive when they work with a single identity no matter what they're accessing, whether they're working in the office, working remotely, or connecting to a cloud-based SaaS application. Having a single username and password not only makes for happy users, it also can increase security.

Providing users with self-service solutions to perform tasks such as resetting their password when they forget, or creating and managing their own groups for collaboration and access to resources, can enable them to work autonomously and focus on their jobs, while reducing support costs and unproductive downtime.

Of course, IT needs to retain control of all that information and access to applications and resources across the corporate datacenter and into the cloud.

For authentication, the people-centric IT solution enables identity sync and federation to create a single identity for each user. It also provides the ability to enforce additional levels of user validation, such as multi-factor authentication, as well as conditional access polices, such as device registration.

Reporting and alerting can help IT better understand usage patterns and identify potential security issues. Risk can also be mitigated by monitoring for inconsistent access patterns.

Azure Active Directory

Azure Active Directory provides identity and access management solutions for the cloud, including self-service capabilities for group management and password reset, single sign-on to SaaS applications, IT management for users, and security reporting. IT can sync user identity information between on-premises directories and Azure Active Directory.

Windows Server 2012 R2

Windows Server Active Directory provides the core of the on-premises identity solutions, authenticating users and devices, and enabling IT to grant access to resources on a granular basis.

Identity Manager

Identity Manager provides on-premises identity management capabilities, including self-service group management and password reset, and identity synchronization between multiple identity directories.

Supporting Features

Feature	Description	Product
Cloud-Based Identity Management	A set of Azure-based identity and access management capabilities, including user and group management, password reset, and security reports.	Azure Active Directory Premium Windows Server 2012 R2 Identity Manager
Identity Synchronization	A new identity sync engine that keeps on-premises identity information synchronized with Azure Active Directory. This includes all supported sync scenarios.	Azure AD Sync

Conclusion

Microsoft's Enterprise Mobility solution makes corporate resources available to users on the devices they use, removing the complexity of configuring the devices and enabling IT to enforce which users and which devices can access which corporate resources.

Unify Your Environment

Deliver unified application and device management on-premises and in the cloud

Overview

Moving from a device-centric to a people-centric enterprise presents a number of challenges. One of the biggest challenges is how to effectively support and manage the diversity of platforms and devices that can now potentially access corporate resources. IT must be able to configure device settings based on a number of variables, including users, groups, and device types, and device location (on-premises, in the cloud, or external). IT administrators also need to protect corporate security and manage compliance policies.

Challenges

Providing **users** with a **common identity** when they are accessing resources that are located both on-premises in a corporate environment, and in cloud-based platforms.

Managing multiple identities and keeping the information in sync across environments is a **drain on IT** resources.

Solutions

Users have a **single sign-on experience** when accessing all resources, regardless of location.

Users and IT can leverage their common identity for access to **external resources through federation**.

IT can **consistently manage identities** across on-premises and cloud-based identity domains.

Figure 9 People-centric IT requires a unified environment

Being able to manage both user- and corporate-owned devices within a single management console can help busy IT administrators efficiently evaluate and manage network activity, regardless of whether it originates on-premises, in the cloud, or remotely.

Devices can be managed—from the cloud or from the corporate network--in the world in which they live. Using a single interface enables IT to identify the devices accessing the corporate network, and then to configure and manage those devices consistently, regardless of device type. A unified solution also provides a cohesive structure for setting policy, delivering reporting capabilities that help IT to maintain corporate compliance.

As people work on a variety of devices and IT adopts a hybrid approach to delivering applications and services (both on-premises and in the cloud), it becomes essential to have a single identity that can be used for authentication. This single identity, which can be used regardless of what resources a person is accessing and where he or she is accessing them from, can make people more productive and provide a better overall experience.

The following sections outline key capabilities and present sample business scenarios that show how Microsoft supports people-centric IT with a unified environment.

Extend Your Existing System Center Configuration Manager Infrastructure and Manage Mobile Devices Through the Cloud

Many enterprises are moving their corporate resources to the cloud to save money and to better provide their users with access to those resources from virtually anywhere. As the enterprise extends to the cloud, managing corporate assets can become fragmented, and it becomes more difficult to set consistent policies across on-premises and cloud environments. A move to the cloud may end up costing more, because managing the complexity of the new enterprise model increases time spent on basic resource management tasks.

