# Table of Contents

Windows Hello for Business Windows Hello for Business Overview How Windows Hello for Business works Manage Windows Hello for Business in your organization Why a PIN is better than a password Prepare people to use Windows Hello Windows Hello and password changes Windows Hello errors during PIN creation Event ID 300 - Windows Hello successfully created Windows Hello biometrics in the enterprise Planning a Windows Hello for Business Deployment Windows Hello for Business Deployment Guide Hybrid Azure AD Joined Key Trust Deployment Hybrid Azure AD Joined Certificate Trust Deployment **On Premises Key Trust Deployment On Premises Certificate Trust Deployment** Windows Hello for Business Features Multifactor Unlock

# Windows Hello for Business

4/9/2018 • 9 min to read • Edit Online

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

Windows Hello for Business lets user authenticate to an Active Directory or Azure Active Directory account.

Windows Hello addresses the following problems with passwords:

- Strong passwords can be difficult to remember, and users often reuse passwords on multiple sites.
- Server breaches can expose symmetric network credentials (passwords).
- Passwords are subject to replay attacks.
- Users can inadvertently expose their passwords due to phishing attacks.





Why PIN is better than a password

i i

Manage Windows Hello in your Organization

### Prerequisites

#### **Cloud Only Deployment**

- Windows 10, version 1511 or later
- Microsoft Azure Account
- Azure Active Directory
- Azure Multifactor authentication
- Modern Management (Intune or supported third-party MDM), optional
- Azure AD Premium subscription *optional*, needed for automatic MDM enrollment when the device joins Azure Active Directory

#### **Hybrid Deployments**

The table shows the minimum requirements for each deployment.

	CERTIFICATE TRUCT	VEN TRUCT	CEDTIFICATE TRUET
KET IKUSI	CERTIFICATE TRUST	KET IKUSI	CERTIFICATE TRUST
GROUP POLICY MANAGED	MIXED MANAGED	MODERN MANAGED	MODERN MANAGED

KEY TRUST GROUP POLICY MANAGED	CERTIFICATE TRUST MIXED MANAGED	KEY TRUST MODERN MANAGED	CERTIFICATE TRUST MODERN MANAGED
Windows 10, version 1511 or later	Hybrid Azure AD Joined: Minimum: Windows 10, version 1703 Best experience: Windows 10, version 1709 or later (supports synchronous certificate enrollment). Azure AD Joined: Windows 10, version 1511 or later	Windows 10, version 1511 or later	Windows 10, version 1511 or later
Windows Server 2016 Schema	Windows Server 2016 Schema	Windows Server 2016 Schema	Windows Server 2016 Schema
Windows Server 2008 R2 Domain/Forest functional level	Windows Server 2008 R2 Domain/Forest functional level	Windows Server 2008 R2 Domain/Forest functional level	Windows Server 2008 R2 Domain/Forest functional level
Windows Server 2016 Domain Controllers	Windows Server 2008 R2 or later Domain Controllers	Windows Server 2016 Domain Controllers	Windows Server 2008 R2 or later Domain Controllers
Windows Server 2012 or later Certificate Authority	Windows Server 2012 or later Certificate Authority	Windows Server 2012 or later Certificate Authority	Windows Server 2012 or later Certificate Authority
N/A	Windows Server 2016 AD FS with KB4088889 update (hybrid Azure AD joined clients), and Windows Server 2012 or later Network Device Enrollment Service (Azure AD joined)	N/A	Windows Server 2012 or later Network Device Enrollment Service
Azure MFA tenant, or AD FS w/Azure MFA adapter, or AD FS w/Azure MFA Server adapter, or AD FS w/3rd Party MFA Adapter	Azure MFA tenant, or AD FS w/Azure MFA adapter, or AD FS w/Azure MFA Server adapter, or AD FS w/3rd Party MFA Adapter	Azure MFA tenant, or AD FS w/Azure MFA adapter, or AD FS w/Azure MFA Server adapter, or AD FS w/3rd Party MFA Adapter	Azure MFA tenant, or AD FS w/Azure MFA adapter, or AD FS w/Azure MFA Server adapter, or AD FS w/3rd Party MFA Adapter
Azure Account	Azure Account	Azure Account	Azure Account
Azure Active Directory	Azure Active Directory	Azure Active Directory	Azure Active Directory
Azure AD Connect	Azure AD Connect	Azure AD Connect	Azure AD Connect
Azure AD Premium, optional	Azure AD Premium, needed for device writeback	Azure AD Premium, optional for automatic MDM enrollment	Azure AD Premium, optional for automatic MDM enrollment

#### **On-premises Deployments**

The table shows the minimum requirements for each deployment.

KEY TRUST GROUP POLICY MANAGED	CERTIFICATE TRUST GROUP POLICY MANAGED
Windows 10, version 1703 or later	Windows 10, version 1703 or later
Windows Server 2016 Schema	Windows Server 2016 Schema
Windows Server 2008 R2 Domain/Forest functional level	Windows Server 2008 R2 Domain/Forest functional level
Windows Server 2016 Domain Controllers	Windows Server 2008 R2 or later Domain Controllers
Windows Server 2012 or later Certificate Authority	Windows Server 2012 or later Certificate Authority
Windows Server 2016 AD FS with KB4088889 update	Windows Server 2016 AD FS with KB4088889 update
AD FS with Azure MFA Server, or AD FS with 3rd Party MFA Adapter	AD FS with Azure MFA Server, or AD FS with 3rd Party MFA Adapter
Azure Account, optional for Azure MFA billing	Azure Account, optional for Azure MFA billing

### Frequently Asked Questions

#### Can I deploy Windows Hello for Business using System Center Configuration Manager?

Windows Hello for Business deployments using System Center Configuration Manager need to move to the hybrid deployment model that uses Active Directory Federation Services. Deployments using System Center Configuration Manager will no long be supported after November 2018.

#### What is the password-less strategy?

Watch Senior Program Manager Karanbir Singh's Ignite 2017 presentation **Microsoft's guide for going password-less** 

#### What is the user experience for Windows Hello for Business?

The user experience for Windows Hello for Business occurs after user sign-in, after you deploy Windows Hello for Business policy settings to your environment.

#### What happens when my user forgets their PIN?

If the user can sign-in with a password, they can reset their PIN by clicking the "I forgot my PIN" link in settings. Beginning with the Fall Creators Update, users can reset their PIN above the lock screen by clicking the "I forgot my PIN" link on the PIN credential provider.

For on-premises deployments, devices must be well connected to their on-premises network (domain controllers and/or certificate authority) to reset their PINs. Hybrid customers can onboard their Azure tenant to use the Windows Hello for Business PIN reset service to reset their PINs without access to their corporate network.

#### Do I need Windows Server 2016 domain controllers?

There are many deployment options from which to choose. Some of those options require an adequate number of

Windows Server 2016 domain controllers in the site where you have deployed Windows Hello for Business. There are other deployment options that use existing Windows Server 2008 R2 or later domain controllers. Choose the deployment option that best suits your environment

#### Is Windows Hello for Business multifactor authentication?

Windows Hello for Business is two-factor authentication based the observed authentication factors of: something you have, something you know, and something part of you. Windows Hello for Business incorporates two of these factors: something you have (the user's private key protected by the device's security module) and something you know (your PIN). With the proper hardware, you can enhance the user experience by introducing biometrics. Using biometrics, you can replace the "something you know" authentication factor with the "something that is part of you" factor, with the assurances that users can fall back to the "something you know factor".

#### Can I use PIN and biometrics to unlock my device?

Starting in Windows 10, version 1709, you can use multifactor unlock to require the user to provide an additional factor to unlock the device. Authentication remains two-factor, but another factor is required before Windows allows the user to reach the desktop. Read more about multifactor unlock in Windows Hello for Business Features

#### What is the difference between Windows Hello and Windows Hello for Business

Windows Hello represents the biometric framework provided in Windows 10. Windows Hello enables users to use biometrics to sign into their devices by securely storing their username and password and releasing it for authentication when the user successfully identifies themselves using biometrics. Windows Hello for Business uses asymmetric keys protected by the device's security module that requires a user gesture (PIN or biometrics) to authenticate.

#### I have extended Active Directory to Azure Active Directory. Can I use the on-prem deployment model?

No. If your organization is federated or using online services, such as Office 365 or OneDrive, then you must use a hybrid deployment model. On-premises deployments are exclusive to organization who need more time before moving to the cloud and exclusively use Active Directory.

#### Does Windows Hello for Business prevent the use of simple PINs?

Yes. Our simple PIN algorithm looks for and disallows any PIN that has a constant delta from one digit to the next. This prevents repeating numbers, sequential numbers and simple patterns. So, for example:

- 1111 has a constant delta of 0, so it is not allowed
- 1234 has a constant delta of 1, so it is not allowed
- 1357 has a constant delta of 2, so it is not allowed
- 9630 has a constant delta of -3, so it is not allowed
- 1231 does not have a constant delta, so it is okay
- 1593 does not have a constant delta, so it is okay

This algorithm does not apply to alphanumeric PINs.

#### How does PIN caching work with Windows Hello for Business?

Windows Hello for Business provides a PIN caching user experience using a ticketing system. Rather than caching a PIN, processes cache a ticket they can use to request private key operations. Azure AD and Active Directory signin keys are cached under lock. This means the keys remain available for use without prompting as long as the user is interactively signed-in. Microsoft Account sign-in keys are considered transactional keys, which means the user is always prompted when accessing the key.

Beginning with Windows 10, Fall Creators Update, Windows Hello for Business used as a smart card (smart card emulation that is enabled by default) provides the same user experience of default smart card PIN caching. Each process requesting a private key operation will prompt the user for the PIN on first use. Subsequent private key operations will not prompt the user for the PIN.

The smart card emulation feature of Windows Hello for Business verifies the PIN and then discards the PIN in

exchange for a ticket. The process does not receive the PIN, but rather the ticket that grants them private key operations. Windows 10 does not provide any Group Policy settings to adjust this caching.

