Microsoft

# Windows Server 2012 R2

## Access & information protection

# Contents

# Introduction

**In a world with many consumer devices and constant mobility, organizations and their IT departments face significant new challenges. With the prevalence, speed, and availability of affordable high-speed cellular and Wi-Fi networks, end users are increasingly mobile and expect to have access to both personal and corporate information—from anywhere and on any device.**

To meet these demands and still retain control of corporate data and meet compliance requirements, organizations need capabilities that provide access to corporate resources and enable information protection. Solutions must provide the means to manage a user's identity across resources found in the data center and those in the cloud; they must provide secure remote access and allow the organization to define which resources a user can access based on who they are, what data or resource they want to access, and which device they're using.

Although some factors, such as hybrid cloud implementations and a mobile workforce may add flexibility and reduce costs, they also lead to a more porous network perimeter. When organizations move more and more resources into the cloud and grant network access to mobile workers and business partners outside the firewall, managing security, identity, and access control becomes a greater challenge. Adding to this challenge are increasingly stringent regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Sarbanes-Oxley Act of 2002 (SOX), both of which increase the cost of compliance.

Some of the trends emerging in this new world of working include:

- Users want to be able to work productively from any location, connected to any network, and on a device of their choice
- Users want access to corporate applications and data from any location using multiple devices
- Users want to use a single set of credentials no matter which data, application or service they need to access; users want the same single set of credentials to work from all of their devices
- Users want seamless access to corporate applications and data from any location, regardless of whether the resources reside in private cloud data centers or on public cloud infrastructure
- IT pros want an access and information protection infrastructure that provides users with consistent access to corporate resources and is easy to deploy

- IT pros need to provide efficient and secure access to applications and data for mobile workers, partners, and customers who use devices that are not under the direct control of the organization

- IT pros need to ensure that corporate information is being accessed and shared appropriately, with the ability to audit against internal and regulatory requirements

With Windows Server 2012 R2, which builds on the Windows Server 2012 platform, Microsoft has delivered several new capabilities that allow us to deliver solutions that meet these requirements (see Table 1).

| Scenario | Windows Server features |
|---|---|
| Users can register their devices so that they can gain access to corporate resources on their own personal devices. | Workplace Join, Web Application Proxy, Active Directory Federation Services (AD FS) v3, Active Directory Domain Services (AD DS) |
| Users can enroll their devices for access so that they can gain access to the company portal and a consistent experience for locating applications and managing personal devices. | Windows Intune, System Center Configuration Manager |
| Users can synchronize their work files to all their devices. | Work Folders |
| The IT department can publish access to corporate resources to users working anywhere on any device. | Web Application Proxy |
| The IT department can enforce multi-factor authentication before allowing users to access corporate resources. | Windows Azure Multi-Factor Authentication, AD FS |
| The IT department can provide users with automatic connections to corporate resources located on the organization's private network. | Microsoft DirectAccess, virtual private network (VPN) |
| The IT department can ensure that compliance requirements are met and use automatic classification methods based on content, location, and device. | Dynamic Access Control, Active Directory Rights Management Services (AD RMS) |

*Table 1. Windows Server features by scenario*

This paper provides an introduction to these Windows Server 2012 and Windows Server 2012 R2 access and information protection technologies for IT pros.

# Building on your existing investments

**A major obstacle that IT pros face is the sheer volume of repetitive work that needs to be done, particularly when large deployments of physical or virtual desktops are involved. Manual work is not only time-consuming but makes systems less secure by introducing many opportunities for errors and misconfiguration. Previous versions of the Windows Server operating system helped reduce this type of work.**

For example, the Windows Server 2008 R2 operating system included the following improvements:

- **File classification infrastructure.** This new infrastructure for classifying files by tagging them enabled IT pros to more easily manage unstructured data in files based on their organizational value.
- **AD DS.** As part of the Information Protection Solution, AD DS was improved to make domain controllers easier to deploy, both on-premises and in the cloud.
- **System management and security.** The Windows PowerShell 2.0 command-line interface (CLI) enabled IT pros to automate many common tasks involved in deploying and managing desktops.

With Windows Server 2012, Microsoft built on these earlier improvements, making it even easier to configure, manage, and monitor users, resources, and devices to improve security and automate the audit process. In addition, Windows Server 2012 included the following new and enhanced identity, access, and data-protection features:

- **Dynamic Access Control** gives you the ability to automatically control and audit access to files in file shares across your organization based on the characteristics of both the files and the users requesting access to them. It uses claims to achieve this high degree of access control specificity. *Claims,* contained in security tokens, consist of assertions about a user or device, such as name or type, department, or security clearance. You can employ user claims, device claims, and file classification tags to centrally control and audit access to files as well as use Rights Management Services (RMS) to protect information in files across your organization.
- **AD DS** is important in new hybrid cloud infrastructures, because it supports the increased need for security, compliance, and access control. Furthermore, unlike many competing cloud services, which require users to have a separate set of credentials hosted with the provider, AD DS provides continuity between your on-premises and cloud resources so that users only need a single set of credentials no matter where the resources are located. A new deployment wizard and support for cloning virtual domain controllers makes AD DS

easier to virtualize and simpler to deploy, both locally and remotely. The introduction of AD DS and Windows PowerShell 3.0 integration and the ability to capture and record command-line syntax as you perform tasks in the Service Manager interface improves automation of manual tasks. Other new features include desktop activation support using AD DS and group Managed Service Accounts.

- **DirectAccess** allows nearly any user who has an Internet connection to more securely access corporate resources, such as email servers, shared folders, or internal websites, with the experience of being easily connected to the corporate network. Windows Server 2012 offers a new, unified management experience, allowing administrators to configure DirectAccess and legacy VPN connections from one location. Other enhancements simplify deployment and improve performance and scalability.

And now, Windows Server 2012 R2 builds on the features of Windows Server 2012 and earlier versions to further reduce the workload on IT pros and respond to emerging needs in a consumerized, People-Centric IT environment.

The way that workers—people—perceive technology and how they expect to access information continue to change, largely driven by the explosion of consumer devices and the ubiquitous access to information—at the office, at home, and on the move. Traditional boundaries between work and home life are blurred, and there is a growing belief that personal technology, selected and customized to fit users' personalities, activities, and schedules, should extend into the workplace.

At the same time, organizations need to make corporate data widely available, often using private or public clouds to let their users or customers get information when and where it's needed. Providing this availability, however, must be done in ways that protect the information and provide for solid, reliable identification of users.

Windows Server 2012 R2 delivers on Microsoft's vision of People-Centric IT—IT that puts users and their relationships with information first—in three main ways:

- Enabling users
- Unifying the environment with hybrid identity features
- Helping to protect data

Specific features in Windows Server 2012 R2 that help achieve these goals include:

- **Registering and enrolling devices.** Users can register their devices, which makes them known to the IT department, which can in turn use device authentication as part of providing access to corporate resources. In addition, users can enroll their devices with the Windows Intune management service, which provides them with the company portal for consistent access to applications and data and the ability to manage their devices.

- **Web Application Proxy.** Using the Web Application Proxy, the IT department can publish access to internal web applications, allowing access from user devices, either by native applications or via a web browser. The Web Application Proxy, in conjunction with AD FS, can also pre-authenticate the user and the device and enforce access policies.

- **Work Folders.** The Work Folders feature allows you to maintain control of corporate data by storing it on server file shares and also makes it available consistently across a user's multiple devices.

- **Hybrid Identity.** This combination of features provides for a single sign-on (SSO) experience, a common identity for access to external resources through federation, and consistent management for on-premises and cloud-based identity domains.

- **Policy-based access and extended Multi-Factor Authentication.** These features allow you to make information available to users but control how and where they can consume that information.

The remaining sections in this paper describe the new Access & Information Protection features in Windows Server 2012 R2 and the Windows Server 2012 platform in more detail.

# Enable users

**IT departments in a modern business face many challenges.**

Users want to use a device of their choice and have access to both their personal and work-related applications, data, and resources. This blending of work and personal worlds causes difficulty, especially if a device is lost, sold, or stolen. If a user leaves the company, how can the company ensure that no information is lost or made available to people not authorized for it?

Users also want easy ways to access their corporate applications from anywhere. Even with a state-of-the-art device and always-on high-speed connectivity, getting access to work-related applications and information can be challenging to users. Internal applications are not often available in public app stores or may not be available for the platform a device uses.

As frustrating as it is for users, it is also a challenge for the IT department. These devices are typically connected to public networks and not internal managed networks. As much as many IT departments want to empower users to work in these new ways, they also need to control access to sensitive information and remain in compliance with regulatory policies.

Microsoft is answering these challenges with several new solutions.

## Registering and enrolling devices

When users want to use their own device or an organization wants to stop supplying corporate devices, immediately concerns are raised, often by both the users and IT pros. The users need access to apps and data, and the IT department needs to ensure that corporate information remains secure and that the business continues to follow compliance and regulatory requirements.

With Windows Server 2012 R2, Microsoft introduces a new concept known as *device registration*. Users can register their Bring Your Own Device (BYOD) for SSO and access to corporate data using Workplace Join.

When a user choses to register a device by using Workplace Join, the device becomes "known" to the organization, allowing the organization's IT department to use device authentication as part of providing access to corporate resources. This is a "give and get" scenario: The user "gives" by registering the device and in turn "gets" access to resources. Although some users may not be willing to make their device known to the organization, the organization may in turn chose not to allow confidential information to be accessed from "unknown" devices.

As part of the registration process, a certificate is installed on the device, and a new device record is created in AD DS. This device record establishes a link between the user and their device. It is this record and the linked relationship that makes the device known to the IT department and that allows the device to be authenticated. The device itself is effectively a seamless second-factor authentication.

From a technical perspective, after the device is registered, it is now represented by a record in AD DS and as such can be used as part of a claims-based authentication process, referenced in conditional access policies.