Business Requirements

Scenario: Matt is the IT administrator responsible for managing the assets that make up the company's on-premises System Center Configuration Manager infrastructure. Now Matt also has to manage mobile devices like tablets and smartphones, and he's finding that in order to view all the physical and virtual assets he's responsible for managing, he must use multiple management tools. He's worried that he's losing track of devices.

IT needs an integrated tool to view and manage devices both on-premises and in the cloud.

The People-Centric IT Solution

As corporate resources extend to the cloud, IT needs a cohesive way to view and manage those resources as part of the entire corporate infrastructure. System Center 2012 R2 Configuration Manager and Microsoft Intune extend management functionality to include support for managing physical and virtual assets from within a single management console.

System Center 2012 R2 Configuration Manager and Microsoft Intune

- IT can manage devices that connect to corporate resources in the world in which they live from a single management console by connecting their on-premises System Center 2012 R2 Configuration Manager infrastructure with the cloud-based Microsoft Intune service.
- From the management console, IT administrators get a comprehensive view that can help them identify and inventory mobile, physical, and virtual assets. This can help them focus on what users need access to in order to be productive, rather than focusing on the devices themselves.

Supporting Features

Feature	Description	Product
Unified Management Infrastructure	Enables IT to view and manage PCs, mobile devices, servers, and virtual machines—both corporate-connected and cloud-based—through a single management console.	System Center 2012 R2 Configuration Manager and Microsoft Intune

Conclusion

Microsoft provides a unified way for organizations to view and manage all the devices accessing corporate resources, including Windows-based PCs, tablets, phones, and servers; Windows Embedded devices; OS X, iOS, and Android devices, and UNIX/Linux servers. This integration saves organizations from having to learn or implement different, segregated products.

Simplify User-Centric Management Across Devices

As the types of devices being used to access corporate resources grows to include mobile devices (such as smartphones and tablets) as well as PCs and laptops, managing devices becomes more challenging.

Moving to people-centric IT increases the number of potential user and device combinations. For example, a user could have multiple devices, some corporate-owned, some personally owned. IT must be able to easily view the devices associated with a user and verify that those devices have the appropriate software installed.

Business Requirements

Scenario: Ann accesses corporate resources from her PC at work, a corporate laptop when she travels on business, and her own Microsoft Surface in the evening and on weekends. Using System Center 2012 R2 Configuration Manager and Microsoft Intune, the IT department can easily view the devices Ann is using. After Ann enrolls her devices for management, she wants to install the software she needs to get her job done.

Ann needs to use a variety of devices to get her job done. IT needs a simple way to manage across a variety of devices.

The People-Centric IT Solution

Integrating the management of the devices that make up the corporate infrastructure—whether those devices are physical, virtual, or mobile—makes the move to people-centric IT more efficient. Through System Center 2012 R2 Configuration Manager and Microsoft Intune, Microsoft provides an integrated console that enables IT to manage all device types and efficiently install software across device types.

With Microsoft's mobile device management capabilities, organizations can choose between two deployment methods for mobile device management: either completely cloud-based with Microsoft Intune, or a hybrid scenario where Microsoft Intune extends a System Center 2012 R2 Configuration Manager infrastructure into the cloud.

Windows Intune

Windows Intune enables BYOD by managing mobile devices and PCs from the cloud, giving people the opportunity to use the devices they choose to access applications and data while following corporate policies.

- The web-based administration console in Microsoft Intune provides simplified management of client computers in the organization, including Windows, Windows RT, Windows Phone 8, Apple iOS, and Android devices. IT can upload and publish software packages, configure and deploy management and security policies, and manage hardware and software computer inventory without on-premises infrastructure.

System Center 2012 R2 Configuration Manager and Microsoft Intune

Choose Microsoft Intune on its own for cloud-based management of PCs and mobile devices, or integrate it with System Center 2012 R2 Configuration Manager to manage corporate-connected Windows PCs, Macs, and Unix/Linux Servers on-premises along with users' mobile devices together in a complete, comprehensive management solution using a single administrative console, infrastructure, and reporting system.

- IT can manage a range of devices, including Windows-based PCs, laptops, tablets, phones, and servers; OS X, iOS, and Android devices; and UNIX/Linux Servers.
- IT administrators can use the single Configuration Manager console to deploy applications, define policies, and view reports across all PCs, mobile devices and servers.