#### Can I disable the PIN while using Windows Hello for Business?

No. The movement away from passwords is accomplished by gradually reducing the use of the password. In the occurence where you cannot authenticate with biometrics, you need a fall back mechansim that is not a password. The PIN is the fall back mechansim. Disabling or hiding the PIN credential provider disabled the use of biometrics.

#### Does Windows Hello for Business work with third party federation servers?

Windows Hello for Business can work with any third-party federation servers that support the protocols used during provisioning experience. Interested third-parties can inquiry at whfbfeedback@microsoft.com

PROTOCOL	DESCRIPTION
[MS-KPP]: Key Provisioning Protocol	Specifies the Key Provisioning Protocol, which defines a mechanism for a client to register a set of cryptographic keys on a user and device pair.
[MS-OAPX]: OAuth 2.0 Protocol Extensions	Specifies the OAuth 2.0 Protocol Extensions, which are used to extend the OAuth 2.0 Authorization Framework. These extensions enable authorization features such as resource specification, request identifiers, and login hints.
[MS-OAPXBC]: OAuth 2.0 Protocol Extensions for Broker Clients	Specifies the OAuth 2.0 Protocol Extensions for Broker Clients, extensions to RFC6749 (The OAuth 2.0 Authorization Framework) that allow a broker client to obtain access tokens on behalf of calling clients.
[MS-OIDCE]: OpenID Connect 1.0 Protocol Extensions	Specifies the OpenID Connect 1.0 Protocol Extensions. These extensions define additional claims to carry information about the end user, including the user principal name, a locally unique identifier, a time for password expiration, and a URL for password change. These extensions also define additional provider metadata that enable the discovery of the issuer of access tokens and give additional information about provider capabilities.

#### Does Windows Hello for Business work with Mac and Linux clients?

Windows Hello for Business is a feature of Windows 10. At this time, Microsoft is not developing clients for other platforms. However, Microsoft is open to third parties who are interested in moving these platforms away from passwords. Interested third parties can inqury at whfbfeedback@microsoft.com

# Windows Hello for Business Overview

2/7/2018 • 7 min to read • Edit Online

#### **Applies to**

- Windows 10
- Windows 10 Mobile

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

#### NOTE

When Windows 10 first shipped, it included Microsoft Passport and Windows Hello, which worked together to provide multifactor authentication. To simplify deployment and improve supportability, Microsoft has combined these technologies into a single solution under the Windows Hello name. Customers who have already deployed these technologies will not experience any change in functionality. Customers who have yet to evaluate Windows Hello will find it easier to deploy due to simplified policies, documentation, and semantics.

Windows Hello addresses the following problems with passwords:

- Strong passwords can be difficult to remember, and users often reuse passwords on multiple sites.
- Server breaches can expose symmetric network credentials (passwords).
- Passwords are subject to replay attacks.
- Users can inadvertently expose their passwords due to phishing attacks.

Windows Hello lets users authenticate to:

- a Microsoft account.
- an Active Directory account.
- a Microsoft Azure Active Directory (Azure AD) account.
- Identity Provider Services or Relying Party Services that support Fast ID Online (FIDO) v2.0 authentication (in progress)

After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.

As an administrator in an enterprise or educational organization, you can create policies to manage Windows Hello for Business use on Windows 10-based devices that connect to your organization.

### Biometric sign-in

Windows Hello provides reliable, fully integrated biometric authentication based on facial recognition or fingerprint matching. Windows Hello uses a combination of special infrared (IR) cameras and software to increase accuracy and guard against spoofing. Major hardware vendors are shipping devices that have integrated Windows Hello-compatible cameras. Fingerprint reader hardware can be used or added to devices that don't currently have it. On devices that support Windows Hello, an easy biometric gesture unlocks users' credentials.

• Facial recognition. This type of biometric recognition uses special cameras that see in IR light, which allows

them to reliably tell the difference between a photograph or scan and a living person. Several vendors are shipping external cameras that incorporate this technology, and major laptop manufacturers are incorporating it into their devices, as well.

• **Fingerprint recognition**. This type of biometric recognition uses a capacitive fingerprint sensor to scan your fingerprint. Fingerprint readers have been available for Windows computers for years, but the current generation of sensors is significantly more reliable and less error-prone. Most existing fingerprint readers (whether external or integrated into laptops or USB keyboards) work with Windows 10.

Windows stores biometric data that is used to implement Windows Hello securely on the local device only. The biometric data doesn't roam and is never sent to external devices or servers. Because Windows Hello only stores biometric identification data on the device, there's no single collection point an attacker can compromise to steal biometric data.

# The difference between Windows Hello and Windows Hello for Business

- Individuals can create a PIN or biometric gesture on their personal devices for convenient sign-in. This use of Windows Hello is unique to the device on which it is set up, however it is not backed by asymmetric (public/private key) or certificate-based authentication.
- Windows Hello for Business, which is configured by Group Policy or mobile device management (MDM) policy, uses key-based or certificate-based authentication.
- Currently Active Directory accounts using Windows Hello are not backed by key-based or certificate-based authentication. Support for key-based or certificate-based authentication is on the roadmap for a future release.

### Benefits of Windows Hello

Reports of identity theft and large-scale hacking are frequent headlines. Nobody wants to be notified that their user name and password have been exposed.

You may wonder how a PIN can help protect a device better than a password. Passwords are shared secrets; they are entered on a device and transmitted over the network to the server. An intercepted account name and password can be used by anyone. Because they're stored on the server, a server breach can reveal those stored credentials.

In Windows 10, Windows Hello replaces passwords. When the identity provider supports keys, the Windows Hello provisioning process creates a cryptographic key pair bound to the Trusted Platform Module (TPM), if a device has a TPM, or in software. Access to these keys and obtaining a signature to validate user possession of the private key is enabled only by the PIN or biometric gesture. The two-step verification that takes place during Windows Hello enrollment creates a trusted relationship between the identity provider and the user when the public portion of the public/private key pair is sent to an identity provider and associated with a user account. When a user enters the gesture on the device, the identity provider knows from the combination of Hello keys and gesture that this is a verified identity and provides an authentication token that allows Windows 10 to access resources and services.

#### NOTE

Windows Hello as a convenience sign-in uses regular user name and password authentication, without the user entering the password.



Imagine that someone is looking over your shoulder as you get money from an ATM and sees the PIN that you enter. Having that PIN won't help them access your account because they don't have your ATM card. In the same way, learning your PIN for your device doesn't allow that attacker to access your account because the PIN is local to your specific device and doesn't enable any type of authentication from any other device.

Windows Hello helps protect user identities and user credentials. Because the user doesn't enter a password (except during provisioning), it helps circumvent phishing and brute force attacks. It also helps prevent server breaches because Windows Hello credentials are an asymmetric key pair, which helps prevent replay attacks when these keys are protected by TPMs.

### How Windows Hello for Business works: key points

- Windows Hello credentials are based on certificate or asymmetrical key pair. Windows Hello credentials can be bound to the device, and the token that is obtained using the credential is also bound to the device.
- Identity provider (such as Active Directory, Azure AD, or a Microsoft account) validates user identity and maps the Windows Hello public key to a user account during the registration step.
- Keys can be generated in hardware (TPM 1.2 or 2.0 for enterprises, and TPM 2.0 for consumers) or software, based on the policy.
- Authentication is the two-factor authentication with the combination of a key or certificate tied to a device and something that the person knows (a PIN) or something that the person is (Windows Hello). The Windows Hello gesture does not roam between devices and is not shared with the server; it is stored locally on a device.
- Private key never leaves a device when using TPM. The authenticating server has a public key that is mapped to the user account during the registration process.
- PIN entry and biometric gesture both trigger Windows 10 to use the private key to cryptographically sign data that is sent to the identity provider. The identity provider verifies the user's identity and authenticates the user.
- Personal (Microsoft account) and corporate (Active Directory or Azure AD) accounts use a single container for keys. All keys are separated by identity providers' domains to help ensure user privacy.
- Certificate private keys can be protected by the Windows Hello container and the Windows Hello gesture.

For details, see How Windows Hello for Business works.

### Comparing key-based and certificate-based authentication

Windows Hello for Business can use either keys (hardware or software) or certificates in hardware or software. Enterprises that have a public key infrastructure (PKI) for issuing and managing certificates can continue to use PKI in combination with Windows Hello. Enterprises that do not use PKI or want to reduce the effort associated with managing certificates can rely on key-based credentials for Windows Hello but still use certificates on their domain controllers as a root of trust.

### Learn more

Implementing Windows Hello for Business at Microsoft

Introduction to Windows Hello, video presentation on Microsoft Virtual Academy

What's new in Active Directory Domain Services (AD DS) in Windows Server Technical Preview

Windows Hello face authentication

**Biometrics hardware guidelines** 

Windows 10: Disrupting the Revolution of Cyber-Threats with Revolutionary Security!

Windows 10: The End Game for Passwords and Credential Theft?

Authenticating identities without passwords through Windows Hello for Business

- How Windows Hello for Business works
- Manage Windows Hello for Business in your organization
- Why a PIN is better than a password
- Prepare people to use Windows Hello
- Windows Hello and password changes
- Windows Hello errors during PIN creation
- Event ID 300 Windows Hello successfully created
- Windows Hello biometrics in the enterprise

# How Windows Hello for Business works

2/7/2018 • 12 min to read • Edit Online

#### Applies to

- Windows 10
- Windows 10 Mobile

Windows Hello for Business requires a registered device. When the device is set up, its user can use the device to authenticate to services. This topic explains how device registration works, what happens when a user requests authentication, how key material is stored and processed, and which servers and infrastructure components are involved in different parts of this process.

### Register a new user or device

A goal of device registration is to allow a user to open a brand-new device, securely join an organizational network to download and manage organizational data, and create a new Windows Hello gesture to secure the device. Microsoft refers to the process of setting up a device for use with Windows Hello as registration.