Workplace Join is available immediately with the release of Windows Server 2012 R2 for Windows 8.1 clients and for Apple iOS devices. Microsoft plans to support additional types of devices over time.

An example of Workplace Join is shown in Figure 1. In this example, the sequence below is followed:

1. A user registers their personal device. If the user is connected to the organization's LAN, AD FS handles the registration directly, but if the user is located on an external network, the request is made through the Web Application Proxy.

2. For external users, Web Application Proxy passes the request to AD FS; for internal users, AD FS receives the request directly. AD FS authenticates the user against AD DS.

3. A record representing the user's device is created in AD DS and linked to the user. The record includes the thumbprint of a Public Key Infrastructure certificate, issued by AD FS, which will be installed on the device.

4. The certificate is installed on the device, which completes the registration of the device through Workplace Join.

5. The user attempts to access an on-premises or cloud-based application. The application may be hosted on Windows Azure or published with the Web Application Proxy.

6. The application requests that AD FS authenticate the user and authorize access based on any conditional access policies that have been defined.

7. AD FS can be configured to examine a variety of claims, including the user's AD DS credentials, device registration, or Multi-Factor Authentication.

8. Apps can also be configured to use Windows Azure Multi-Factor Authentication, which is integrated with AD FS.

9. If the claims meet the requirements the administrators have defined, access is granted to the app. Otherwise, access is denied. You can configure a custom message that explains to the user why access was denied.

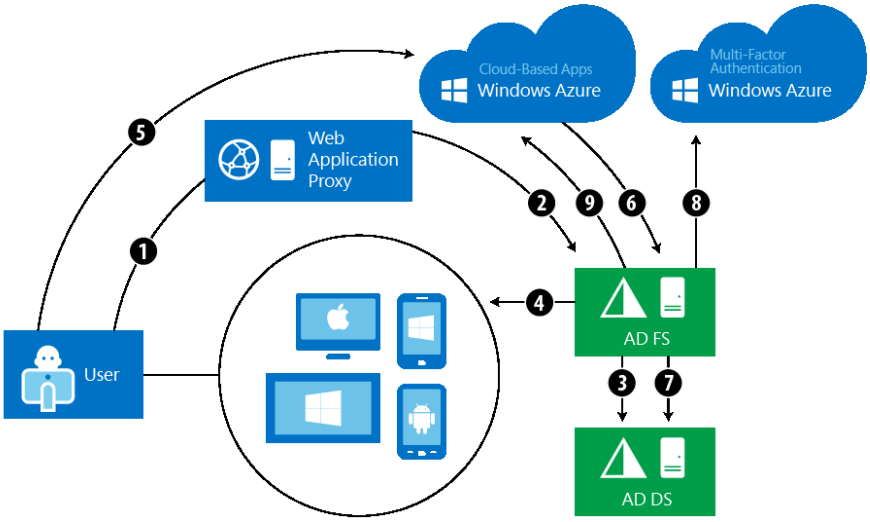


*Figure 1. Workplace Join*

Beyond registering a device, users can enroll their devices with the Windows Intune management service. Doing so provides access to the company portal that provides users with consistent access to applications and data as well as management of their devices. Enrollment is an easy way for users to get all their corporate applications in one place.

IT pros can populate the company portal with internal line-of-business (LOB) applications as well as links to applications that are available in the public app stores. From within the company portal, users can also manage their devices and perform actions such as wiping a lost or replaced device.

From the IT pro side, another advantage to enrollment is that data from Windows Intune is synchronized with Microsoft System Center Configuration Manager, often used for on-premises device management, which can provide a unified management platform for devices locally (on-premises) and remotely (connected through the cloud).

# Publishing access to resources with the Web Application Proxy

A goal of People-Centric IT is that users can access corporate applications and data wherever they are on the device of their choice. In meeting this goal, though, the IT department needs a way to validate the user's identity, and there may be additional conditions, such as limiting access to certain types of devices or even to specific, known devices.

In Windows Server 2012 R2, organizations can use the Web Application Proxy to publish resources. The Web Application Proxy is tightly integrated with AD FS and uses the information stored in AD DS for both user identity information (user credentials) and the device registration information. Both types of information can then be used in the authentication or authorization process. In addition, users and potentially their devices can be pre-authenticated. Integration with Multi-Factor Authentication is also supported.

The Web Application Proxy can also provide a generic reverse-HTTPS proxy for publishing applications that will then use NTLM or Basic authentication to validate the user.

These two services allow you to choose to either pass-through authentication to the application or to leverage AD FS and apply conditional access rules for granular control over how and where the application can be accessed. Granular control can be implemented with applications that use AD FS claims such as Kerberos web apps, Microsoft Office Forms Based Access, and RESTful OAuth apps.

IT pros, as part of this publishing, can also use AD FS to authenticate users and devices with Multi-Factor Authentication, such as Windows Azure Multi-Factor Authentication. In this case, when users connect, they can be asked to provide not only their identity credentials but pass additional credential challenges. By publishing corporate resources with conditional access based on the user's identity, the user's device and location (internal versus external), the IT department has new levels of capability to control where information can be synchronized to and accessed from.

# Making corporate data available to users with Work Folders

Organizations often have vast amounts of user data. However, usually "user data" is "corporate data" and should be stored on corporate file servers. The organization needs to maintain control of the data but also needs to make it available. It has typically been difficult to do both, especially on mobile devices.

Users are well adapted at working around corporate restrictions. Their strategies have included emailing the documents to themselves; copying files to USB flash drives; or uploading data to consumer-based storage platforms such as Box.com, Dropbox, or SkyDrive. These strategies are often inconvenient for the user and result in a loss of control of corporate information, which in turn exposes the company to risk of data loss (the data becoming inaccessible to the corporation), data leakage (data being available to unauthorized users), and compliance failures.

With Work Folders, several goals are achieved. First, users can sync their work data to their devices, but information can still be classified and protection can be applied to sensitive data. Second, the data is centralized—that is, a copy of the information is kept within the corporate realm so that the information is available and backed up.

Third, the IT department is able to selectively wipe the corporate data from clients in the event that the device is lost, stolen, or otherwise decommissioned or returned to solely personal use. This ability is delivered through the Windows Intune Selective Wipe Feature or through other management tools that make use of the Windows Encrypting File System application programming interface (API). The specific implementation of how the data is wiped varies by device platform. In all cases, information becomes inaccessible; where possible, it is removed.

Figure 2 demonstrates the use of Work Folders. Work Folders are implemented on file servers on which sync shares are set up. One share is configured per user, and a quota can be enforced. AD DS stores information about the location of each Work Folder. Domain-Joined devices on the corporate network can access Work Folders directly. For non-domain devices, or devices outside the corporate network, Work Folders can then be published directly through a reverse-proxy or conditional access can be enforced using AD FS, which in turn can use device registration information.

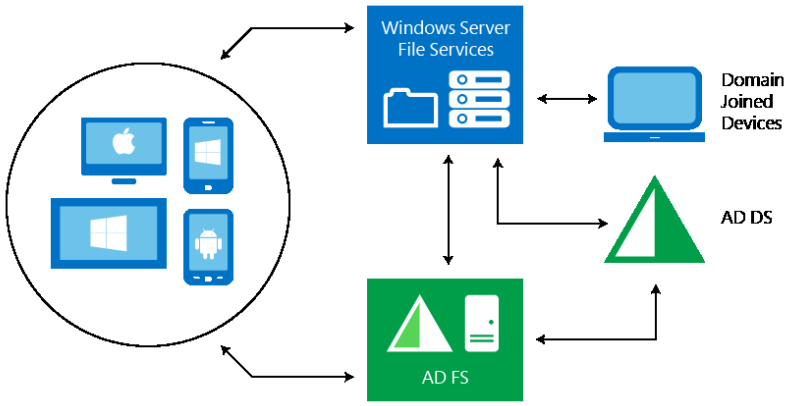


*Figure 2. Work Folders*

# DirectAccess and remote access

Windows Server 2012 R2 and the Windows Server 2012 platform provide an integrated remote access solution that is easier to deploy and manage compared with earlier versions that relied on multiple tools and consoles. Employees can gain access to corporate network resources while they work remotely, and IT administrators can manage corporate computers in AD DS that are located outside the internal network. Windows Server 2012 accomplishes this by integrating two existing remote access technologies: DirectAccess for automatic, transparent connectivity and traditional VPNs for compatibility.

**DirectAccess** was introduced in the Windows 7 and Windows Server 2008 R2 operating systems to help remote users more securely access shared resources, websites, and applications on an internal network without connecting to a VPN. DirectAccess establishes bidirectional connectivity with an organization's corporate network every time a DirectAccess-enabled computer is connected to the Internet. Users never have to think about connecting to the corporate network, and IT administrators can manage remote computers outside the office, even when the computers are not connected to the VPN. Windows Server 2012 R2 and Windows Server 2012 continue to offer this transparent connection to the corporate network, with improvements around deployment, management, performance, and scalability. Remote access improvements include:

- **Integrated remote access.** DirectAccess and VPNs can be configured together in the Remote Access Management console by using a single wizard. The new role allows easier migration of Windows 7 Routing and Remote Access Service (RRAS) and DirectAccess deployments.

- **Cross-premises connectivity.** Windows Server 2012 provides a highly cloud-optimized operating system. VPN site-to-site functionality in remote access provides cross-premises connectivity between enterprises and hosting service providers, including Windows Azure.

- **Improved management experience.** By using the new Remote Access Management console, you can configure, manage, and monitor multiple DirectAccess and VPN remote access servers in a single location. The console provides a dashboard that allows you to view information about server and client activity.

- **Simplified deployment.** In simple deployments, you can configure DirectAccess without being required to set up a certificate infrastructure. DirectAccess clients can now authenticate themselves by using only AD DS credentials; no computer certificate is required.