Supporting Features

Feature	Description	Product
Unified Device Management	Enables IT to inventory, apply policies, and distribute software to a wide range of devices across multiple platforms.	System Center 2012 R2 Configuration Manager and Microsoft Intune

Conclusion

Microsoft is committed to helping reduce client management infrastructure costs and complexity. Organizations can use Microsoft Intune as a cloud-only solution for mobile device management, or integrate their existing Configuration Manager infrastructure with Microsoft Intune to provide a single console that consolidates on-premises and in-the-cloud management, providing client management and security in a single, unified solution. This streamlined approach to managing devices and applications simplifies complexity, while identifying threats and rectifying non-compliance.

Enable Comprehensive Settings Management Across Platforms

As the number of device types allowed in the corporate environment grows, keeping track of the settings possible for each device becomes crucial and more complex for IT, because the wrong settings could create a security risk.

Business Requirements

Scenario: Ben in IT is responsible for extending enterprise support to employee-owned devices. A brief survey of users reveals that not all devices are Windows-based and that some users want to use their mobile devices as well as personal PCs and laptops for work tasks.

Ben doesn't have the time to research the functionality supported by each type of device, but he still needs to be sure that the devices are configured in a way that mitigates risk to corporate resources. For example, Ben plans to require that all mobile devices accessing the corporate network have a PIN associated with them.

IT needs a comprehensive management solution that extends support across all device types, platforms, and users, and offers flexibility in configuring and inventorying devices based on whether they're corporate- or employee-owned.

The People-Centric IT Solution

Viewing all the devices accessing corporate resources is useful, but without the ability to centralize configuration or management tasks for those devices, it can be difficult to provision them for use in a way that makes it possible to enforce compliance policies. System Center 2012 R2 Configuration Manager and Microsoft Intune provide a unified way to configure devices, regardless of device type. Within System Configuration Manager, IT can also generate reports about all devices that use corporate resources.

Because Ben's organization is using System Center 2012 R2 Configuration Manager and Microsoft Intune, he can manage settings for all device types from one management console. To support corporate compliance, Ben can also generate reports that include all devices. He can also make choices about how to deploy software and inventory devices based on whether the devices are corporate- or employee-owned.

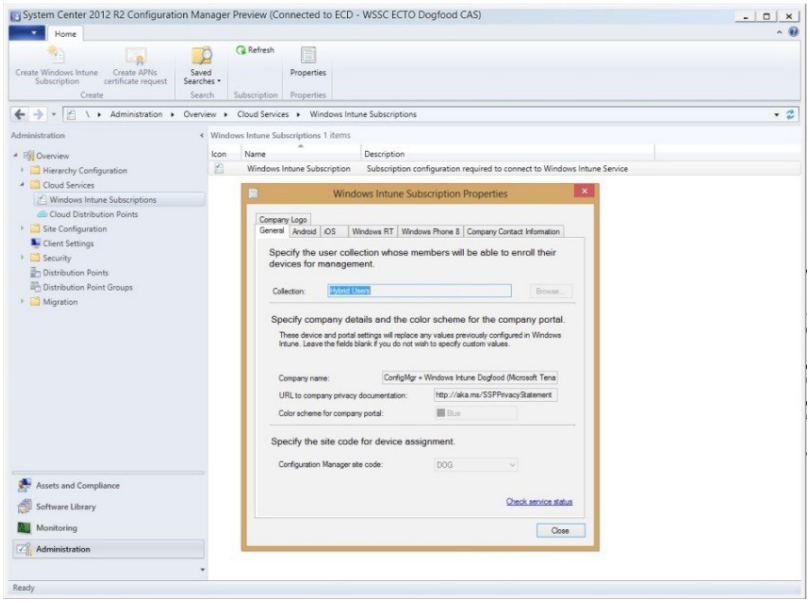


Figure 10 The unified management console streamlines device configuration

System Center 2012 R2 Configuration Manager

- IT can configure settings across different device types, including:
  - Security and compliance settings, including passwords and PINs, encryption, and wireless communication certificates.
  - Applications, including email, store, browser, and content ratings.
- IT can deploy applications and inventory them on the devices.
- IT can generate reports that show the usage of software distribution points within their infrastructure, and IT can establish content-distribution priorities, which can result in more effective infrastructure and deployment planning.