#### NOTE

This is separate from the organizational configuration required to use Windows Hello with Active Directory or Azure Active Directory (Azure AD); that configuration information is in Manage Windows Hello for Business in your organization. Organizational configuration must be completed before users can begin to register.

The registration process works like this:

- The user configures an account on the device. This account can be a local account on the device, a domain account stored in the on-premises Active Directory domain, a Microsoft account, or an Azure AD account. For a new device, this step may be as simple as signing in with a Microsoft account. Signing in with a Microsoft account on a Windows 10 device automatically sets up Windows Hello on the device; users don't have to do anything extra to enable it.
- 2. To sign in using that account, the user has to enter the existing credentials for it. The identity provider (IDP) that "owns" the account receives the credentials and authenticates the user. This IDP authentication may include the use of an existing second authentication factor, or proof. For example, a user who registers a new device by using an Azure AD account will have to provide an SMS-based proof that Azure AD sends.
- 3. When the user has provided the proof to the IDP, the user enables PIN authentication. The PIN will be associated with this particular credential. When the user sets the PIN, it becomes usable immediately

The PIN chosen is associated with the combination of the active account and that specific device. The PIN must comply with whatever length and complexity policy the account administrator has configured; this policy is enforced on the device side. Other registration scenarios that Windows Hello supports are:

- A user who upgrades from the Windows 8.1 operating system will sign in by using the existing enterprise password. That triggers a second authentication factor from the IDP side (if required); after receiving and returning a proof, such as a text message or voice code, the IDP authenticates the user to the upgraded Windows 10 device, and the user can set his or her PIN.
- A user who typically uses a smart card to sign in will be prompted to set up a PIN the first time he or she signs in to a Windows 10 device the user has not previously signed in to.
- A user who typically uses a virtual smart card to sign in will be prompted to set up a PIN the first time he or

she signs in to a Windows 10 device the user has not previously signed in to.

When the user has completed this process, Windows Hello generates a new public–private key pair on the device. The TPM generates and protects this private key; if the device doesn't have a TPM, the private key is encrypted and stored in software. This initial key is referred to as the protector key. It's associated only with a single gesture; in other words, if a user registers a PIN, a fingerprint, and a face on the same device, each of those gestures will have a unique protector key. Each unique gesture generates a unique protector key. The protector key securely wraps the authentication key. The container has only one authentication key, but there can be multiple copies of that key wrapped with different unique protector keys. Windows Hello also generates an administrative key that the user or administrator can use to reset credentials, when necessary. In addition to the protector key, TPM-enabled devices generate a block of data that contains attestations from the TPM.

At this point, the user has a PIN gesture defined on the device and an associated protector key for that PIN gesture. That means he or she is able to securely sign in to the device with the PIN and thus that he or she can establish a trusted session with the device to add support for a biometric gesture as an alternative for the PIN. When you add a biometric gesture, it follows the same basic sequence: the user authenticates to the system by using his or her PIN, and then registers the new biometric ("smile for the camera!"), after which Windows generates a unique key pair and stores it securely. Future sign-ins can then use either the PIN or the registered biometric gestures.

### What's a container?

You'll often hear the term *container* used in reference to mobile device management (MDM) solutions. Windows Hello uses the term, too, but in a slightly different way. Container in this context is shorthand for a logical grouping of key material or data. Windows 10 Hello uses a single container that holds user key material for personal accounts, including key material associated with the user's Microsoft account or with other consumer identity providers, and credentials associated with a workplace or school account.

The container holds enterprise credentials only on devices that have been registered with an organization; it contains key material for the enterprise IDP, such as on-premises Active Directory or Azure AD.

It's important to keep in mind that there are no physical containers on disk, in the registry, or elsewhere. Containers are logical units used to group related items. The keys, certificates, and credentials Windows Hello stores are protected without the creation of actual containers or folders.

The container actually contains a set of keys, some of which are used to protect other keys. The following image shows an example: the protector key is used to encrypt the authentication key, and the authentication key is used to encrypt the individual keys stored in the container.



Containers can contain several types of key material:

- An authentication key, which is always an asymmetric public–private key pair. This key pair is generated during registration. It must be unlocked each time it's accessed, by using either the user's PIN or a previously generated biometric gesture. The authentication key exists until the user resets the PIN, at which time a new key will be generated. When the new key is generated, all the key material that the old key previously protected must be decrypted and re-encrypted using the new key.
- Virtual smart card keys are generated when a virtual smart card is generated and stored securely in the container. They're available whenever the user's container is unlocked.
- The IDP key. These keys can be either symmetric or asymmetric, depending on which IDP you use. A single container may contain zero or more IDP keys, with some restrictions (for example, the enterprise container can contain zero or one IDP keys). IDP keys are stored in the container. For certificate-based Windows Hello for Work, when the container is unlocked, applications that require access to the IDP key or key pair can request access. IDP keys are used to sign or encrypt authentication requests or tokens sent from this device to the IDP. IDP keys are typically long-lived but could have a shorter lifetime than the authentication key. Microsoft accounts, Active Directory accounts, and Azure AD accounts all require the use of asymmetric key pairs. The device generates public and private keys, registers the public key with the IDP (which stores it for later verification), and securely stores the private key. For enterprises, the IDP keys can be generated in two ways:
  - The IDP key pair can be associated with an enterprise Certificate Authority (CA) through the Windows Network Device Enrollment Service (NDES), described more fully in Network Device Enrollment Service Guidance. In this case, Windows Hello requests a new certificate with the same key as the certificate from the existing PKI. This option lets organizations that have an existing PKI continue to use it where appropriate. Given that many applications, such as popular virtual private network systems, require the use of certificates, when you deploy Windows Hello in this mode, it allows a faster transition away from user passwords while still preserving certificate-based functionality. This option also allows the enterprise to store additional certificates in the protected container.
  - The IDP can generate the IDP key pair directly, which allows quick, lower-overhead deployment of Windows Hello in environments that don't have or need a PKI.

### How keys are protected

Any time key material is generated, it must be protected against attack. The most robust way to do this is through specialized hardware. There's a long history of using hardware security modules (HSMs) to generate, store, and process keys for security-critical applications. Smart cards are a special type of HSM, as are devices that are compliant with the Trusted Computing Group TPM standard. Wherever possible, the Windows Hello for Work implementation takes advantage of onboard TPM hardware to generate and protect keys. However, Windows Hello and Windows Hello for Work do not require an onboard TPM. Administrators can choose to allow key operations in software, in which case any user who has (or can escalate to) administrative rights on the device can use the IDP keys to sign requests. As an alternative, in some scenarios, devices that don't have a TPM can be remotely authenticated by using a device that does have a TPM, in which case all the sensitive operations are performed with the TPM and no key material is exposed.

Whenever possible, Microsoft recommends the use of TPM hardware. The TPM protects against a variety of known and potential attacks, including PIN brute-force attacks. The TPM provides an additional layer of protection after an account lockout, too. When the TPM has locked the key material, the user will have to reset the PIN (which means he or she will have to use MFA to reauthenticate to the IDP before the IDP allows him or her to re-register). Resetting the PIN means that all keys and certificates encrypted with the old key material will be removed.

### Authentication

When a user wants to access protected key material, the authentication process begins with the user entering a PIN or biometric gesture to unlock the device, a process sometimes called releasing the key. Think of it like using a physical key to unlock a door: before you can unlock the door, you need to remove the key from your pocket or

purse. The user's PIN unlocks the protector key for the container on the device. When that container is unlocked, applications (and thus the user) can use whatever IDP keys reside inside the container.

These keys are used to sign requests that are sent to the IDP, requesting access to specified resources. It's important to understand that although the keys are unlocked, applications cannot use them at will. Applications can use specific APIs to request operations that require key material for particular actions (for example, decrypt an email message or sign in to a website). Access through these APIs doesn't require explicit validation through a user gesture, and the key material isn't exposed to the requesting application. Rather, the application asks for authentication, encryption, or decryption, and the Windows Hello layer handles the actual work and returns the results. Where appropriate, an application can request a forced authentication even on an unlocked device. Windows prompts the user to reenter the PIN or perform an authentication gesture, which adds an extra level of protection for sensitive data or actions. For example, you can configure the Microsoft Store to require reauthentication any time a user purchases an application, even though the same account and PIN or gesture were already used to unlock the device.

For example, the authentication process for Azure Active Directory works like this:

- 1. The client sends an empty authentication request to the IDP. (This is merely for the handshake process.)
- 2. The IDP returns a challenge, known as a nonce.
- 3. The device signs the nonce with the appropriate private key.
- 4. The device returns the original nonce, the signed nonce, and the ID of the key used to sign the nonce.
- 5. The IDP fetches the public key that the key ID specified, uses it to verify the signature on the nonce, and verifies that the nonce the device returned matches the original.
- 6. If all the checks in step 5 succeed, the IDP returns two data items: a symmetric key, which is encrypted with the device's public key, and a security token, which is encrypted with the symmetric key.
- 7. The device uses its private key to decrypt the symmetric key, and then uses that symmetric key to decrypt the token.
- 8. The device makes a normal authentication request for the original resource, presenting the token from the IDP as its proof of authentication.

When the IDP validates the signature, it is verifying that the request came from the specified user and device. The private key specific to the device signs the nonce, which allows the IDP to determine the identity of the requesting user and device so that it can apply policies for content access based on user, device type, or both together. For example, an IDP could allow access to one set of resources only from mobile devices and a different set from desktop devices.

### The infrastructure

Windows Hello depends on having compatible IDPs available to it. As of this writing, that means you have four deployment possibilities:

- Use an existing Windows-based PKI centered around Active Directory Certificate Services. This option requires additional infrastructure, including a way to issue certificates to users. You can use NDES to register devices directly, or Microsoft Intune where it's available to manage mobile device participation in Windows Hello.
- The normal discovery mechanism that clients use to find domain controllers and global catalogs relies on Domain Name System (DNS) SRV records, but those records don't contain version data. Windows 10 computers will query DNS for SRV records to find all available Active Directory servers, and then query each server to identify those that can act as Windows Hello IDPs. The number of authentication requests your users generate, where your users are located, and the design of your network all drive the number of Windows Server 2016 domain controllers required.
- Azure AD can act as an IDP either by itself or alongside an on-premises AD DS forest. Organizations that use Azure AD can register devices directly without having to join them to a local domain by using the capabilities the Azure AD Device Registration service provides. In addition to the IDP, Windows Hello requires an MDM

system. This system can be the cloud-based Intune if you use Azure AD, or an on-premises System Center Configuration Manager deployment that meets the system requirements described in the Deployment requirements section of this document.