- **New deployment scenarios.** Remote access in Windows Server 2012 includes integrated deployment for several scenarios that required manual configuration in Windows Server 2008 R2, including force tunneling (which sends all traffic through the DirectAccess connection), Network Access Protection compliance, support for locating the nearest remote access server from DirectAccess clients in different geographical locations, and deploying DirectAccess for remote management only.

- **Improved scalability.** Remote access in Windows Server 2012 offers several scalability improvements that support more users while providing better performance and lower costs. These improvements include support for network load balancing (NLB), better performance in virtualized environments, and underlying platform improvements.

With DirectAccess, users who have an Internet connection can more securely access corporate resources, such as email servers, shared folders, or internal websites, with the experience of being easily connected to the corporate network.

DirectAccess transparently connects client computers to the internal network whenever the computer connects to the Internet, even before the user logs on, as shown in Figure 3. This transparent, automatic connectivity means that access is provided without additional steps or configuration required by the user.

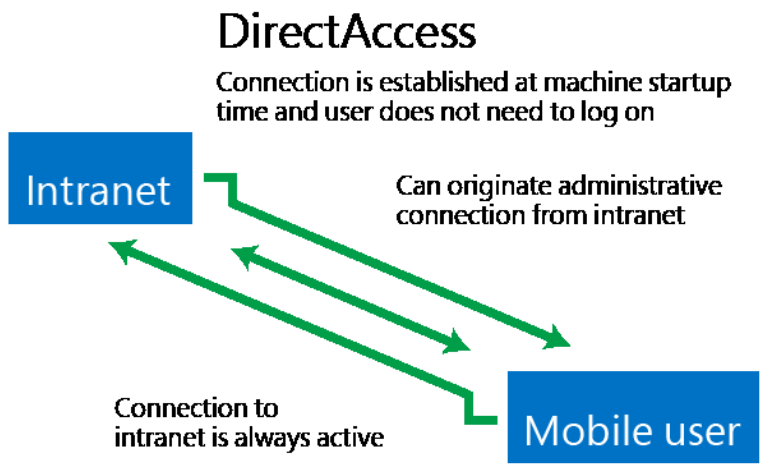


*Figure 3. DirectAccess connection architecture*

DirectAccess also lets you easily monitor connections and remotely manage DirectAccess client computers on the Internet.

At the same time, RRAS provides traditional client VPN connectivity for unmanaged client computers, such as computers running client operating systems earlier than Windows 7. In addition, RRAS site-to-site VPN provides connectivity between VPN servers, as shown in Figure 4.

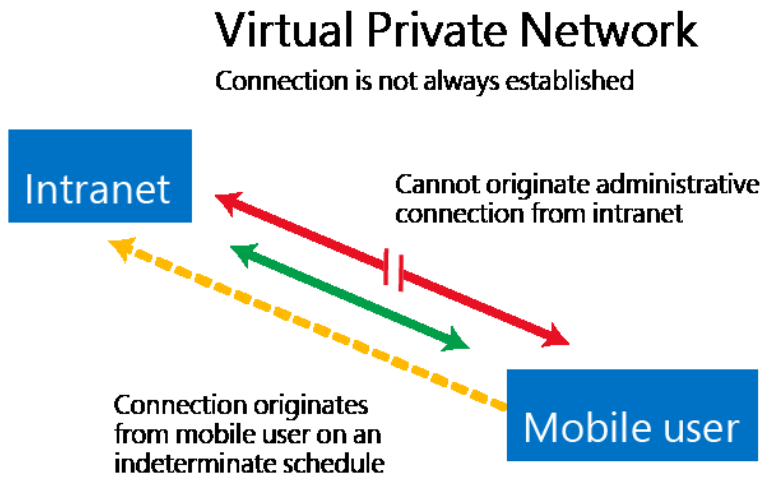


*Figure 4. VPN connection architecture*

The Remote Access Server role in Windows Server 2012 integrates DirectAccess and RRAS VPN. You can configure DirectAccess and VPNs together in the Remote Access Management console by using a single wizard. You can also configure other RRAS features by using the legacy RRAS management console. The new role allows easier migration of Windows 7 RRAS and DirectAccess deployments, and it provides new features and improvements.

## Cross-premises connectivity

Windows Server 2012 provides an operating system that is highly optimized for the cloud. VPN site-to-site functionality in remote access provides cross-premises connectivity between enterprises and hosting service providers. Cross-premises connectivity enables organizations to connect to private subnetworks in a hosted cloud network. It also enables connectivity between geographically separate enterprise locations.

With cross-premises connectivity, you can use existing networking equipment to connect to hosting providers by using the industry-standard Internet Key Exchange version 2 (IKEv2) and IP security (IPsec).

Figure 5 demonstrates how these two organizations implement cross-premises deployments by using Windows Server 2012.

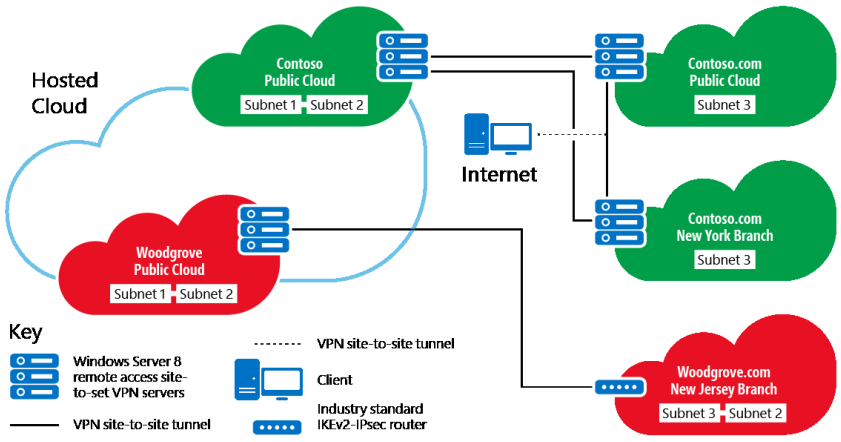


*Figure 5. Example of a cross-premises deployment*

The following steps are the procedures that Contoso and Woodgrove use for the cross-premises deployment shown in Figure 5:

1. Contoso.com and Woodgrove.com offload some of their enterprise infrastructure in a hosted cloud.

2. The hosting provider provides private clouds for each organization.

3. In the hosted cloud, virtual machines (VMs) running Windows Server 2012 are configured as remote access servers running site-to-site VPN.

4. In each hosted private cloud, a cluster of two or more remote access servers is deployed to provide continuous availability and failover.

5. Contoso.com has two branch office locations. In each location, a Windows Server 2012 remote access server is deployed to provide a cross-premises connectivity solution to the hosted cloud and between the branch offices.

6. The Contoso.com branch office computers running the Unified Remote Access Server role in Windows Server 2012 are also configured as DirectAccess servers in a multisite deployment. DirectAccess clients can access any resource in the Contoso.com public cloud or Contoso.com branch offices from nearly any location on the Internet.

7. Woodgrove.com can use existing routers to connect to the hosted cloud, because cross-premises functionality in Windows Server 2012 complies with IKEv2 and IPsec standards.

### Improved management experience

By using the new Remote Access Management console, you can configure, manage, and monitor multiple DirectAccess and VPN remote access servers in a single location. The console provides a dashboard that allows you to view information about server and client activity. You can also generate reports for additional, more detailed information. Operations status provides comprehensive monitoring information about specific server components. Event logs and tracing help diagnose specific issues. By using client monitoring, you can see detailed views of connected users and computers, and you can even monitor which resources the clients are accessing. Accounting data can be logged to a local database or a Remote Authentication Dial-In User Service server.

In addition to the Remote Access Management console, you can use Windows PowerShell CLI tools and automated scripts for remote access setup, configuration, management, monitoring, and troubleshooting.

On client computers, users can access the Network Connectivity Assistant application, integrated with Windows Network Connection

Manager, to see a concise view of the DirectAccess connection status and links to corporate help resources, diagnostics tools, and troubleshooting information. Users can also enter one-time password (OTP) credentials if OTP authentication for DirectAccess is configured.

### Easier deployment

The enhanced installation and configuration design in Windows Server 2012 allows you to set up a working deployment without changing your internal networking infrastructure. In simple deployments, you can configure DirectAccess without setting up a certificate infrastructure. DirectAccess clients can now authenticate themselves by using only AD DS credentials; no computer certificate is required. In addition, you can choose to use a self-signed certificate created automatically by DirectAccess for IP-HTTPS and for authentication of the network location server.

To further simplify deployment, DirectAccess in Windows Server 2012 supports access to internal servers that are running Internet Protocol version 4 (IPv4) only. An IP version 6 infrastructure is not required for DirectAccess deployment.

### Improved deployment scenarios

The Remote Access Server role in Windows Server 2012 has additional enhancements, including integrated deployment for several scenarios:

- With Windows Server 2012, you can now configure a DirectAccess server with two network adapters at the network edge or behind an edge device or with a single network adapter running behind a firewall or network address translation device. The ability to use a single adapter removes the requirement to have dedicated public IPv4 addresses for DirectAccess deployment. With this configuration, clients connect to the DirectAccess server by using IP-HTTPS.

- In Windows Server 2012, you can configure remote access servers in a multisite deployment that allows users in dispersed geographical locations to connect to the multisite entry point closest to them. You can distribute and balance traffic across the multisite deployment by using an external global load balancer. To support fault tolerance, redundancy, and scalability, DirectAccess servers can now be deployed in a cluster configuration that uses Windows load balancer or an external hardware load balancer.

- DirectAccess in Windows Server 2012 adds support for two-factor authentication that uses an OTP. For two-factor smart card authentication, Windows Server 2012 supports the use of Trusted Platform Module (TPM)–based virtual smart card capabilities that are available in the Windows 8 operating system. The TPM of client computers can act as a virtual smart card for two-factor

authentication, which reduces the overhead and costs incurred in smart card deployment.