Supporting Features

Feature	Description	Product
Mobile Device Management Policies	Enables IT to define and deploy configuration policies specific to each mobile device platform to help meet compliance requirements.	System Center 2012 R2 Configuration Manager and Microsoft Intune
Software Distribution	Publishes or deploys applications to users' corporate or personal devices based on policy.	System Center 2012 R2 Configuration Manager and Microsoft Intune
Distribution Point Usage Reports and Management	Provides usage information about software distribution points across the infrastructure to help identify under- or over-used resources and prioritize package replication.	System Center 2012 R2 Configuration Manager

Conclusion

Together, System Center 2012 R2 Configuration Manager and Microsoft Intune provide organizations with a holistic view of all devices accessing corporate resources, whether they're PCs or mobile devices, on-premises or in the cloud. IT can define security and compliance settings to help ensure that devices accessing corporate resources meet corporate policies.

Define a Common Identity for Accessing Resources On-Premises and in the Cloud

A paramount concern of any IT department is protecting the security of corporate resources. Every time a user attempts to access data, it creates a potential security risk. Managing the risks associated with how people work was simpler when they accessed corporate resources using only corporate-owned and managed assets. Security becomes far more complex as enterprises move to a people-centric model in which corporate resources can be accessed using either corporate- or employee-owned devices of any type.

Business Requirements

Scenario: Phil is a security administrator for his organization. The number of devices that Phil manages continues to grow. He wants a centralized way to provide a consistent authentication process across device types, while continuing to make sure that the security of corporate assets is maintained.

IT needs a way to define a common identity that users can use to access resources on-premises, in the cloud, and outside the corporate network

The People-Centric IT Solution

Microsoft recognizes the need to provide more secure access to sensitive corporate resources when they're accessed and stored on mobile devices. Windows Server Active Directory and Microsoft Azure Active Directory provide functionality that enables IT security administrators to manage a person's identity regardless of whether the resources the person is accessing are on-premises, in the cloud, or from external networks.

Phil's organization has deployed Windows Server 2012 R2 and connected their Active Directory to Microsoft Azure Active Directory, so Phil uses the services associated with these products to set authentication options for access to resources on-premises and in the cloud, for users and devices wherever they're being used.

Windows Server 2012 R2

- With Active Directory, IT gains a single view of all user information, so they can efficiently manage security settings for users, devices, groups, printers, applications, and other directory-enabled objects (such as Workplace Join devices) from one secure, centralized location.
- Because authentication options can be set for the cloud, on-premises, or federated, IT can set up a model in which users can sign on once and then access their data and applications regardless of whether those resources reside in the cloud or on the corporate network.

Windows Azure Active Directory

- IT can use cloud-based identity, which serves as the central authentication endpoint for all users and devices outside the corporate environment and cloud/hybrid applications.
- IT can use Microsoft Azure Active Directory for the authoritative authentication directory or can check user validation and device verification through federated connections to other directories, such as on-premises Windows Server Active Directory or other cloud-based identity repositories.
- Azure Active Directory helps IT departments to effectively protect enterprise data and resources on any cloud platform by offering synchronization with on-premises directories, group-based single sign-on to thousands of SaaS applications, machine learning–based security and usage reports, alerting, and Multi-Factor Authentication.

Supporting Features

Feature	Description	Product
Windows Server Active Directory Domain Services	Provides an identity directory used to authenticate users and devices, and for the enforcement of access policies and centralized configuration policies.	Windows Server 2012 R2
Microsoft Azure Active Directory	Provides a comprehensive and high available IAM cloud solution that combines core directory services, advanced identity governance, and application access management. Also offers a rich standards-based platform that enables developers to deliver access control to their applications, based on centralized policy and rules.	Microsoft Azure Active Directory

Conclusion

As IT adopts a hybrid delivery model for applications and services across on-premises and in the public cloud, Microsoft provides a way for IT to provide a single sign-on experience for users by providing a common identity for accessing all their resources regardless of the location or device being used.

Protect Your Data

Protect corporate information and manage risk

Overview

Moving from device-centric to people-centric IT means moving from a world where the devices accessing corporate tools and data are company-owned and provisioned to one where devices are owned by users and contain applications and data not under corporate control. This introduces new challenges for IT administrators, who must provide flexible user models while making sure that corporate resources are protected from unauthorized access. Users expect consistent access to corporate resources, yet that access can't compromise the security of the enterprise.

Challenges

As users **bring their own devices** in to use for work, they will also want to **access sensitive information** and have access to this information locally on the device.

A significant amount of **corporate** data can only be found **locally on user devices**.

IT needs to be able to **secure, classify, and protect data** based on the content it contains, not just where it resides, including **maintaining regulatory compliance**.

Solutions

Users can work **on the device of their choice** and be able to access **all their resources**, regardless of location or device.