- Windows Hello for Business
- Manage Windows Hello for Business in your organization
- Why a PIN is better than a password
- Prepare people to use Windows Hello
- Windows Hello and password changes
- Windows Hello errors during PIN creation
- Event ID 300 Windows Hello successfully created
- Windows Hello biometrics in the enterprise

# Manage Windows Hello for Business in your organization

2/7/2018 • 8 min to read • Edit Online

#### **Applies to**

- Windows 10
- Windows 10 Mobile

You can create a Group Policy or mobile device management (MDM) policy that will implement Windows Hello on devices running Windows 10.

#### IMPORTANT

The Group Policy setting **Turn on PIN sign-in** does not apply to Windows Hello for Business. It still prevents or enables the creation of a convenience PIN for Windows 10, version 1507 and 1511.

Beginning in version 1607, Windows Hello as a convenience PIN is disabled by default on all domain-joined computers. To enable a convenience PIN for Windows 10, version 1607, enable the Group Policy setting **Turn on convenience PIN signin**.

Use PIN Complexity policy settings to manage PINs for Windows Hello for Business.

### Group Policy settings for Windows Hello for Business

The following table lists the Group Policy settings that you can configure for Windows Hello use in your workplace. These policy settings are available in both **User configuration** and **Computer Configuration** under **Policies > Administrative Templates > Windows Components > Windows Hello for Business**.

POLICY	OPTIONS
Use Windows Hello for Business	<ul> <li>Not configured: Users can provision Windows Hello for Business, which encrypts their domain password.</li> <li>Enabled: Device provisions Windows Hello for Business using keys or certificates for all users.</li> <li>Disabled: Device does not provision Windows Hello for Business for any user.</li> </ul>

Use a hardware security device		<ul> <li>Not configured: Windows Hello for Business will be provisioned using TPM if available, and will be provisioned using software if TPM is not available.</li> <li>Enabled: Windows Hello for Business will only be provisioned using TPM.</li> <li>Disabled: Windows Hello for Business will be provisioned using TPM if available, and will be provisioned using software if TPM is not available.</li> </ul>
Use biometrics		<ul> <li>Not configured: Biometrics can be used as a gesture in place of a PIN.</li> <li>Enabled: Biometrics can be used as a gesture in place of a PIN.</li> <li>Disabled: Only a PIN can be used as a gesture.</li> </ul>
PIN Complexity	Require digits	Not configured: Users must include a digit in their PIN. Enabled: Users must include a digit in their PIN. Disabled: Users cannot use digits in their PIN.
	Require lowercase letters	Not configured: Users cannot use lowercase letters in their PIN. Enabled: Users must include at least one lowercase letter in their PIN. Disabled: Users cannot use lowercase letters in their PIN.
	Maximum PIN length	<ul> <li>Not configured: PIN length must be less than or equal to 127.</li> <li>Enabled: PIN length must be less than or equal to the number you specify.</li> <li>Disabled: PIN length must be less than or equal to 127.</li> </ul>

	Minimum PIN length	Not configured: PIN length must be greater than or equal to 4. Enabled: PIN length must be greater than or equal to the number you specify. Disabled: PIN length must be greater than or equal to 4.
	Expiration	Not configured: PIN does not expire. Enabled: PIN can be set to expire after any number of days between 1 and 730, or PIN can be set to never expire by setting policy to 0. Disabled: PIN does not expire.
	History	Not configured: Previous PINs are not stored. Enabled: Specify the number of previous PINs that can be associated to a user account that can't be reused. Disabled: Previous PINs are not stored. Note Current PIN is included in PIN history.
	Require special characters	Not configured: Users cannot include a special character in their PIN. Enabled: Users must include at least one special character in their PIN. Disabled: Users cannot include a special character in their PIN.
	Require uppercase letters	Not configured: Users cannot include an uppercase letter in their PIN. Enabled: Users must include at least one uppercase letter in their PIN. Disabled: Users cannot include an uppercase letter in their PIN.
	Use Phone Sign-in	Not currently supported.

>Phone Sign-in

### MDM policy settings for Windows Hello for Business

The following table lists the MDM policy settings that you can configure for Windows Hello for Business use in your workplace. These MDM policy settings use the PassportForWork configuration service provider (CSP).

#### IMPORTANT

Starting in Windows 10, version 1607, all devices only have one PIN associated with Windows Hello for Business. This means that any PIN on a device will be subject to the policies specified in the PassportForWork CSP. The values specified take precedence over any complexity rules set via Exchange ActiveSync (EAS) or the DeviceLock CSP.

POLICY	SCOPE	DEFAULT	OPTIONS
UsePassportForWork	Device	True	True: Windows Hello for Business will be provisioned for all users on the device. False: Users will not be able to provision Windows Hello for Business. Note If Windows Hello for Business is enabled, and then the policy is changed to False, users who previously set up Windows Hello for Business can continue to use it, but will not be able to set up Windows Hello for Business on other devices.
RequireSecurityDevic e	Device	False	True: Windows Hello for Business will only be provisioned using TPM. False: Windows Hello for Business will be provisioned using TPM if available, and will be provisioned using software if TPM is not available.

Biometrics	UseBiometrics	Device	False	True: Biometrics can be used as a gesture in place of a PIN for domain sign-in. False: Only a PIN can be used as a gesture for domain sign-in.
	FacialFeaturesUse r EnhancedAntiSpo ofing	Device	Not configured	Not configured: users can choose whether to turn on enhanced anti-spoofing. True: Enhanced anti-spoofing is required on devices which support it. False: Users cannot turn on enhanced anti- spoofing.
PINComplexity	Digits	Device or user	2	<ol> <li>1: Numbers are not allowed.</li> <li>2: At least one number is required.</li> </ol>
	Lowercase letters	Device or user	1	<ol> <li>1: Lowercase letters are not allowed.</li> <li>2: At least one lowercase letter is required.</li> </ol>
	Maximum PIN length	Device or user	127	Maximum length that can be set is 127. Maximum length cannot be less than minimum setting.
	Minimum PIN length	Device or user	4	Minimum length that can be set is 4. Minimum length cannot be greater than maximum setting.

Expiration	Device or user	0	Integer value specifies the period of time (in days) that a PIN can be used before the system requires the user to change it. The largest number you can configure for this policy setting is 730. The lowest number you can configure for this policy setting is 0. If this policy is set to 0, then the user's PIN will never expire.
History	Device or user	0	Integer value that specifies the number of past PINs that can be associated to a user account that can't be reused. The largest number you can configure for this policy setting is 50. The lowest number you can configure for this policy setting is 0. If this policy is set to 0, then storage of previous PINs is not required.
Special characters	Device or user	1	<ol> <li>Special characters are not allowed.</li> <li>At least one special character is required.</li> </ol>
Uppercase letters	Device or user	1	1: Uppercase letters are not allowed 2: At least one uppercase letter is required

#### NOTE

If policy is not configured to explicitly require letters or special characters, users will be restricted to creating a numeric PIN.

### How to use Windows Hello for Business with Azure Active Directory

There are three scenarios for using Windows Hello for Business in Azure AD-only organizations:

- Organizations that use the version of Azure AD included with Office 365. For these organizations, no additional work is necessary. When Windows 10 was released to general availability, Microsoft changed the behavior of the Office 365 Azure AD stack. When a user selects the option to join a work or school network, the device is automatically joined to the Office 365 tenant's directory partition, a certificate is issued for the device, and it becomes eligible for Office 365 MDM if the tenant has subscribed to that feature. In addition, the user will be prompted to log on and, if MFA is enabled, to enter an MFA proof that Azure AD sends to his or her phone.
- Organizations that use the free tier of Azure AD. For these organizations, Microsoft has not enabled automatic domain join to Azure AD. Organizations that have signed up for the free tier have the option to enable or disable this feature, so automatic domain join won't be enabled unless and until the organization's administrators decide to enable it. When that feature is enabled, devices that join the Azure AD domain by using the Connect to work or school dialog box will be automatically registered with Windows Hello for Business support, but previously joined devices will not be registered.
- Organizations that have subscribed to Azure AD Premium have access to the full set of Azure AD MDM features. These features include controls to manage Windows Hello for Business. You can set policies to disable or force the use of Windows Hello for Business, require the use of a TPM, and control the length and strength of PINs set on the device.

If you want to use Windows Hello for Business with certificates, you'll need a device registration system. That means that you set up Configuration Manager, Microsoft Intune, or a compatible non-Microsoft MDM system and enable it to enroll devices. This is a prerequisite step to use Windows Hello for Business with certificates, no matter the IDP, because the enrollment system is responsible for provisioning the devices with the necessary certificates.

- Windows Hello for Business
- How Windows Hello for Business works
- Why a PIN is better than a password
- Prepare people to use Windows Hello
- Windows Hello and password changes
- Windows Hello errors during PIN creation
- Event ID 300 Windows Hello successfully created
- Windows Hello biometrics in the enterprise

# Why a PIN is better than a password

2/7/2018 • 4 min to read • Edit Online

#### **Applies to**

- Windows 10
- Windows 10 Mobile

Windows Hello in Windows 10 enables users to sign in to their device using a PIN. How is a PIN different from (and better than) a password? On the surface, a PIN looks much like a password. A PIN can be a set of numbers, but enterprise policy might allow complex PINs that include special characters and letters, both upper-case and lower-case. Something like **t758A!** could be an account password or a complex Hello PIN. It isn't the structure of a PIN (length, complexity) that makes it better than a password, it's how it works.