- Windows Server 2012 also introduces the ability of computers to join an AD DS domain and receive domain settings remotely via the Internet. By using this capability, you will find that deployment of new computers in remote offices and provisioning of client settings to DirectAccess clients is easier. You can configure client computers running Windows 8, Windows 7, and Windows Server 2008 R2 as DirectAccess clients. Clients running Windows 8 have access to all DirectAccess features, and they have an improved experience when connecting from behind a proxy server that requires authentication. Clients not running Windows 8 have the following limitations:

  - They must download and install the DirectAccess Connectivity Assistant tool.

  - They require a computer certificate for authentication.

  - In a multisite deployment, they must be configured to always connect through the same entry point.

### Automatic VPN connection

New in Windows Server 2012 R2 are automatic VPN connections, which provide automated starting of the VPN when a user launches an app that requires access to corporate resources. The user may still be prompted for two-factor credentials, but the requirement to initiate the connection before starting the app is removed; the connection will start whenever an app requires it.

### Scalability improvements

Remote access offers several scalability improvements, including support for more users with better performance and lower costs:

- You can cluster multiple remote access servers for load balancing, continuous availability, and failover. Cluster traffic can be load balanced by using NLB or a non-Microsoft load balancer. Servers can be added to or removed from the cluster with few interruptions to the connections in progress.

- The Remote Access Server role takes advantage of Single Root I/O Virtualization for improved I/O performance when running on a VM. In addition, remote access improves the overall scalability of the server host with support for IPsec hardware offload capabilities, available on many server interface cards that perform packet encryption and decryption in hardware.

- Optimization improvements in IP-HTTPS use the encryption that IPsec provides. This optimization, combined with the removal of the

Secure Sockets Layer encryption requirement, increases scalability and performance.

With the new DirectAccess and remote access enhancements, you can easily provide more secure remote access connections for your users as well as log reports for monitoring and troubleshooting those connections. The new features in Windows Server 2012 support deployments in dispersed geographical locations, improved scalability with continuous availability, and improved performance in virtualized environments.

For more information, see "What's New in Remote Access in Windows Server 2012 R2" at http://technet.microsoft.com/en-us/library/dn383589.aspx

# Hybrid Identity

**By using Windows Server 2012 R2 and Windows Azure, organizations can build Hybrid Identity solutions to unify their environment across on-premises and cloud-based services and applications.**

Organizations face new challenges as applications move into the cloud, including wanting to provide users with a common identity when they are accessing resources, no matter where those resources are located; finding ways to manage the multiple identities that each user has; and keeping the information in sync across environments, databases, and authentication sources.

With Windows Server 2012 R2, you can build solutions that give users an SSO experience when accessing all resources; users can leverage a common identity for access to external resources through federation, and IT pros can consistently manage identities across on-premises and cloud-based identity domains.

AD DS has been at the center of IT infrastructure for more than 10 years, and its features, adoption, and business value have grown with each new release. Today, most AD DS infrastructure remains on premises, but the trend toward cloud computing is creating the need to deploy AD DS in the cloud, as well.

New hybrid infrastructures are emerging, and AD DS must support the needs of new and unique deployment models that include services hosted entirely in the cloud, services that consist of both cloud and on-premises components, and services that remain exclusively on premises. These new hybrid models further increase the importance of security and compliance and compound the already complex and time-consuming exercise of ensuring that access to information and services is appropriately audited and accurately expresses the intent of the organization.

# Active Directory on-premises

AD DS in Windows Server 2012 R2 addresses these emerging needs with features that help you more quickly and easily deploy domain controllers both on-premises and in the cloud; audit and authorize access to files; and perform administrative tasks at scale—either locally or remotely—through consistent graphical and scripted management interfaces. AD DS in Windows Server 2012 improvements include:

- Simpler on-premises deployment, which replaces DCpromo with a new, streamlined domain controller configuration wizard that is integrated with Server Manager and built on Windows PowerShell 3.0

- More rapid deployment of virtual domain controllers through cloning
- Better support for public and private cloud implementations through safer virtualization of domain controllers
- A consistent graphical and scripted management interface that enables you to perform tasks in the Active Directory Administrative Center and automatically generate the syntax required to fully automate the task in Windows PowerShell 3.0
- Functionality that uses AD DS to simplify client activations
- Group Managed Services Accounts for groups of servers, such as server clusters that share their identity and service principal name

Using these features, you can effectively and efficiently deploy and manage AD DS over multiple servers locally and around the globe.

# Simplified deployment

The new Active Directory Domain Services Configuration Wizard in Windows Server 2012 integrates all the required steps to deploy new domain controllers into a single graphical interface. It requires only one organization-level credential and can prepare the forest or domain by remotely targeting the appropriate operations' master role holders. It conducts extensive prerequisite validation tests that minimize the opportunity for errors that might have otherwise blocked or slowed the installation. The wizard is built on Windows PowerShell 3.0 and is integrated with Server Manager. It can configure multiple servers and remotely deploy domain controllers, resulting in a deployment experience that is simpler, more consistent, and less time-consuming.

The Active Directory Domain Services Configuration Wizard includes the following features:

- **Adprep integration into the AD DS deployment process.** This integration reduces the time required to deploy AD DS and reduces the chances for errors that might block domain controller promotion.
- **Remote execution against multiple servers.** This feature greatly reduces the probability of administrative errors and the overall time required for deployment, especially when you deploy multiple domain controllers across global countries or regions and domains.
- **Prerequisite validation.** This feature identifies potential errors before the deployment begins. You can correct error conditions before they occur without the concerns that result from a partially complete upgrade.

- **Configuration pages grouped in a sequence that mirrors the requirements of the most common promotion options.** With related options grouped in fewer wizard pages, this feature provides a better context for making installation choices and reduces the number of steps and time that is required to complete domain controller installation.

- **Options that were specified in the wizard are exported into a Windows PowerShell script.** This feature simplifies the process of automating later AD DS installations through automatically generated Windows PowerShell scripts.

## Deployment with cloning

With earlier versions of Windows Server, administrators found that deploying virtualized replica domain controllers was as labor intensive as deploying physical domain controllers. In theory, this should not be the case, because virtualization brings the possibility of cloning domain controllers instead of performing all deployment steps separately for each one. Domain controllers within the same domain or forest are nearly identical, except for name, IP address, and so on. Therefore, virtualization should be fairly easy. With earlier versions of Windows Server, however, deployment still involved many (redundant) steps.

With Windows Server 2012, you can deploy replica virtual domain controllers by "cloning" existing virtual domain controllers. This ability significantly reduces the number of steps and time involved by eliminating repetitive deployment tasks and also lets you fully deploy additional domain controllers that are authorized and configured for cloning by the AD DS domain administrator.

## Safer virtualization of domain controllers

AD DS has been successfully virtualized for several years, but features present in most hypervisors can invalidate strong assumptions that the Active Directory replication algorithms make—primarily, the assumption that the logical clocks the domain controllers use to determine relative levels of convergence only go forward in time. Windows Server 2012 includes improvements that enable virtual domain controllers to detect when snapshots are applied to a VM or a VM is copied, causing the domain controller clock to go backward in time.

This new functionality is made possible by a virtual domain controller that uses a unique ID exposed by the hypervisor, called the *VM GenerationID*. The VM GenerationID changes when the VM experiences an event that affects its position in time. The VM GenerationID is exposed to the VM's address space within its BIOS and is made available to its operating system and applications through a Windows Server 2012 driver.

During startup and before completing any transactions, a Windows Server 2012 virtual domain controller compares the current value of the VM GenerationID against the value that it stored in the directory. A mismatch is interpreted as a "rollback" event, and the domain controller uses safeguards in AD DS that are new to Windows Server 2012. The safeguards enable the virtual domain controller to converge with other domain controllers and prevent it from creating duplicate security principals.

For Windows Server 2012 virtual domain controllers to gain this extra level of protection, the virtual domain controller must be hosted on a VM GenerationID–aware hypervisor, such as Windows Server 2012 Hyper-V.

## Windows PowerShell script generation

The Windows PowerShell cmdlets for Active Directory are a set of tools that help you to manipulate and query AD DS by using Windows PowerShell commands and to create scripts that automate common administrative tasks. The Active Directory Administrative Center uses these cmdlets to query and modify AD DS according to the actions performed within the Active Directory Administrative Center.

In Windows Server 2012, the Windows PowerShell History viewer in the Active Directory Administrative Center, shown in Figure 6, lets an administrator view the Windows PowerShell commands as they execute in real time. For example, when you create a new fine-grained password policy, the Active Directory Administrative Center displays the equivalent Windows PowerShell commands in the Windows PowerShell History viewer task pane. You can then use those commands to automate the process by creating a Windows PowerShell script.

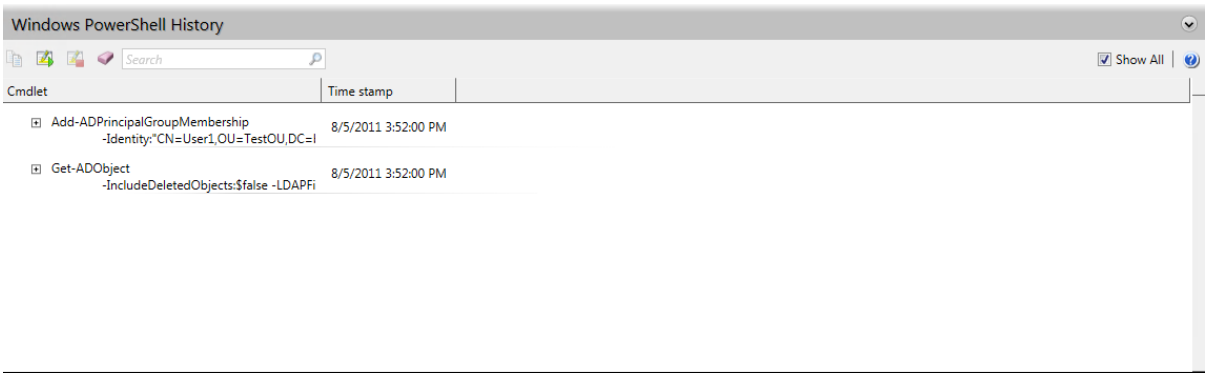


*Figure 6. Windows Server 2012 Windows PowerShell History viewer*

By combining scripts with scheduled tasks, you can automate everyday administrative duties that were previously completed manually. Because the cmdlets and required syntax are created for you, little experience with Windows PowerShell is required. Because the Windows PowerShell commands are the same as those the Active Directory Administrative Center executes, they should replicate their original function exactly.