IT can enforce a set of **central access and audit polices**, and be able to protect sensitive information **based on the content of the documents**.

IT can **centrally audit and report** on information access.

Figure 11 IT must be able to protect data and maintain regulatory compliance

IT must deploy a solution that supports efficient and secure access to corporate resources regardless of whether the user's location is within or outside corporate control. To meet compliance requirements, IT must also be able to gather reporting information for regulatory and internal auditing purposes across the range of devices accessing the corporate network.

The following sections outline key capabilities and present sample business scenarios that show how Microsoft helps you protect your data in people-centric IT.

Selectively Wipe Devices

The portability of devices such as smartphones and tablets makes them attractive to people wanting to get work done on the go, but there's a risk associated with that portability—the potential for devices to be lost or stolen. To protect corporate data, it's imperative that users and IT have ways to wipe devices remotely.

Along with the portability of mobile devices, frequent advances in mobile device technology mean that people may change the devices they use to access corporate data more rapidly than in the past, re-purposing their old devices for family use or selling them back to wireless companies as they upgrade. When users discontinue using a device, having an easy way to remove corporate resources (or at a minimum render the data inaccessible) from those devices is essential in protecting the security of corporate tools and data.

Business Requirements

Scenario: Lisa is a corporate recruiter traveling on business to college job fairs. While she's out of the office, the team she recruits for is interviewing a few job candidates. Feedback on the candidates is recorded in the company's proprietary interview feedback application, and Lisa frequently checks the feedback from her smartphone. While at the job fair, Lisa sets her smartphone down for a minute, and before she can reach for it again, it disappears into the crowd.

Lisa needs to be able to quickly block access to corporate resources from her stolen mobile device. In case she's unable to wipe the device herself, IT needs a way to wipe the device for her, thereby maintaining the security of the company's data and applications.

The People-Centric IT Solution

With System Center 2012 R2 Configuration Manager and Microsoft Intune, mobile devices can be selectively wiped to protect corporate data and applications. This combined solution also provides a way for people to retire a device when they no longer use it to access corporate resources.

Luckily for Lisa, she has her laptop with her. She opens the company portal installed on her laptop, and she can view all the devices that she's using to access corporate resources. Lisa selects her smartphone, and then follows the steps to wipe the device. This removes all proprietary corporate applications and (where possible) associated data from her device. In all cases where the data was provisioned through the company portal, the data is rendered inaccessible, and, when the underlying platform supports it, the data is also removed. Because the IT department at Lisa's company also has the ability to manage the device, if she were unable to wipe the device herself, she could alert IT to wipe her device from the management console.

System Center 2012 R2 Configuration Manager and Microsoft Intune

- IT and individual users can selectively and remotely wipe a device, including removing applications, email, and data, management policies, and networking profiles.
- Users can also retire a device from management, which removes the device's ability to access corporate tools and data.

Supporting Features

Feature	Description	Product
Selective Wipe	Removes corporate-related applications, data, and management policies from the mobile device.	System Center 2012 R2 Configuration Manager and Microsoft Intune

Conclusion

Whenever people lose or upgrade their mobile devices, or if they no longer work for the organization, it's crucial to make sure that any corporate-related information, including applications and data, is no longer available on their devices. With System Center 2012 R2 Configuration Manager and Microsoft Intune, corporate resources can be remotely removed from the device by either the user or IT, while personal data on the device remains untouched.

Centralize Corporate Information for Compliance and Data Protection

With new models for how users access corporate resources, IT needs a new way to balance access and sharing of corporate information with the ability to audit against internal and regulatory requirements. The costs for meeting regulatory and compliance requirements are rising at a time when IT budgets are facing new constraints, so implementing changes to the infrastructure that enables people-centric IT must be cost-effective without sacrificing security. A centralized information protection model for access control, coupled with robust compliance reporting capabilities, supports a cost-effective transition to people-centric IT.

Microsoft Desktop Virtualization enables IT to deliver corporate desktop and applications without compromising compliance. Apps and data stay in the datacenter or in the cloud, so the risk of information loss due to lost or stolen devices is reduced. Centralized desktops and apps, hosted in the datacenter or the cloud, can be easily managed, and apps and data can be secured. Administrators can set policy to control from where users can access the remote resources, what devices they can use for access, and whether features such as accessing local disks or USB devices from within the remote session are allowed.

Business Requirements

Scenario: Kelly is responsible for setting the security, access policies, and auditing for compliance with corporate policy. Her role has expanded, and she must now provide access to sensitive corporate information on devices that users provide without compromising network security or compliance requirements.