### PIN is tied to the device

One important difference between a password and a Hello PIN is that the PIN is tied to the specific device on which it was set up. That PIN is useless to anyone without that specific hardware. Someone who steals your password can sign in to your account from anywhere, but if they steal your PIN, they'd have to steal your physical device too!

Even you can't use that PIN anywhere except on that specific device. If you want to sign in on multiple devices, you have to set up Hello on each device.

### PIN is local to the device

A password is transmitted to the server -- it can be intercepted in transmission or stolen from a server. A PIN is local to the device -- it isn't transmitted anywhere and it isn't stored on the server. When the PIN is created, it establishes a trusted relationship with the identity provider and creates an asymmetric key pair that is used for authentication. When you enter your PIN, it unlocks the authentication key and uses the key to sign the request that is sent to the authenticating server.

#### NOTE

For details on how Hello uses asymetric key pairs for authentication, see Windows Hello for Business.

### PIN is backed by hardware

The Hello PIN is backed by a Trusted Platform Module (TPM) chip, which is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper resistant, and malicious software is unable to tamper with the security functions of the TPM. All Windows 10 Mobile phones and many modern laptops have TPM.

User key material is generated and available within the Trusted Platform Module (TPM) of the user device, which protects it from attackers who want to capture the key material and reuse it. Because Hello uses asymmetrical key pairs, users credentials canâ€<sup>™</sup>t be stolen in cases where the identity provider or websites the user accesses have been compromised.

The TPM protects against a variety of known and potential attacks, including PIN brute-force attacks. After too many incorrect guesses, the device is locked.

### PIN can be complex

The Windows Hello for Business PIN is subject to the same set of IT management policies as a password, such as complexity, length, expiration, and history. Although we generally think of a PIN as a simple four-digit code, administrators can set policies for managed devices to require a PIN complexity similar to a password. You can require or block: special characters, uppercase characters, lowercase characters, and digits.

### What if someone steals the laptop or phone?

To compromise a Windows Hello credential that TPM protects, an attacker must have access to the physical device, and then must find a way to spoof the userâ€<sup>™</sup>s biometrics or guess his or her PINâ€" and all of this must be done before TPM anti-hammering protection locks the device. You can provide additional protection for laptops that don't have TPM by enabling BitLocker and setting a policy to limit failed sign-ins.

#### **Configure BitLocker without TPM**

1. Use the Local Group Policy Editor (gpedit.msc) to enable the following policy:

#### Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Require additional authentication at startup

- 2. In the policy option, select Allow BitLocker without a compatible TPM, and then click OK.
- 3. Go to Control Panel > **System and Security > BitLocker Drive Encryption** and select the operating system drive to protect. **Set account lockout threshold**
- 4. Use the Local Group Policy Editor (gpedit.msc) to enable the following policy:

#### Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policy > Account lockout threshold

5. Set the number of invalid logon attempts to allow, and then click OK.

### Why do you need a PIN to use biometrics?

Windows Hello enables biometric sign-in for Windows 10: fingerprint, iris, or facial recognition. When you set up Windows Hello, you're asked to create a PIN first. This PIN enables you to sign in using the PIN when you can't use your preferred biometric because of an injury or because the sensor is unavailable or not working properly.

If you only had a biometric sign-in configured and, for any reason, were unable to use that method to sign in, you would have to sign in using your account and password, which doesn't provide you the same level of protection as Hello.

- Windows Hello for Business
- How Windows Hello for Business works
- Manage Windows Hello for Business in your organization
- Prepare people to use Windows Hello
- Windows Hello and password changes
- Windows Hello errors during PIN creation
- Event ID 300 Windows Hello successfully created
- Windows Hello biometrics in the enterprise

# Prepare people to use Windows Hello

2/7/2018 • 2 min to read • Edit Online

#### **Applies to**

- Windows 10
- Windows 10 Mobile

When you set a policy to require Windows Hello for Business in the workplace, you will want to prepare people in your organization by explaining how to use Hello.

After enrollment in Hello, users should use their gesture (such as a PIN or fingerprint) for access to corporate resources. Their gesture is only valid on the enrolled device.

Although the organization may require users to change their Active Directory or Azure Active Directory (AD) account password at regular intervals, changes to their passwords have no effect on Hello.

People who are currently using virtual or physical smart cards for authentication can use their virtual smart card to verify their identity when they set up Hello.

### On devices owned by the organization

When someone sets up a new device, they are prompted to choose who owns the device. For corporate devices, they select **This device belongs to my organization**.



Next, they select a way to connect. Tell the people in your enterprise which option they should pick here.



They sign in, and are then asked to verify their identity. People have options to choose from, such as a text message, phone call, or authentication app. After verification, they create their PIN. The **Create a PIN** screen displays any complexity requirements that you have set, such as minimum length.

After Hello is set up, people use their PIN to unlock the device, and that will automatically log them on.

### On personal devices

People who want to access work resources on their personal devices can add a work or school account in **Settings** > **Accounts** > **Work or school**, and then sign in with work credentials. The person selects the method for receiving the verification code, such as text message or email. The verification code is sent and the person then enters the verification code. After verification, the person enters and confirms new PIN. The person can access any token-based resource using this device without being asked for credentials.

People can go to **Settings** > **Accounts** > **Work or school**, select the work account, and then select **Unjoin** to remove the account from their device.

### Using Windows Hello and biometrics

If your policy allows it, people can use biometrics (fingerprint, iris, and facial recognition) with Windows Hello for Business, if the hardware supports it.



- Windows Hello for Business
- How Windows Hello for Business works
- Manage Windows Hello for Business in your organization
- Why a PIN is better than a password
- Windows Hello and password changes
- Windows Hello errors during PIN creation
- Event ID 300 Windows Hello successfully created
- Windows Hello biometrics in the enterprise

# Windows Hello and password changes

2/7/2018 • 1 min to read • Edit Online

#### **Applies to**

- Windows 10
- Windows 10 Mobile

When you set up Windows Hello, the PIN or biometric gesture that you use is specific to that device. You can set up Hello for the same account on multiple devices. If the PIN or biometric is configured as part of Windows Hello for Business, changing the account password will not impact sign-in or unlock with these gestures since it uses a key or certificate. However, if Windows Hello for Business is not deployed and the password for that account changes, you must provide the new password on each device to continue to use Hello.

### Example

Let's suppose that you have set up a PIN for your Microsoft account on **Device A**. You use your PIN to sign in on **Device A** and then change the password for your Microsoft account. Because you were using **Device A** when you changed your password, the PIN on **Device A** will continue to work with no other action on your part.

Suppose instead that you sign in on **Device B** and change your password for your Microsoft account. The next time that you try to sign in on **Device A** using your PIN, sign-in will fail because the account credentials that Hello on **Device A** knows will be outdated.

#### NOTE

This example also applies to an Active Directory account when Windows Hello for Business is not implemented.

# How to update Hello after you change your password on another device

- 1. When you try to sign in using your PIN or biometric, you will see the following message: **Your password was** changed on a different device. You must sign in to this device once with your new password, and then you can sign in with your PIN.
- 2. Click **OK.**
- 3. Click Sign-in options.
- 4. Click the **Password** button.
- 5. Sign in with new password.
- 6. The next time that you sign in, you can select **Sign-in options** and then select **PIN** to resume using your PIN.

- Windows Hello for Business
- How Windows Hello for Business works
- Manage Windows Hello for Business in your organization
- Why a PIN is better than a password
- Prepare people to use Windows Hello
- Windows Hello errors during PIN creation

- Event ID 300 Windows Hello successfully created
- Windows Hello biometrics in the enterprise

# Windows Hello errors during PIN creation

2/7/2018 • 4 min to read • Edit Online

#### **Applies to**

- Windows 10
- Windows 10 Mobile

When you set up Windows Hello in Windows 10, you may get an error during the **Create a PIN** step. This topic lists some of the error codes with recommendations for mitigating the problem. If you get an error code that is not listed here, contact Microsoft Support.

### Where is the error code?

The following image shows an example of an error during Create a PIN.



### Error mitigations

When a user encounters an error when creating the work PIN, advise the user to try the following steps. Many errors can be mitigated by one of these steps.

- 1. Try to create the PIN again. Some errors are transient and resolve themselves.
- 2. Sign out, sign in, and try to create the PIN again.
- 3. Reboot the device and then try to create the PIN again.
- 4. Unjoin the device from Azure Active Directory (Azure AD), rejoin, and then try to create the PIN again. To unjoin a desktop PC, go to Settings > System > About and select Disconnect from organization. To unjoin a device running Windows 10 Mobile, you must reset the device.
- 5. On mobile devices, if you are unable to setup a PIN after multiple attempts, reset your device and start over. For help on how to reset your phone go to Reset my phone. If the error occurs again, check the error code against the following table to see if there is another mitigation for that error. When no mitigation is listed in the table, contact Microsoft Support for assistance.

НЕХ	CAUSE	MITIGATION
0x801C044D	Authorization token does not contain device ID	Unjoin the device from Azure AD and rejoin
0x80090036	User cancelled an interactive dialog	User will be asked to try again
0x80090011	The container or key was not found	Unjoin the device from Azure AD and rejoin
0x8009000F	The container or key already exists	Unjoin the device from Azure AD and rejoin
0x8009002A	NTE_NO_MEMORY	Close programs which are taking up memory and try again.
0x80090005	NTE_BAD_DATA	Unjoin the device from Azure AD and rejoin
0x80090029	TPM is not set up.	Sign on with an administrator account. Click <b>Start</b> , type "tpm.msc", and select <b>tpm.msc Microsoft Common</b> <b>Console Document</b> . In the <b>Actions</b> pane, select <b>Prepare the TPM</b> .
0x80090031	NTE_AUTHENTICATION_IGNORED	Reboot the device. If the error occurs again after rebooting, reset the TPM or run Clear-TPM
0x80090035	Policy requires TPM and the device does not have TPM.	Change the Windows Hello for Business policy to not require a TPM.
0x801C0003	User is not authorized to enroll	Check if the user has permission to perform the operation.
0x801C000E	Registration quota reached	Unjoin some other device that is currently joined using the same account or increase the maximum number of devices per user.
0x801C000F	Operation successful but the device requires a reboot	Reboot the device.
0x801C0010	The AIK certificate is not valid or trusted	Sign out and then sign in again.
0x801C0011	The attestation statement of the transport key is invalid	Sign out and then sign in again.
0x801C0012	Discovery request is not in a valid format	Sign out and then sign in again.
0x801C0015	The device is required to be joined to an Active Directory domain	Join the device to an Active Directory domain.