# Active Directory for client activation

Client licensing is an additional labor-intensive task that can be eased with the improved Active Directory functionality in Windows Server 2012. With earlier versions of Windows Server, Microsoft Volume Licensing for Windows and Office required Key Management Service (KMS) servers. These servers entail several drawbacks:

- They require remote procedure call (RPC) network traffic, which some organizations want to disable.
- Additional training is necessary.
- The turnkey solution only covers approximately 90 percent of deployments.
- There is no graphical administration console, so the process is more complex than it needs to be.
- KMS does not support any kind of authentication, because the Microsoft Software License terms prohibit the customer from connecting the KMS server to any external network.
- Access to the service means that anyone can be activated.

This situation is improved in Windows Server 2012, because it helps leverage your existing Active Directory infrastructure to activate clients. No additional computers are required, and no RPC is needed. The activation uses Lightweight Directory Access Protocol (LDAP) exclusively and includes support for read-only domain controllers.

In this activation process, the only data written back to the directory is what's required for the installation and service. Activating the initial customer-specific volume license key requires the following:

- One-time contact with Microsoft Activation Services over the Internet (identical to retail activation)
- A key entered using the Volume Activation server role or the command line
- Repetition of the activation process for additional forests (by default, up to six times)

Another benefit of Active Directory integration is that the activation object is maintained in the configuration partition. This represents proof of purchase and means that the activated computers can be members of any domain in the forest. And, perhaps most important, with Active Directory activation integration, all computers that are running Windows 8 are automatically activated. This represents a significant workflow improvement over earlier versions of Windows Server and is achieved by using additional resources that are provided in Active Directory.

# Group Managed Service Account

Managed Service Accounts were a new type of account introduced in Windows Server 2008 R2 and Windows 7 to enhance the service isolation and manageability of network applications such as Microsoft SQL Server and Exchange Server. They eliminate the need for an administrator to manually administer the service principal name (SPN) and credentials for domain-level service accounts.

Until now, however, this feature has not been available for server groups, such as clusters, that share their identity and SPN. This creates a problem for IT administrators.

When a client connects to a service hosted on a server farm using NLB or some other method where all the servers appear to be the same service to the client, authentication protocols supporting mutual authentication, such as Kerberos, cannot be used unless all the instances of the services use the same principal (which means that they use the same passwords or keys to prove their identity). Service administrators find it difficult to manage this setup.

When a client connects to a shared service, it cannot know in advance which instance it will connect to, so the authentication must succeed regardless of the host. Therefore, each instance of the server must use the same security principal. Today, services have four principals to choose from, each with its own issues: computer, virtual, managed service, or user.

Computer, Managed Service Accounts, or virtual accounts cannot be shared across multiple systems, which leaves the option of using a user account for services on server farms. Because user accounts do not have password management, each organization then has to create a solution to update keys for the service in AD DS and distribute the keys to all instances of the services. This is expensive and problematic.

By creating a group Managed Service Account, services and service administrators do not have to manage password synchronization between service instances. The group Managed Service Account supports credential reset, hosts that are kept offline for some time, and

seamless management of member host group management for all instances of a service:

- You can deploy single-identity server farms or clusters on Windows Server 2012 to which domain clients can authenticate without knowing which instance of a server farm or cluster they are connecting to.
- You can configure services by using Service Control Manager to use a shared domain identity that automatically manages passwords.
- As soon as the group Managed Service Account is created, a domain administrator can delegate management of the group Managed Service Account to a service administrator.
- You can deploy single identity server farms or clusters on Windows Server 2012 servers running Windows 8 for identities in mixed-mode domains.

# Active Directory for the cloud

Today's organizations' identity solutions that have the flexibility to respond rapidly to new opportunities, many of which will be delivered through the cloud. As organizations move more and more resources into the cloud and grant network access to mobile workers and business partners outside the firewall, managing security, identity, and access control becomes a greater challenge.

In Windows Server 2012 R2, Microsoft enhanced Active Directory in a number of ways that support Hybrid Identity solutions and cloud infrastructure.

Organizations can leverage cloud platforms to run Windows Server AD DS and AD FS to reduce infrastructure on-premises. Microsoft supports running domain controllers and AD FS on Windows Azure Infrastructure as a Service, and these cloud services can be connected to the on-premises AD DS with the Windows Azure Virtual Network for secure site-to-site connections, including connecting your data center to Windows Azure. This combination can make it easier and faster to connect and authenticate cloud-based users, devices, and applications.

Developers can integrate applications for SSO across on-premises and cloud-based applications, providing a more productive experience for users and an easier way for customers to manage the identity of users within these applications.

### Managing cloud identities

As organizations blend their existing on-premises applications with new cloud-based services, they need ways to consistently manage identity

across their on-premises environments and cloud-based services. The primary goal is to make users more productive by having an SSO to all their resources.

This goal can be achieved in several ways:

- The IT department can provide users with a common identity across on-premises or cloud-based services by leveraging Windows Server AD DS, and then connecting to Windows Azure Active Directory.
- The IT department can use AD FS to connect with Windows Azure for a consistent cloud-based identity.
- Users can leverage their common identity through accounts in Windows Azure AD and use them in Windows Azure, Microsoft Office 365, and non-Microsoft applications.
- Developers can build applications that leverage the common identity model, integrating applications into AD DS on-premises or Windows Azure for cloud-based applications.

Directory Synchronization, or DirSync, synchronizes the local AD DS database with Windows Azure AD. Synchronizing credentials—password hashes—is optional. If you choose to synchronize credentials, then all authentication can happen against Windows Azure AD. If you prefer to have authentication occur against your on-premises AD DS, you can deploy AD FS for Federated authentication. Windows Azure Multi-Factor Authentication can provide additional control.

These scenarios are shown in Figure 7.

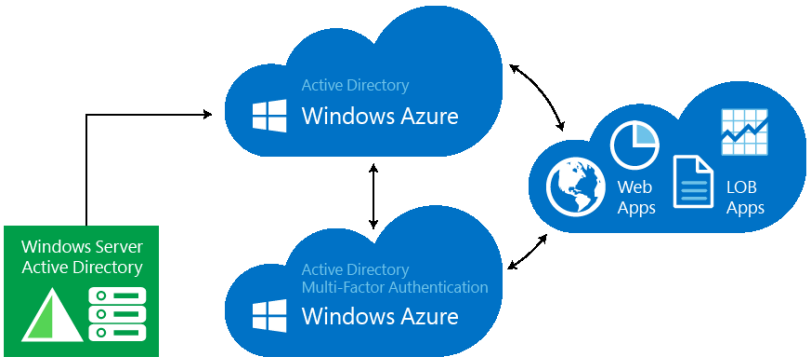


*Figure 7.Active Directory in the Cloud*

## Delivering a seamless user authentication experience

There are two main approaches to giving users a seamless experience.

In the first scenario, an on-premises AD DS forest is synchronized with Windows Azure AD by using DirSync. DirSync is configured to include the synchronization of the password hash and other user attributes. User authentication can be performed against Windows Azure AD or locally against AD DS. Organizations can also use Windows Azure to configure Multi-Factor Authentication.

Alternatively, organizations can use Federated authentication via AD FS. DirSync is used to replicate user attributes to Windows Azure AD but without synchronizing the password hashes. Instead, authentication is passed back to on-premises AD DS via federation, and the on-premises AD DS performs the authentication. In this case, AD FS can be configured, if desired, for Multi-Factor Authentication. In addition, AD FS can leverage Workplace Join or other claims presented by the user. AD FS is discussed in more detail in the following section.

With either of these approaches, the user need know only one set of credentials and authenticate the minimum number of times. See Figure 8.

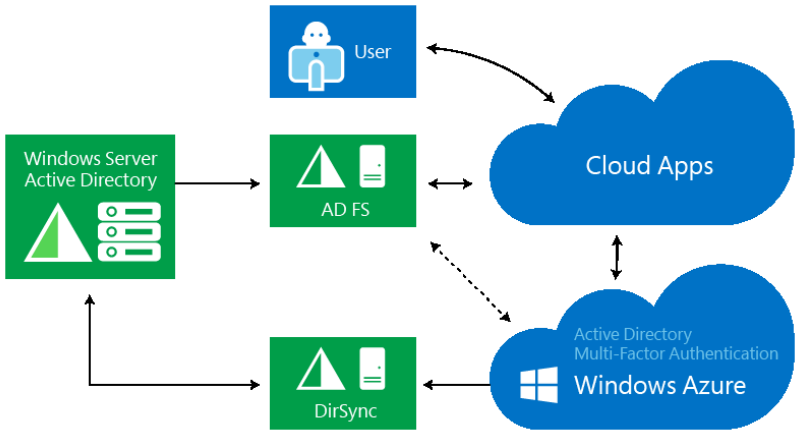


*Figure 8 Synchronizing or Federating with Windows Azure AD*

## Increasing the value in Active Directory Federation Services

AD FS simplifies end-user access to systems and applications by using a claims-based access authorization mechanism to maintain application security. Windows Server 2012 R2 offers significant enhancements to AD FS, including simplified deployment and management and the inclusion of a new plug-in model for Multi-Factor Authentication.