Kelly needs an enterprise solution that centralizes corporate resources and enables her to define policies that both enable users and allow her to remain in control of the information. Like in most enterprises, Kelly has responsibility for data stored in multiple locations, so she requires a centralized solution for setting and enforcing policy, and for configuring auditing policies for reporting.

The People-Centric IT Solution

Windows Server 2012 delivered a new solution, Dynamic Access Control, which allows IT to configure content classification policies along with dynamic conditional access policies and actions based on the outcome of the classification process, such as automatically encrypting documents using Rights Management Services.

With Windows Server 2012 R2, IT can now publish access to corporate resources using the Web Application Proxy and, through integration with ADFS, enforce conditional access policies with multi-factor authentication. IT can also enable users to sync their files to their devices using Work Folders, and this includes integration with the Dynamic Access Control policies.

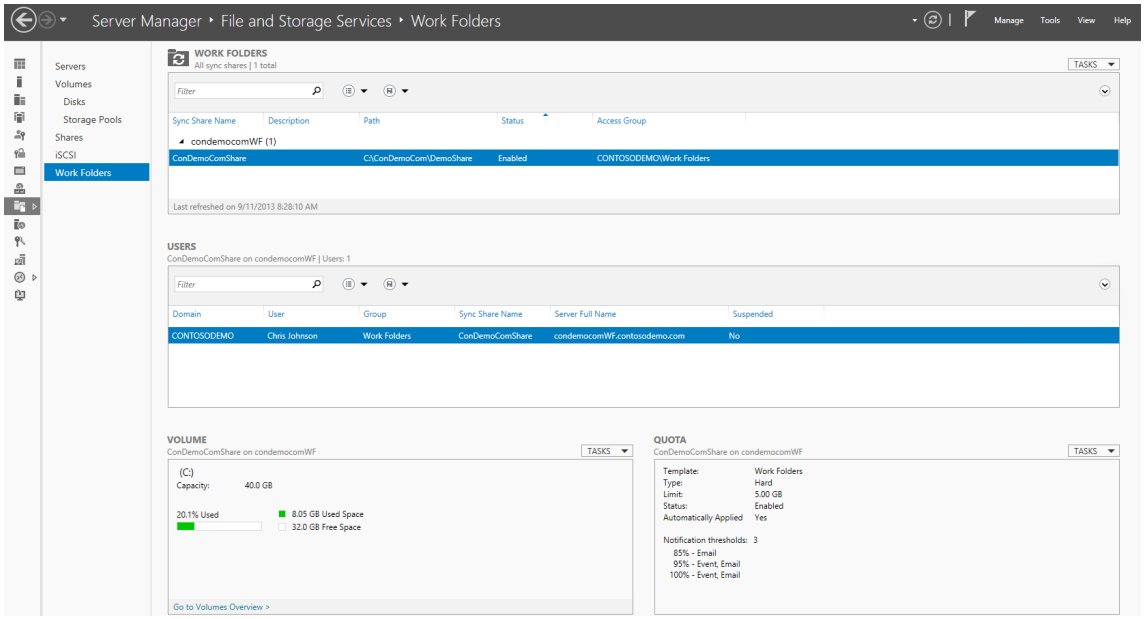


Figure 12 Manage Work Folders with Windows Server 2012 R2

Enabling users to get their work done while providing IT the control that helps them protect information and remain compliant is required for organizations adopting BYOD as part of a people-centric model.

Windows Server 2012 R2

- With the Web Application Proxy, IT can selectively publish corporate resources to remote users based on user, device, location (internal or external), and application.
- IT can safeguard data when it's distributed outside the corporate network by controlling whether a user can open, modify, print, forward, or take other action with rights-managed information. Active Directory Rights Management Services protects Microsoft Office documents and Exchange email by identifying the rights that a user has to the file and removing the option to perform actions outside those rights.
- IT can set central access policies and classify data to protect important information on their file servers by using Dynamic Access Control, which includes the ability to automatically encrypt documents with Rights Management.
- Using Dynamic Access Control audit functionality, IT can generate reports that show which users have accessed classified information.
- Using Work Folders, users can synchronize files on corporate servers with their devices from virtually anywhere through a sync service, and IT can apply Dynamic Access Control policies to this data.