HEX	CAUSE	MITIGATION
0x801C0016	The federation provider configuration is empty	Go to http://clientconfig.microsoftonline- p.net/FPURL.xml and verify that the file is not empty.
0x801C0017	The federation provider domain is empty	Go to http://clientconfig.microsoftonline- p.net/FPURL.xml and verify that the FPDOMAINNAME element is not empty.
0x801C0018	The federation provider client configuration URL is empty	Go to http://clientconfig.microsoftonline- p.net/FPURL.xml and verify that the CLIENTCONFIG element contains a valid URL.
0x801C03E9	Server response message is invalid	Sign out and then sign in again.
0x801C03EA	Server failed to authorize user or device.	Check if the token is valid and user has permission to register Windows Hello for Business keys.
0x801C03EB	Server response http status is not valid	Sign out and then sign in again.
0x801C03EC	Unhandled exception from server.	sign out and then sign in again.
0x801C03ED	Multi-factor authentication is required for a 'ProvisionKey' operation, but was not performed -or- Token was not found in the Authorization header -or- Failed to read one or more objects -or- The request sent to the server was invalid.	Sign out and then sign in again. If that doesn't resolve the issue, unjoin the device from Azure Active Directory (Azure AD) and rejoin.
0x801C03EE	Attestation failed	Sign out and then sign in again.
0x801C03EF	The AIK certificate is no longer valid	Sign out and then sign in again.
0x801C044D	Unable to obtain user token	Sign out and then sign in again. Check network and credentials.
0x801C044E	Failed to receive user creds input	Sign out and then sign in again.

## Errors with unknown mitigation

For errors listed in this table, contact Microsoft Support for assistance.

HEX	CAUSE
0x80072f0c	Unknown
0x80070057	Invalid parameter or argument is passed
0x80090027	Caller provided wrong parameter. If third-party code receives this error they must change their code.
0x8009002D	NTE_INTERNAL_ERROR
0x80090020	NTE_FAIL
0x801C0001	ADRS server response is not in valid format
0x801C0002	Server failed to authenticate the user
0x801C0006	Unhandled exception from server
0x801C000C	Discovery failed
0x801C001B	The device certificate is not found
0x801C000B	Redirection is needed and redirected location is not a well known server
0x801C0019	The federation provider client configuration is empty
0x801C001A	The DRS endpoint in the federation provider client configuration is empty
0x801C0013	Tenant ID is not found in the token
0x801C0014	User SID is not found in the token
0x801C03F1	There is no UPN in the token
0x801C03F0	There is no key registered for the user
0x801C03F1	There is no UPN in the token
0x801C044C	There is no core window for the current thread

- Windows Hello for Business
- How Windows Hello for Business works
- Manage Windows Hello for Business in your organization
- Why a PIN is better than a password
- Prepare people to use Windows Hello
- Windows Hello and password changes
- Event ID 300 Windows Hello successfully created

• Windows Hello biometrics in the enterprise

# Event ID 300 - Windows Hello successfully created

2/7/2018 • 1 min to read • Edit Online

#### **Applies to**

- Windows 10
- Windows 10 Mobile

This event is created when Windows Hello for Business is successfully created and registered with Azure Active Directory (Azure AD). Applications or services can trigger actions on this event. For example, a certificate provisioning service can listen to this event and trigger a certificate request.

### Event details

PRODUCT:	WINDOWS 10 OPERATING SYSTEM
ID:	300
Source:	Microsoft Azure Device Registration Service
Version:	10
Message:	The NGC key was successfully registered. Key ID: {4476694e- 8e3b-4ef8-8487-be21f95e6f07}. UPN:test@contoso.com. Attestation: ATT_SOFT. Client request ID: . Server request ID: db2da6bd-3d70-4b9b-b26b-444f669902da. Server response: {"kid":"4476694e-8e3b-4ef8-8487- be21f95e6f07","upn":"test@contoso.com"}

### Resolve

This is a normal condition. No further action is required.

- Windows Hello for Business
- How Windows Hello for Business works
- Manage Windows Hello for Business in your organization
- Why a PIN is better than a password
- Prepare people to use Windows Hello
- Windows Hello and password changes
- Windows Hello errors during PIN creation
- Windows Hello biometrics in the enterprise

# Windows Hello biometrics in the enterprise

2/7/2018 • 4 min to read • Edit Online

#### **Applies to:**

• Windows 10

Windows Hello is the biometric authentication feature that helps strengthen authentication and helps to guard against potential spoofing through fingerprint matching and facial recognition.

#### NOTE

When Windows 10 first shipped, it included Microsoft Passport and Windows Hello, which worked together to provide multi-factor authentication. To simplify deployment and improve supportability, Microsoft has combined these technologies into a single solution under the Windows Hello name. Customers who have already deployed these technologies will not experience any change in functionality. Customers who have yet to evaluate Windows Hello will find it easier to deploy due to simplified policies, documentation, and semantics.

Because we realize your employees are going to want to use this new technology in your enterprise, we've been actively working with the device manufacturers to create strict design and performance recommendations that help to ensure that you can more confidently introduce Windows Hello biometrics into your organization.

### How does Windows Hello work?

Windows Hello lets your employees use fingerprint or facial recognition as an alternative method to unlocking a device. With Windows Hello, authentication happens when the employee provides his or her unique biometric identifier while accessing the device-specific Windows Hello credentials.

The Windows Hello authenticator works to authenticate and allow employees onto your enterprise network. Authentication doesn't roam among devices, isn't shared with a server, and can't easily be extracted from a device. If multiple employees share a device, each employee will use his or her own biometric data on the device.

### Why should I let my employees use Windows Hello?

Windows Hello provides many benefits, including:

- It helps to strengthen your protections against credential theft. Because an attacker must have both the device and the biometric info or PIN, it's much more difficult to gain access without the employee's knowledge.
- Employees get a simple authentication method (backed up with a PIN) that's always with them, so there's nothing to lose. No more forgetting passwords!
- Support for Windows Hello is built into the operating system so you can add additional biometric devices and polices as part of a coordinated rollout or to individual employees or groups using Group Policy or Mobile Device Management (MDM) configurations service provider (CSP) policies.
   For more info about the available Group Policies and MDM CSPs, see the Implement Windows Hello for Business in your organization topic.

### Where is Microsoft Hello data stored?

The biometric data used to support Windows Hello is stored on the local device only. It doesn't roam and is never

sent to external devices or servers. This separation helps to stop potential attackers by providing no single collection point that an attacker could potentially compromise to steal biometric data. Additionally, even if an attacker was actually able to get the biometric data, it still can't be easily converted to a form that could be recognized by the biometric sensor.

### Has Microsoft set any device requirements for Windows Hello?

We've been working with the device manufacturers to help ensure a high-level of performance and protection is met by each sensor and device, based on these requirements:

- False Accept Rate (FAR). Represents the instance a biometric identification solution verifies an unauthorized person. This is normally represented as a ratio of number of instances in a given population size, for example 1 in 100 000. This can also be represented as a percentage of occurrence, for example, 0.001%. This measurement is heavily considered the most important with regards to the security of the biometric algorithm.
- **False Reject Rate (FRR).** Represents the instances a biometric identification solution fails to verify an authorized person correctly. Usually represented as a percentage, the sum of the True Accept Rate and False Reject Rate is 1. Can be with or without anti-spoofing or liveness detection.

#### **Fingerprint sensor requirements**

To allow fingerprint matching, you must have devices with fingerprint sensors and software. Fingerprint sensors, or sensors that use an employee's unique fingerprint as an alternative log on option, can be touch sensors (large area or small area) or swipe sensors. Each type of sensor has its own set of detailed requirements that must be implemented by the manufacturer, but all of the sensors must include anti-spoofing measures (required).

#### Acceptable performance range for small to large size touch sensors

- False Accept Rate (FAR): <0.001 0.002%
- Effective, real world FRR with Anti-spoofing or liveness detection: <10%

#### Acceptable performance range for swipe sensors

- False Accept Rate (FAR): <0.002%
- Effective, real world FRR with Anti-spoofing or liveness detection: <10%

#### Facial recognition sensors

To allow facial recognition, you must have devices with integrated special infrared (IR) sensors and software. Facial recognition sensors use special cameras that see in IR light, letting them tell the difference between a photo and a living person while scanning an employee's facial features. These sensors, like the fingerprint sensors, must also include anti-spoofing measures (required) and a way to configure them (optional).

- False Accept Rate (FAR): <0.001
- False Reject Rate (FRR) without Anti-spoofing or liveness detection: <5%
- Effective, real world FRR with Anti-spoofing or liveness detection: <10%

- Windows Hello for Business
- How Windows Hello for Business works
- Manage Windows Hello for Business in your organization
- Why a PIN is better than a password
- Prepare people to use Windows Hello
- Windows Hello and password changes
- Windows Hello errors during PIN creation
- Event ID 300 Windows Hello successfully created
- PassportforWork CSP

## Planning a Windows Hello for Business Deployment

4/9/2018 • 21 min to read • Edit Online

## **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1511 or higher.

Congratulations! You are taking the first step forward in helping move your organizations away from password to a two-factor, convenience authentication for Windows â€" Windows Hello for Business. This planning guide helps you understand the different topologies, architectures, and components that encompass a Windows Hello for Business infrastructure.