AD FS can be used to support a number of federated identity and claims-based scenarios. For example, conditional access with Multi-Factor Authentication is provided on a per-application basis, leveraging user identity, device registration, and network location. For external access, the Web Application Proxy is integrated with AD FS and makes it easy to publish applications securely.

In many cases, separate organizations need to interact with each other. AD FS allows organizations to federate with partners for seamless access to shared resources, allowing each organization to authenticate users from other federated organizations.

Finally, organizations can connect to Software as a Service applications running in Windows Azure, Office 365, and non-Microsoft providers, in each case providing users with an SSO experience.

Organizations can deploy AD FS to:

- Provide employees or customers with seamless access to web-based resources in any federated partner organization on the Internet without requiring employees or customers to log on more than once
- Retain complete control over employee or customer identities without using other sign-on providers
- Provide employees or customers with a web-based, SSO experience when they need remote access to internally hosted websites or services or to provide employees or customers with a web-based, SSO experience when they access cross-organizational websites or services from within the firewalls of your network
- Provide access control for apps that use claims directly for authentication
- Provide federated access control for Windows Store apps that use traditional Windows token-based authentication through the Windows Token-Based Agent

Windows Server 2012 R2 includes enhancements in AD FS to specifically support BYOD, such as the registration service, device authentication, and conditional access. Support for modern LOB apps include support for OAuth and JavaScript Object Notation Web Tokens.

The sign-in process for users has also been improved and now allows for extranet password changes, password expiry notifications, more easily customized sign-in experiences, soft account lockout and persistent SSO ("Keep Me Signed In"). Deployment has also been simplified for IT pros, including more graphical user interfaces (GUIs) and easier remote deployments of AD FS and the SQL Server databases required.

# Delivering single sign-on experiences

The new capabilities introduced with Windows Server 2012 R2 allow for devices that are known to the organization but not joined to the domain—in other words, there is a new "middle ground." With regard to AD DS, a device can be assigned to one of three possible states:

- **A user-provided device, which is "unknown" and over which the IT department has no control.** This device is not domain joined. Partial access can be provided to corporate information in this state, such as the ability to sync email or access information that is not sensitive.

- **When a user registers a device, it becomes "known" to the organization.** A certificate present on the device and the AD DS registration record allows for conditional access to corporate information. The device can effectively provide seamless two-factor authentication.

- **Domain-joined computers are under the full control of the organization** and can be provided with complete access to corporate information.

Depending on the "state" of the device, different types of SSO can be available. For example, browser session SSO is possible in all three states, because the sign-on is cached only so long as the browser is open and may be subject to time-out limits.

Seamless two-factor authentication for web apps is possible after the device has been registered. This functionality is achieved by leveraging the certificate on the device paired with the registration record in AD DS. Organizations can also enable enterprise apps with SSO after a device is registered.

Desktop SSO is possible only with a domain-joined device.

### Corporate identify management

Managing users' identity often involves some complex tasks that extend beyond management of the attributes of a user in AD DS. To support these advanced scenarios, Microsoft provides additional capabilities through Forefront Identity Manager (FIM) 2010 R2.

FIM 2010 R2 enables self-service group and distribution list management, including dynamic membership calculation based on the user's attributes; management of the complete life cycle of certificates and smart cards as well as integration with AD DS; the ability for users to reset their passwords at the Windows logon screen; synchronization of user identities across directories, including AD DS, Oracle, SQL Server,

IBM DS, and LDAP; and an easy-to-use portal through which users can manage their own identity attributes.

A common goal of many IT organizations is to reduce the administrative burden on IT staff, often through automation. FIM 2010 R2 provides an integrated solution for the automation of the processes, including on-boarding new users and the real-time de-provisioning from all systems when someone leaves the organization. In the case of de-provisioning, real-time actions help prevent unauthorized access and information leakage.

FIM 2010 R2 allows an organization to automatically synchronize all user information to different directories across the enterprise, creating a more productive environment and maintaining user identity across the entire environment.

### User provisioning, de-provisioning, and role updates

FIM 2010 R2 also includes built-in workflows for identity management to ensure that appropriate approvals are obtained for changes, as required.

# Protect your data

**As users bring their own devices to work, they will need or want to access sensitive information and in many cases will require access to this information locally on the device. As they go through their daily tasks, data is not only consumed on devices, but new data and updates are created. Thus, a significant amount of corporate data may exist only locally on user devices.**

The organization needs to be able to secure, classify, and protect data based not on where it resides but rather on the content it contains, including maintaining regulatory compliance. By implementing Windows Server 2012 R2, users can work on the device of their choice and be able to access all their resources, regardless of location or the device in use. The organization can enforce a set of central access and audit polices, be able to protect sensitive information based on content, and centrally audit and report on information access.

## Policy-based access to corporate information

In Windows Server 2012 R2, Microsoft has made it much easier to make information available to users but retain control of how and where they can consume the information.

Users can access corporate data regardless of device or location with Work Folders for data sync and desktop virtualization for centralized applications. Work Folders allow the publishing and synchronization of data from inside the corporate boundary to client devices (and vice versa). When applications are not able to or prohibited from being available locally on devices, Microsoft has desktop virtualization solutions to allow users to work effectively. IT pros can control the synchronization and access through policies.

Desktop virtualization, including Microsoft Virtual Desktop Infrastructure and RemoteApp technologies, allow access to applications without storing data on user devices, particularly for applications and data that should be kept centralized rather than being available locally on user devices.

The organization can publish resources using the Web Application Proxy and create business-driven access policies with Multi-Factor Authentication based on the content being accessed. AD FS is able to authenticate users and devices and make policy-based decisions on who and what can access information, including integration with Multi-Factor Authentication options such as Window Azure Multi-Factor Authentication and products from other providers through the plug-in model.

After access has been granted (or in cases where it is denied), the organization can audit access to information based on central audit policies, configured and distributed through Group Policy.

# Protecting data with Multi-Factor Authentication

One way to enforce Multi-Factor Authentication is by using Windows Azure Multi-Factor Authentication.

When an application is configured for Multi-Factor Authentication using Windows Azure, the following sequence occurs:

1. The user attempts to log in or perform an action that is subject to Multi-Factor Authentication.
2. When the user authenticates, the app or service performs a Multi-Factor Authentication call.
3. The user must respond to the challenge, which can be configured as a text, a phone call, or through a mobile app.
4. The response is returned to the app, which then allows the user to proceed.

Note that the organization can configure the type and frequency of the Multi-Factor Authentication to which the user must respond.

# Protecting data with Dynamic Access Control

Dynamic Access Control in Windows Server 2012 gives IT pros new ways to control access to file data and monitor regulatory compliance. It provides next-generation authorization and auditing controls, along with classification capabilities that let you apply information governance to the unstructured data on file servers.

Until now, file security was handled at the file and folder level. IT pros had little control over the way users handled security day to day. However, by using Dynamic Access Control, you can restrict access to sensitive files regardless of user actions by establishing and enforcing file security policy at the domain level, which is then enforced across all Windows Server 2012 file servers. For instance, if a development engineer accidentally posts confidential files to a publicly shared folder, those files can still be protected from access by unauthorized users.

In addition, security auditing is now more powerful than ever, and audit tools make it easier to prove compliance with regulatory standards, such as the requirement that access to health and biomedical information be appropriately guarded and regularly monitored.

Windows Server 2012 provides the following new and enhanced ways to control access to your files while providing authorized users the resources they need:

- **Classify.** Automatic and manual file classification using an improved file classification infrastructure. Several methods exist to manually or automatically apply classification tags to files on file servers across the organization.

- **Control.** Central access control for information governance. You can control access to classified files by applying central access policies (CAPs). CAPs is a new feature of Active Directory that enables you to define and enforce specific requirements for granting access to classified files. For example, you can define which users can have access to files that contain health information within the organization by using claims that might include employment status (such as full-time or contractor) or access method (such as managed computer or guest). You can even require two-factor authentication, such as that provided by smart cards. Central access control functionality includes the ability to provide automated assisted access-denied remediation when users have problems gaining access to files and shares.

- **Audit.** File access auditing for forensic analysis and compliance. You can audit access to files by using central audit policies—for example, to identify who gained (or tried to gain) access to highly sensitive information.

- **Protect.** Classification-based encryption. You can apply protection by using automatic RMS encryption for sensitive documents. For example, you can configure Dynamic Access Control to automatically apply RMS protection to all documents that contain HIPAA information. This feature requires a previously provisioned RMS environment.

Dynamic Access Control can provide these classification, control, audit, and protection capabilities, because it is built on top of the following technologies:

- A new Windows authorization and audit engine that can process conditional expressions and central policies

- Kerberos support for user claims and device claims within AD DS

- Improvements to the file classification infrastructure

- RMS extensibility support so that partners can provide solutions that encrypt non-Microsoft files

You can use the Dynamic Access Control API to extend these technologies and create custom classification tools, audit software, and more.

### Classification

The first step in establishing secure file access policies is to identify the files, and then classify them by applying tags to group files based on the information they contain. In Windows Server 2012, files are tagged in one of four ways:

- **By location.** When a file is stored on a file server, it inherits the tags from its parent folder. Folder owners specify the folder tags.
- **Manually.** Users and administrators can manually apply tags through File Explorer in Windows 8 or use data-entry apps to apply them.
- **Automatically.** Automatic classification processes in Windows Server 2012 can automatically tag files, depending on the content of the file. This method is useful for applying tags to large numbers of files.
- **By application API.** Apps can use APIs to tag files that they manage. For example, tags can be specified by LOB applications that store information on file servers or by data-management applications.