Azure RemoteApp

- Azure RemoteApp provides a secure application delivery solution: Applications aren't sent to or stored on user devices; instead, they're centralized in Azure. Users access their corporate applications through Microsoft's Remote Desktop Protocol (RDP).
- Leading governments, financial services organizations, and companies around the world rely on Microsoft because our services are global, reliable, and designed for fault tolerance. With Azure RemoteApp, users can centralize and protect their data in Azure's trusted and protected platform.

Supporting Features

Feature	Description	Product
Web Application Proxy	Allows the publishing of corporate resources to external users and devices, and, through integration with ADFS, can enforce multi-factor authentication and conditional access polices when users connect to resources.	Windows Server 2012 R2
Dynamic Access Control	Provides the ability to classify and set conditional policies for which users and devices can access certain information, and allows tasks such as automatic encryption with Rights Management.	Windows Server 2012 Windows Server 2012 R2

Work Folders	Provides a centralized location on a file server in the corporate environment that's configured to allow the synchronization of files with user devices. Work Folders can be published directly through a reverse proxy or integrated with ADFS and published via the Web Application Proxy for conditional access policy enforcement.	Windows Server 2012 R2
Remote Desktop Services (RDS)	Provides a solution to deliver corporate desktops and applications to unmanaged devices. Desktops and applications are streamed but never stored on the device. IT can publish session-based desktops, RemoteApp, or pooled or personal virtual desktops from a single unified console.	Windows Server 2012 R2
Cloud-based RemoteApps	Provides Windows Server-based applications delivered from the trusted and reliable Azure platform. Corporate applications are centralized on Azure and never stored on user devices.	Azure RemoteApp

Conclusion

Windows Server 2012 R2 gives IT the ability to make sensitive corporate information available to users, while retaining control over which users and devices can access the information through the enforcement of conditional access policies.

Enable Multi-Factor Authentication and Rights Management Services

As the enterprise adapts to the proliferation of consumer devices attempting to access the network, the security model must evolve to allow for consistent secure access to corporate resources based on a combination of factors, including user, device type, and location. With tools that enable IT security professionals to manage and federate user identities and credentials across the organization and in the cloud, Microsoft makes it possible to provide users with secure, always available access to the corporate network.

Business Requirements

Scenario: John is responsible for the security of the corporate network. In the past, users were directly connected to the internal network while on site through domain authentication. For users who needed remote access, it was required that they used corporate-provided equipment configured with multi-layer authentication procedures. Now that John's company is allowing users to work on their own devices from virtually anywhere, John must create a solution for user devices that enables remote access to corporate applications and data via highly secure and always-on connections.

IT needs a way develop a multi-layer security solution that allows remote access to corporate applications and data via secure connections regardless of the device being used. The users this security model supports want a consistent authentication process for accessing company resources. The authentication process must also protect corporate data from unauthorized access.

The People-Centric IT Solution

Windows Server 2012 R2 provides an information protection solution that includes multi-factor authentication and data encryption. IT can grant access based on user, device, and location, and selectively publish corporate resources to remote users, integrating with multi-factor authentication at the back end and providing a single sign-on experience for users.

With Microsoft Azure Multi-Factor Authentication (formerly PhoneFactor), Microsoft has integrated this service into the ADFS role, as well as continuing to make it available to Windows Server customers for integration with Active Directory and other applications.

Windows Server 2012 R2

- IT can control access to company resources based on the identity of the user, the identity of the registered device, and the user's network location (whether the user is within the corporate boundary or not).
- With the Web Application Proxy, IT can selectively publish corporate resources to remote users using managed and unmanaged devices.
- With multi-factor authentication integrated into ADFS, IT can take advantage of additional layers of authentication as users and devices connect to the corporate environment.

Supporting Features

Feature	Description	Product
Active Directory Federation Services (ADFS)	Through Microsoft Azure Multi-Factor Authentication (formerly PhoneFactor), IT can apply additional layers of authentication and verification of users and devices.	Windows Server 2012 R2 Windows Azure Multi-Factor Authentication
Web Application Proxy	Allows the publishing of corporate resources to external users and devices.	Windows Server 2012 R2
Rights Management Services	Encrypts documents to prevent unwanted viewing or use of corporate data	Windows Server 2012 R2 Azure Rights Management

Conclusion

Microsoft provides IT with new ways to make corporate resources available on devices that are outside of corporate management or control. IT can use the additional layers of validation provided to help maintain security and to control access to sensitive information.