This guide explains the role of each component within Windows Hello for Business and how certain deployment decisions affect other aspects of the infrastructure. Armed with your planning worksheet, youâ€<sup>™</sup>II use that information to select the correct deployment guide for your needs.

## Using this guide

There are many options from which you can choose when deploying Windows Hello for Business. Providing multiple options ensures nearly every organization can deploy Windows Hello for Business. Providing many options makes the deployment appear complex, however, most organization will realize they've already implemented most of the infrastructure on which the Windows Hello for Business deployment depends. It is important to understand that Windows Hello for Business is a distributed system and does take proper planning across multiple teams within an organization.

This guide removes the appearance of complexity by helping you make decisions on each aspect of your Windows Hello for Business deployment and the options youâ€<sup>™</sup>II need to consider. Using this guide also identifies the information needed to help you make decisions about the deployment that best suits your environment. Download the Windows Hello for Business planning worksheet from the Microsoft Download Center to help track your progress and make your planning easier.

## How to Proceed

Read this document and record your decisions on the worksheet. When finished, your worksheet has all the necessary information for your Windows Hello for Business deployment.

There are six major categories you need to consider for a Windows Hello for Business deployment. Those categories are:

- Deployment Options
- Client
- Management
- Active Directory
- Public Key Infrastructure
- Cloud

## **Baseline Prerequisites**

Windows Hello for Business has a few baseline prerequisites with which you can begin. These baseline prerequisites are provided in the worksheet.

## **Deployment Options**

The goal of Windows Hello for Business is to enable deployments for all organizations of any size or scenario. To provide this type of granular deployment, Windows Hello for Business offers a diverse choice of deployment options.

#### Deployment models

There are three deployment models from which you can choose: cloud only, hybrid, and on-premises.

#### Cloud only

The cloud only deployment model is for organizations who only have cloud identities and do not access onpremises resources. These organizations typically join their devices to the cloud and exclusively use resources in the cloud such as SharePoint, OneDrive, and others. Also, because these users do not use on-premises resources, they do not need certificates for things like VPN because everything they need is hosted in Azure.

#### Hybrid

The hybrid deployment model is for organizations that:

- Are federated with Azure Active Directory
- Have identities synchronized to Azure Active Directory using Azure Active Directory Connect
- Use applications hosted in Azure Active Directory, and want a single sign-in user experience for both onpremises and Azure Active Directory resources

#### On-premises

The on-premises deployment model is for organizations that do not have cloud identities or use applications hosted in Azure Active Directory.

Itâ€<sup>™</sup>s fundamentally important to understand which deployment model to use for a successful deployment. Some of aspects of the deployment may already be decided for you based on your current infrastructure.

### Trust types

A deployment's trust type defines how each Windows Hello for Business client authenticates to the on-premises Active Directory. There are two trust types: key trust and certificate trust.

The key trust type does not require issuing authentication certificates to end users. Users authenticate using a hardware-bound key created during an in-box provisioning experience, which requires an adequate distribution of Windows Server 2016 domain controllers relative to your existing authentication and the number of users included in your Windows Hello for Business deployment. Read the Planning an adequate number of Windows Server 2016 Domain Controllers for Windows Hello for Business deployments to learn more.

The certificate trust type issues authentication certificates to end users. Users authenticate using a certificate requested using a hardware-bound key created during the in-box provisioning experience. Unlike key trust, certificate trust does not require Windows Server 2016 domain controllers. Users can authentication using their certificate to any Windows Server 2008 R2 or later domain controller.

#### **Device registration**

All devices included in the Windows Hello for Business deployment must go through device registration. Device registration enables devices to authenticate to identity providers. For cloud only and hybrid deployment, the identity provider is Azure Active Directory. For on-premises deployments, the identity provider is the on-premises server running the Windows Server 2016 Active Directory Federation Services (AD FS) role.

### Key registration

The in-box Windows Hello for Business provisioning experience creates a hardware bound asymmetric key pair as their userâ€<sup>™</sup>s credentials. The private key is protected by the deviceâ€<sup>™</sup>s security modules; however, the credential is a user key (not a device key). The provisioning experience registers the userâ€<sup>™</sup>s public key with the identity provider. For cloud only and hybrid deployments, the identity provider is Azure Active Directory. For on-premises deployments, the identity provider is the on-premises server running Windows Server 2016 Active Directory Federation Services (AD FS) role.

#### Multifactor authentication

The goal of Windows Hello for Business is to move organizations away from passwords by providing them a strong credential that provides easy two-factor authentication. The inbox provisioning experience accepts the userâ€<sup>™</sup>s weak credentials (username and password) as the first factor authentication; however, the user must provide a second factor of authentication before Windows provisions a strong credential.

Cloud only and hybrid deployments provide many choices for multifactor authentication. On-premises deployments must use a multifactor authentication that provides an AD FS multifactor adapter to be used in conjunction with the on-premises Windows Server 2016 AD FS server role. Organizations can use the on-premises Azure Multifactor Authentication server, or choose from several third parties (Read Microsoft and third-party additional authentication methods for more information).

### NOTE

Azure Multi-Factor Authentication is available through:

- Microsoft Enterprise Agreement
- Open Volume License Program
- Cloud Solution Providers program
- Bundled with
  - Azure Active Directory Premium
  - Enterprise Mobility Suite
  - Enterprise Cloud Suite
- A per-user and per-authentication consumption-based model that is billed monthly against Azure monetary commitment (Read Multi-Factor Authentication Pricing for more information)

#### Directory synchronization

Hybrid and on-premises deployments use directory synchronization, however, each for a different purpose. Hybrid deployments use Azure Active Directory Connect to synchronize Active Directory identities or credentials between itself and Azure Active Directory. This helps enable single sign-on to Azure Active Directory and its federated components.

#### Management

Windows Hello for Business provides organizations with a rich set of granular policy settings with which they can use to manage their devices and users. There are three ways in which you can manage Windows Hello for Business: Group Policy, Modern Management, and Mixed.

#### **Group Policy**

Group Policy is the easiest and most popular way to manage Windows Hello for Business on domain joined devices. Simply create a Group Policy object with the settings you desire. Link the Group Policy object high in your Active Directory and use security group filtering to target specific sets of computers or users. Or, link the GPO directly to the organizational units.

#### Modern management

Modern management is an emerging device management paradigm that leverages the cloud for managing domain joined and non-domain joined devices. Organizations can unify their device management into one platform and apply policy settings using a single platform

### Client

Windows Hello for Business is an exclusive Windows 10 feature. As part of the Windows as a Service strategy, Microsoft has improved the deployment, management, and user experience with each new release of Windows 10 and introduced support for new scenarios.

Most deployment scenarios require a minimum of Windows 10, version 1511, also known as the November Update. The client requirement may change based on different components in your existing infrastructure, or other infrastructure choices made later in planning your deployment. Those components and choices may require a minimum client running Windows 10, version 1703, also known as the Creators Update.

## **Active Directory**

Hybrid and on-premises deployments include Active Directory as part of their infrastructure. Most of the Active Directory requirements, such as schema, and domain and forest functional levels are predetermined. However, your trust type choice for authentication determines the version of domain controller needed for the deployment.

## Public Key Infrastructure

The Windows Hello for Business deployment depends on an enterprise public key infrastructure as a trust anchor for authentication. Domain controllers for hybrid and on-prem deployments need a certificate in order for Windows 10 devices to trust the domain controller as legitimate. Deployments using the certificate trust type need an enterprise public key infrastructure and a certificate registration authority to issue authentication certificates to users. Hybrid deployments may need to issue VPN certificates to users to enable connectivity on-premises resources.

## Cloud

Some deployment combinations require an Azure account and some require Azure Active Directory for user identities. These cloud requirements may only need an Azure account while other features need an Azure Active Directory Premium subscription. The planning process identifies and differentiates the components that are needed from the those that are optional.

## Planning a Deployment

Planning your Windows Hello for Business deployment begins with choosing a deployment type. Like all distributed systems, Windows Hello for Business depends on multiple components within your organizationâ€<sup>™</sup>s infrastructure.

Use the remainder of this guide to help with planning your deployment. As you make decisions, write the results of those decisions in your planning worksheet. When finished, youâ€<sup>™</sup>II have all the information needed to complete the planning process and the appropriate deployment guide that best helps you with your deployment.

## **Deployment Model**

Choose the deployment model based on the resources your users access. Use the following guidance to make your decision.

If your organization does not have on-premises resources, write **Cloud Only** in box **1a** on your planning worksheet.

If your organization is federated with Azure or uses any online service, such as Office365 or OneDrive, or your users access cloud and on-premises resources, write **Hybrid** in box **1a** on your planning worksheet.

If your organization does not have cloud resources, write **On-Premises** in box **1a** on your planning worksheet.

### NOTE

If you're unsure if your organization is federated, run the following Active Directory Windows PowerShell command from an elevated Windows PowerShell prompt and evaluate the results.

Get-AdObject "CN=62a0ff2e-97b9-4513-943f-0d221bd30080,CN=Device Registration Configuration,CN=Services,CN=Configuration,DC=corp,DC=[forest\_root\_CN\_name],DC=com" -Properties keywords

- If the command returns an error stating it could not find the object, then you have yet to configured AAD Connect or onpremises Device Registration Services using AD FS. Ensure the name is accurate and validate the object does not exist with another Active Directory Management tool such as **ADSIEdit.msc**. If the object truly does not exist, then you environment does not bind you to a specific deployment or require changes to accommodate the desired deployment type.
- If the command returns a value, compare that value with the values below. The value indicates the deployment model you should implement
  - If the value begins with **azureADName:** â€" write **Hybrid** in box **1a**on your planning worksheet.
    - If the value begins with **enterpriseDrsName:** â€" write **On-Premises** in box **1a** on your planning worksheet.

## Trust type

Choose a trust type that is best suited for your organizations. Remember, the trust type determines two things. Whether you issue authentication certificates to your users and if your deployment needs Windows Server 2016 domain controllers.