### Control access

Access to files is enforced by CAPs—sets of authorization policies that you centrally manage in AD DS and deploy to file servers by using Group Policy. You can use CAPs to comply with both organizational and regulatory requirements. CAPs help you to create more complete access policies by pairing information about files in the form of file tags with user and device claims.

In earlier versions of Windows Server, claims were used only by AD FS to authorize users in one domain to use applications in different, federated domains based on attributes submitted to AD FS. In Dynamic Access Control, the functionality of claims is essentially the same. In both cases, a claim consists of one or more statements (for example, name, identity, key, group, privilege, or capability) made about a user or device. These statements are contained in a security token that is issued and signed by a trusted partner or entity (such as AD DS) and used for authorizing that user or device to access a resource. You can create claim properties, either manually by using the Active Directory management tools or by using an identity management tool. In the case of Dynamic Access Control, the token is issued by AD DS, and the resource to be accessed is a file.

In Dynamic Access Control, claims can be combined into logical policies that enable fine-grained control over arbitrarily defined subsets of files. The following are two examples of situations where you might want to apply such policies:

- To obtain access to high-business-impact information, a user might be required to be a full-time employee. In this scenario, you would have to do the following:
  - Identify and tag the files that contain high-business-impact information.
  - Identify the full-time employees in your organization.
  - Create a CAP that applies to all files that have high business impact on all file servers across the organization.
- To enforce an organization-wide requirement to restrict access to personally identifiable information (PII) in files so that only the file owner and members of the human resources (HR) department are allowed to view it, you might implement a policy that applies to all PII files independent of their location. In this scenario, you would have to do the following:
  - Identify and classify (tag) the files that contain PII.
  - Identify the group of HR members who are allowed to view PII information.
  - Create a CAP that applies to all files that contain PII on all file servers across the organization.

The motivation to deploy and enforce an authorization policy can arise for different reasons and from multiple levels of the organization. The following are some examples:

- **Organization-wide authorization policy.** Most commonly initiated from the information security office, this type of authorization policy arises from compliance or another high-level requirement that is relevant across the organization. For example, only full-time employees should be able to access high-business-impact files.
- **Departmental authorization policy.** Various departments in an organization may have special data-handling requirements that they want to enforce. For example, the finance department might want to limit access to finance servers to finance employees.
- **Specific data-management policy.** This type of policy usually arises from compliance and organizational requirements for protecting information that is being managed, such as to prevent modification or deletion of files that are under retention or files that are subject to electronic discovery.

- **Need-to-know policy.** This type of policy is typically used in conjunction with the policy types mentioned earlier. The following are two examples:

  - Vendors should be able to access and edit only those files that relate to a project that they are working on.

  - In financial institutions, information barriers are important so that analysts do not access brokerage information and brokers do not access analysis information.

### The structure of central access policies

CAPs stored in AD DS act as security umbrellas that an organization applies across its file servers. These policies supplement but do not replace the local access policy or discretionary access control list (DACL) applied to files and folders. For example, if a local DACL allows access to a specific user but a CAP that is applied to the file denies access to the same user, the user cannot access the file. The reverse also applies: If a CAP allows access to a user but the local DACL denies it, the user cannot access the file. File access is possible only when permitted by both local DACL and CAP.

A CAP can contain many rules, each of which is evaluated and deployed as part of an overall CAP. Each rule contained in the CAP has the following logical parts:

- **Applicability.** This is a condition that defines which files the rule applies to. For example, the condition can define all files tagged as containing personal information.

- **Access conditions.** This is a list of one or more access control entries that define who can access the data, such as allowing Read and Write access if the user has a high clearance level and their device is a managed device.

Figure 9 shows the components of a CAP rule and how they can be combined to create explicit data access policies.

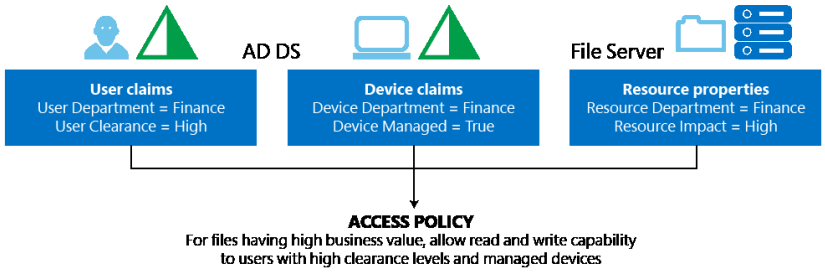


*Figure 9. CAP components*

## Central access policies and file servers

Figure 10 shows the interrelationships between AD DS, where CAPs, user claims, and property definitions are defined and stored; the file server, where these policies are applied; and the user, who is trying to gain access to a file on the file server.

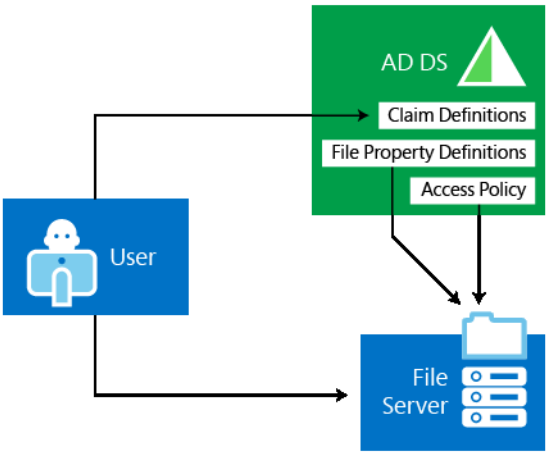


*Figure 10. CAP structure*

Figure 11 shows how you can combine different rules (blue boxes) into a CAP (green boxes) that can then be applied to shares on file servers across the organization.

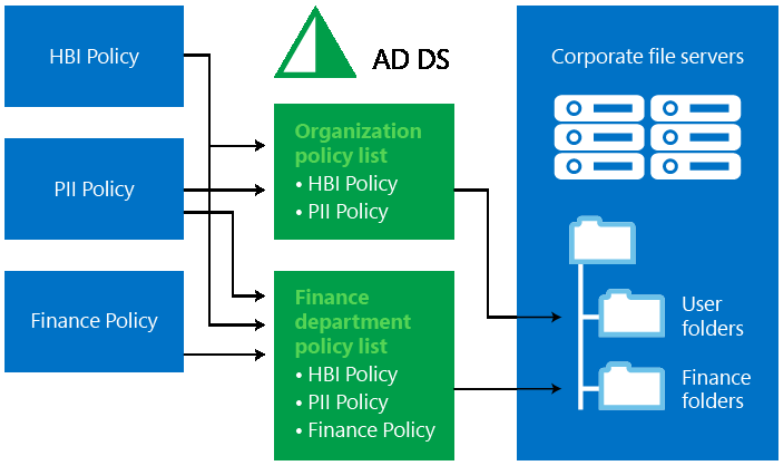


*Figure 11. Combining multiple policies into policy lists and applying them to resources*

## Policy staging

When you want to change a policy, Windows Server 2012 lets you test a proposed policy that runs parallel to the current policy so that you can identify the consequences of the new policy without enforcing it. This feature, which is known as *policy staging,* lets you measure the effects of a new policy in the production environment.

When policy staging is enabled, Windows Server 2012 continues to use the current policy to authorize user access to files. However, if the access the proposed policy allows differs from that of the current policy, the system logs an event with the details. You can use the logged events to determine whether the policy has to be changed or is ready to be deployed.

## Access-denied remediation

Of course, denying access is only part of an effective central access control strategy, and sometimes access must be granted after first being denied. Today, when access is denied, the user does not receive additional information on how to get access, which causes a lot of pain both for users and for help desk or IT administrators. To mitigate this problem, assisted access-denied remediation in Windows Server 2012 enables you to provide the user with additional information and the opportunity to send an access request email message to the appropriate owner. Access-denied remediation reduces the need for manual intervention by providing the following three processes for granting users access to resources:

- **Self-remediation.** If users can determine what the issue is and correct the problem so that they can get the requested access, the impact on the organization is low, and minimal special exceptions are needed in the organization policy. Windows Server 2012 helps you to create a general access-denied message to help users self-remediate when access is denied. This message can include URLs to direct the users to self-remediation websites that the organization provides.

- **Remediation by the file owner.** Windows Server 2012 enables you to create a distribution list of file or folder owners so that users can directly connect with them to request access. This resembles the Microsoft SharePoint model, where the share owner receives a user's request for access to a file. Remediation can range from adding user rights to the appropriate file or folder to editing share permissions. For example, if a local DACL on a file allows access to a specific user but a CAP restricts access to the same user, the user will be unable to gain access to the file. In Windows Server 2012, when a user requests access to a file or folder, an email message with the request details is sent to the file owner. When additional help is required, the file owner can in turn forward this information to the appropriate IT administrator.

- **Remediation by help desk and file server administrators.** When the user cannot self-remediate an access problem and the file owner cannot help, the help desk or file server administrator can correct the issue manually. This is the most costly and time-consuming remediation. Windows Server 2012 provides a UI to view the effective permissions for users on a file or a folder so that it is easier to troubleshoot access issues.

Figure 12 shows the series of events involved in access-denied remediation.