Summary

Summary

The consumerization of enterprise IT is an irreversible trend. Organizations that develop clear goals and policies to accommodate a burgeoning number of personal devices, ubiquitous information access, and the resulting flexible work styles can benefit from employees who are more motivated and productive—while retaining the efficient management and enterprise security and governance required by IT departments. Microsoft supports and enables the consumerization of IT and the associated flexible work styles—as part of people-centric IT.

That's why Microsoft consistently advises customers and partners to look across the entire consumerization stack—the user, device, applications, and data—to make sure proper policies and technologies are in place at each level. Rights management, dynamic access control, and auditing are just as important, if not more so, than the configuration policies for any particular device.

With an intelligent infrastructure built on Microsoft technologies, organizations can provide easy access to applications and data so that users can remain productive. With Microsoft tools, IT administrators can implement technologies and procedures to manage disparate devices. Microsoft tools also help to protect the organization's systems, data, and network.

Embracing and managing the consumerization of IT goes beyond simply allowing people to choose which devices they want to use. The Microsoft people-centric IT solution addresses these IT requirements:

- Devices must be easily integrated into the corporate infrastructure.
- Devices must be configured to become and remain compliant with corporate access and security policies as long as they're used for work.
- People must be able to access the applications and data they need to be productive in a consistent way.
- Corporate applications and data must be protected and accessed only by compliant devices.
- Corporate information must be removed from devices when they're lost, stolen, or replaced.

Together, Windows Server 2012 R2, System Center 2012 R2 Configuration Manager, Microsoft Azure, and Microsoft Intune help organizations address the consumerization of IT. With Microsoft's people-centric IT solution, organizations can empower their users, unify their environment, and protect their data, ultimately helping to embrace consumerization and a people- centric IT model, while maintaining corporate compliance.

Feature Summary

Enable Users		
Solution	**Feature**	**Products**
Simplify BYOD Registration and Enrollment	Web Application Proxy Active Directory Federation Services (ADFS) Device Management	Windows Server 2012 R2 System Center 2012 R2 Configuration Manager and Microsoft Intune
Enable Consistent Access to Corporate Resources	Work Folders Web Application Proxy Company Portal	Windows Server 2012 R2 System Center 2012 R2 Configuration Manager and Microsoft Intune
Deliver Windows Desktops and Applications with Microsoft Desktop Virtualization	Session Shadowing Deduplication Storage Storage Tiering RemoteApp Quick Reconnect Dynamic Resolution Change Codec and Display Improvements Microsoft Remote Desktop App	Windows Server 2012 R2 Windows Server 2012 R2 Azure RemoteApp
Automate How Users Connect to Internal Resources	Web Application Proxy Support for VPN, Email, and Wi-Fi Profiles	Windows Server 2012 R2 System Center 2012 R2 Configuration Manager and Microsoft Intune
Use a Single User Identify for Each User	Cloud-Based Identity Management Identity Synchronization	Azure Active Directory Premium Windows Server 2012 R2 Identity Manager Azure AD Sync

Unify Your Environment		
Solution	**Feature**	**Products**
Extend Your Existing System Center Configuration Manager Infrastructure and Manage Mobile Devices Through the Cloud	Unified Management Infrastructure	System Center 2012 R2 Configuration Manager and Microsoft Intune

Simplify User-Centric Management Across Devices	Mobile Device Management	System Center 2012 R2 Configuration Manager and Microsoft Intune
Enable Comprehensive Settings Management Across Platforms	Mobile Device Management Policies Software Distribution Distribution Point Usage Reports and Management	System Center 2012 R2 Configuration Manager and Microsoft Intune System Center 2012 R2 Configuration Manager
Define a Common Identity for Accessing Resources On-Premises and in the Cloud	Windows Server Active Directory Domain Services Microsoft Azure Active Directory	Windows Server 2012 R2 Microsoft Azure Active Directory

Protect Your Data		
Solution	**Feature**	**Products**
Selectively Wipe Devices	Selective Wipe	System Center 2012 R2 Configuration Manager and Microsoft Intune
Centralize Corporate Information for Compliance and Data Protection	Web Application Proxy Work Folders Dynamic Access Control Remote Desktop Services Microsoft Azure RemoteApp	Windows Server 2012 R2 Microsoft Azure
Enable Multi-factor Authentication and Rights Management Services	Active Directory Federation Services (ADFS) Web Application Proxy Active Rights Management Services	Microsoft Azure Multi-Factor Authentication Windows Server 2012 R2 Windows Server 2012 R2 Microsoft Azure Rights Management