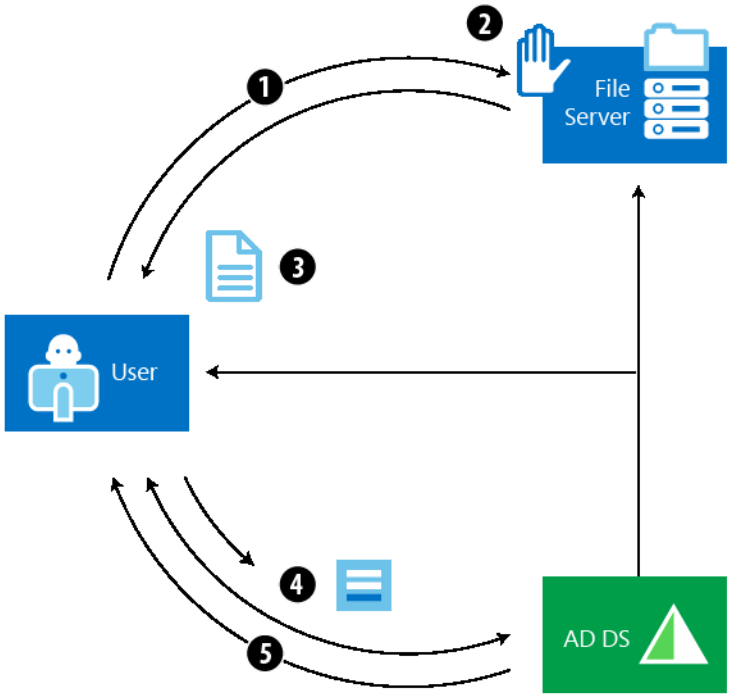


*Figure 12. Access-denied remediation*

Access-denied remediation provides a user with access to a file after access has initially been denied:

1. The user attempts to read a file.
2. The server returns an "access denied" error message, because the user has not been assigned the appropriate claims.
3. On a computer running Windows 8, Windows retrieves the access information from the File Server Resource Manager on the file server and presents a message with the access-remediation options, which may include a link for requesting access.
4. When the user has satisfied the access requirements (for example, by signing a nondisclosure agreement or providing other authentication), the user's claims are updated.
5. The user can access the file.

## Security auditing

Security auditing of file access is one of the most powerful tools to help maintain the security of an organization. A key goal of security auditing is regulatory compliance. For example, industry standards such as SOX, HIPAA, and Payment Card Industry (PCI) require organizations to follow a strict set of rules related to data security and privacy. Security audits help establish the presence or absence of such policies and thereby prove compliance or noncompliance with these standards. In addition, security audits help detect anomalous behavior, identify and reduce gaps in security policy, and deter irresponsible behavior by creating a trail of user activity that can be used for forensic analysis. Audit policy requirements typically arise from three levels:

- **Information security.** File access audit trails are frequently used for forensic analysis and intrusion detection. The ability to monitor specified events regarding access to high-value information lets organizations significantly improve their response time and investigative accuracy.

- **Organizational policy.** For example, organizations regulated by PCI standards can have a central policy to monitor access to all files that are marked as containing credit card information and PII, or organizations may want to monitor all unauthorized attempts to view information about their projects.

- **Departmental policy.** For example, the finance department may require that the ability to modify certain finance documents (such as a quarterly earnings report) be restricted to the finance department and thus want to monitor all other attempts to change these documents. In addition, the compliance department may want to monitor all changes to central policies and policy constructs such as user, computer, and resource attributes.

One of the biggest considerations for security audits is the cost of collecting, storing, and analyzing audit events. If the audit policies are too broad, the volume of audit events that are collected increases, making it more time-consuming and expensive to identify the most important audit events. However, if the audit policies are too narrow, you risk missing important events.

With Windows Server 2012, you can create audit policies by combining claims and resource properties (file tags). This combination leads to audit policies that are richer, more selective, and easier to manage by reducing the number of potential audit events to those most relevant to your auditing requirements. It enables scenarios that until now were either impossible or too difficult to implement. The following are examples of such audit policies:

- Audit everyone who does not have a high security clearance and yet tries to access a high-business-impact document. In this example, “high security clearance” is a claim, and “high business impact” is a file tag. The audit policy triggers an event when a user who does not have a high security clearance tries to gain access to a high-business-impact document.

- Audit all vendors when they try to access documents related to projects that they are not working on. In this example, the user’s claims include an employment status of “vendor” as well as a list of projects on which the user is authorized to work. In addition, each file in the organization to which a vendor could potentially have access was tagged to identify its associated project. The audit policy triggers an event if a vendor tries to access a project file and none of the projects in the vendor’s claim list matches the file’s project tag.

To view and query audit events, you can use familiar tools such as Event Viewer on the local server or Microsoft System Center Operations Manager Audit Collection Service across multiple servers. The Dynamic Access Control API also provides support for integrating Dynamic Access Control audit events into non-Microsoft audit software consoles. These tools help you to answer such questions as, “Who is accessing my high-business-impact data?” or “Was there an unauthorized attempt to access sensitive data?”

Figure 13 shows the file-access auditing workflow and the interrelationships between Active Directory, where claim types and resource properties are created; Group Policy, where the audit policies are defined and stored; the file server, where policies and resource properties are applied as file tags; and the user, who is trying to access information on the file server.

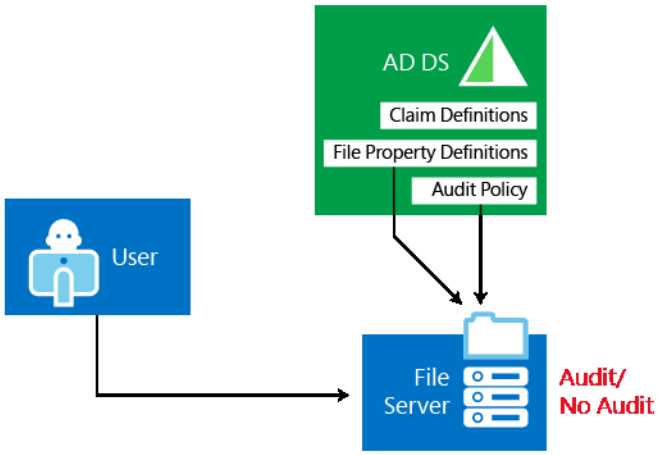


*Figure 13. Central auditing workflow*

## Protection

Protecting sensitive information involves reducing risk for the organization. Various regulations, such as HIPAA or the PCI Data Security Standard, require encryption of information, and there are many business reasons to encrypt sensitive information, as well. However, encryption is expensive and can adversely affect productivity. Therefore, organizations usually have different approaches and priorities for it.

To support this scenario, Windows Server 2012 lets you automatically encrypt sensitive Office files based on their classification. This is done through automatic file management of tasks that are running on the server and that start RMS protection for sensitive Office documents a few seconds after the file is identified as being a sensitive file on the file server (continuous file management tasks).

RMS encryption provides another layer of protection for files. If a person with access to a sensitive file inadvertently sends that file out through email, the file is still protected by the RMS encryption. Nearly any user who wants to gain access to the file must first authenticate to an RMS server to receive the decryption key. This process is illustrated in Figure 14.

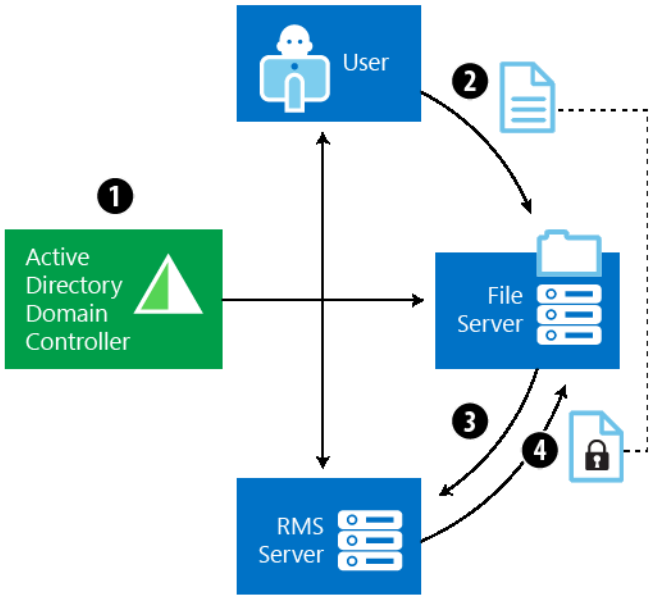


*Figure 14. Classification-based RMS protection*

Dynamic Access Control allows sensitive information to be automatically protected using Active Directory RMS:

1. A rule is created to automatically apply RMS protection to nearly any file that contains the word *confidential*.
2. A user creates a file with the word *confidential* in the text and saves it.
3. The RMS Dynamic Access Control classification engine, following rules set in the CAP, discovers the document with the word *confidential* and initiates RMS protection accordingly.
4. The RMS template and encryption are applied to the document on the file server, and it is classified and encrypted.

Note that support for non-Microsoft file formats is available through non-Microsoft vendors. Also be aware that if a file is RMS protected, data management features such as search- or content-based classification are no longer available for that file.

# Conclusion

**Access & Information Protection is an area that requires critical attention from IT pros, particularly when you move to virtualized and private- or public-cloud environments. Microsoft looks at delivering solutions in Windows Server 2012 R2 in three distinct ways:**

### Enable users

Enabling users is about ensuring that they can work on the device of their choice and access resources they need to get their jobs done.

### Hybrid Identity

Windows Server 2012 R2 offers unified solutions that can provide a consistent way to manage their environments regardless of where the services are delivered and consumed from. This is achieved through a common identity for users along with a unified way to manage identities.

### Protect your data

With Windows Server 2012 R2, users can access their information on the devices that they bring into the corporate world, while the IT department can ensure that corporate compliance policies are met.

# For more information

**With the release of Windows Server 2012 R2 and other supporting products, Microsoft offers a comprehensive solution to help you manage your users and devices. Microsoft encourages you to evaluate and deploy all of these technologies.**

More information about technologies and products mentioned in this paper is available from the Microsoft website.

### Related products

- Windows Server 2012 R2
- Microsoft System Center 2012 R2 Configuration Manager
- Windows Intune
- Windows Azure AD
- FIM 2010 R2

### Related solutions

- User and device management

### Technical resources

- Access and information protection
- Active Directory in Windows Server 2012 R2
- Active Directory Federation Services
- Work Folders overview
- Dynamic Access Control scenario overview
- DirectAccess, Routing and Remote Access overview