One trust model is not more secure than the other. The major difference is based on the organization comfort with deploying Windows Server 2016 domain controllers and not enrolling users with end entity certificates (key-trust) against using existing domain controllers (Windows Server 2008R2 or later) and needing to enroll certificates for all their users (certificate trust).

Because the certificate trust types issues certificates, there is more configuration and infrastructure needed to accomodate user certificate enrollment, which could also be a factor to consider in your decision. Additional infrastructure needed for certificate-trust deployements includes a certificate registration authority. Hybrid Azure AD joined devices managed by Group Policy need the Windows Server 2016 AD FS role to issue certificates. Hybrid Azure AD joined devices and Azure AD joined devices managed by Intune or a compatible MDM need the Windows Server NDES server role to issue certificates.

If your organization wants to use the key trust type, write **key trust** in box **1b** on your planning worksheet. Write **Windows Server 2016** in box **4d**. Write **N/A** in box **5b**.

If your organization wants to use the certificate trust type, write **certificate trust** in box **1b** on your planning worksheet. Write **Windows Server 2008 R2 or later** in box **4d**. In box **5c**, write **smart card logon** under the **Template Name** column and write **users** under the **Issued To** column on your planning worksheet.

### **Device Registration**

A successful Windows Hello for Business requires all devices to register with the identity provider. The identity provider depends on the deployment model.

If box **1a** on your planning worksheet reads **cloud only** or **hybrid**, write **Azure** in box **1c** on your planning worksheet.

If box 1a on your planning worksheet reads on-premises, write AD FS in box 1c on your planning worksheet.

### **Key Registration**

All users provisioning Windows Hello for Business have their public key registered with the identity provider. The identity provider depends on the deployment model.

If box 1a on your planning worksheet reads cloud only or hybrid, write Azure in box 1d on your planning

worksheet.

If box 1a on your planning worksheet reads on-premises, write AD FS in box 1d on your planning worksheet.

## **Directory Synchronization**

Windows Hello for Business is strong user authentication, which usually means there is an identity (a user or username) and a credential (typically a key pair). Some operations require writing or reading user data to or from the directory. For example, reading the userâ€<sup>™</sup>s phone number to perform multifactor authentication during provisioning or writing the userâ€<sup>™</sup>s public key.

If box **1a** on your planning worksheet reads **cloud only**, write **N/A** in box **1e**. User information is written directly to Azure Active Directory and there is not another directory with which the information must be synchronized.

If box **1a** on your planning worksheet reads **hybrid**, then write **Azure AD Connect** in box **1e** on your planning worksheet.

If box **1a** on your planning worksheet reads **on-premises**, then write **Azure MFA Server**. This deployment exclusively uses Active Directory for user information with the exception of the multifactor authentication. The on-premises Azure MFA server synchronizes a subset of the user information, such as phone number, to provide multifactor authentication while the userâ€<sup>™</sup>s credential remain on the on-premises network.

## Multifactor Authentication

The goal of Windows Hello for Business is to move user authentication away from passwords to a strong, keybased user authentication. Passwords are weak credentials and cannot be trusted by themselves as an attacker with a stolen password could be attempting to enroll in Windows Hello for Business. To keep the transition from a weak to a strong credential secure, Windows Hello for Business relies on multifactor authentication during provisioning to have some assurances that the user identity provisioning a Windows Hello for Business credential is the proper identity.

If box **1a** on your planning worksheet reads **cloud only**, then your only option is to use the Azure MFA cloud service. Write **Azure MFA** in box **1f** on your planning worksheet.

If box **1a** on your planning worksheet reads **hybrid**, then you have a few options, some of which depend on your directory synchronization configuration. The options from which you may choose include:

- Directly use Azure MFA cloud service
- Use AD FS w/Azure MFA cloud service adapter
- Use AD FS w/Azure MFA Server adapter
- Use AD FS w/3rd Party MFA Adapter

You can directly use the Azure MFA cloud service for the second factor of authentication. Users contacting the service must authenticate to Azure prior to using the service.

If your Azure AD Connect is configured to synchronize identities (usernames only), then your users are redirected to your local on-premises federation server for authentication and then redirected back to the Azure MFA cloud service. Otherwise, your Azure AD Connect is configured to synchronize credentials (username and passwords), which enables your users to authenticate to Azure Active Directory and use the Azure MFA cloud service. If you choose to use the Azure MFA cloud service directly, write **Azure MFA** in box **1f** on your planning worksheet.

You can configure your on-premises Windows Server 2016 AD FS role to use the Azure MFA service adapter. In this configuration, users are redirected to the on premises AD FS server (synchronizing identities only). The AD FS server uses the MFA adapter to communicate to the Azure MFA service to perform the second factor of authentication. If you choose to use AD FS with the Azure MFA cloud service adapter, write **AD FS with Azure MFA cloud adapter** in box **1f** on your planning worksheet.

Alternatively, you can use AD FS with an on-premises Azure MFA server adapter. Rather than AD FS communicating directly with the Azure MFA cloud service, it communicates with an on-premises Azure MFA server

that synchronizes user information with the on-premises Active Directory. The Azure MFA server communicates with Azure MFA cloud services to perform the second factor of authentication. If you choose to use AD FS with the Azure MFA server adapter, write **AD FS with Azure MFA server adapter** in box **1f** on your planning worksheet.

The last option is for you to use AD FS with a third-party adapter as the second factor of authentication. If you choose to use AD FS with a third-party MFA adapter, write **AD FS with third party** in box **1f** on your planning worksheet.

If box **1a** on your planning worksheet reads **on-premises**, then you have two second factor authentication options. You must use Windows Server 2016 AD FS with your choice of the on-premises Azure MFA server or with a thirdparty MFA adapter.

If you choose to use AD FS with the Azure MFA server adapter, write **AD FS with Azure MFA server adapter** in box **1f** on your planning worksheet. If you choose to use AD FS with a third-party MFA adapter, write **AD FS with third party** in box **1f** on your planning worksheet.

### Management

Windows Hello for Business provides organizations with many policy settings and granular control on how these settings may be applied to both computers and users. The type of policy management you can use depends on your selected deployment and trust models.

If box **1a** on your planning worksheet reads **cloud only**, write **N/A** in box **2a** on your planning worksheet. You have the option to manage non-domain joined devices. If you choose to manage Azure Active Directory joined devices, write **modern management** in box **2b** on your planning worksheet. Otherwise, write\*\* N/A\*\* in box **2b**.

### NOTE

Azure Active Directory joined devices without modern management automatically enroll in Windows Hello for Business using the default policy settings. Use modern management to adjust policy settings to match the business needs of your organization.

If box **1a** on your planning worksheet reads **on-prem**, write **GP** in box **2a** on your planning worksheet. Write **N/A** in box **2b** on your worksheet.

Managing hybrid deployments includes two categories of devices to consider for your Windows Hello for Business deploymentâ€" domain joined and non-domain joined. All devices are registered, however, not all devices are domain joined. You have the option of using Group Policy for domain joined devices and modern management for non-domain joined devices. Or, you can use modern management for both domain and non-domain joined devices.

If you use Group Policy to manage your domain joined devices, write **GP** in box **2a** on your planning worksheet. Write **modern management** in box **2b** if you decide to manage non-domain joined devices; otherwise, write **N/A**.

If you use modern management for both domain and non-domain joined devices, write **modern management** in box **2a** and **2b** on your planning worksheet.

### Client

Windows Hello for Business is a feature exclusive to Windows 10. Some deployments and features are available using earlier versions of Windows 10. Others need the latest versions.

If box **1a** on your planning worksheet reads **cloud only**, write **N/A** in box **3a** on your planning worksheet. Optionally, you may write **1511 or later** in box **3b** on your planning worksheet if you plan to manage non-domain joined devices.

### NOTE

Azure Active Directory joined devices without modern management automatically enroll in Windows Hello for Business using the default policy settings. Use modern management to adjust policy settings to match the business needs of your organization.

Write 1511 or later in box 3a on your planning worksheet if any of the following are true.

- Box 2a on your planning worksheet read modern management.
  - Optionally, you may write **1511 or later** in box **3b** on your planning worksheet if you plan to manage non-domain joined devices.
- Box **1a** on your planning worksheet reads **hybrid**, box **1b** reads **key trust**, and box **2a** reads **GP**. *Optionally, you may write \*\*1511 or later\** in box **3b** on your planning worksheet if you plan to manage non-domain joined devices.

Write 1703 or later in box 3a on your planning worksheet if any of the following are true.

- Box **1a** on your planning worksheet reads **on-premises**. Write **N/A** in box **3b** on your planning worksheet.
- Box 1a on your planning worksheet reads hybrid, box 1b reads certificate trust, and box 2a reads GP.
  - Optionally, you may write **1511 or later** in box **3b** on your planning worksheet if you plan to manage non-domain joined devices.

## **Active Directory**

The Active Directory portion of the planning guide should be complete. Most of the conditions are baseline prerequisites except for your domain controllers. The domain controllers used in your deployment are decided by the chosen trust type.

Review the trust type portion of this section if box **4d** on your planning worksheet remains empty.

## Public Key Infrastructure

Public key infrastructure prerequisites already exist in your planning worksheet. These conditions are the minimum requirements for any hybrid or on-premises deployment. Additional conditions may be needed based on your trust type.

If box **1a** on your planning worksheet reads **cloud only**, ignore the public key infrastructure section of your planning worksheet. Cloud only deployments do not use a public key infrastructure.

If box 1b on your planning worksheet reads key trust, write N/A in box 5b on your planning worksheet.

The registration authority only relates to certificate trust deployments and the management used for domain and non-domain joined devices. Hybrid Azure AD joined devices managed by Group Policy need the Windows Server 2016 AD FS role to issue certificates. Hybrid Azure AD joined devices and Azure AD joined devices managed by Intune or a compatible MDM need the Windows Server NDES server role to issue certificates.

If box **2a** reads **GP** and box **2b** reads **modern management**, write **AD FS RA and NDES** in box **5b** on your planning worksheet. In box **5c**, write the following certificate templates names and issuances:

CERTIFICATE TEMPLATE NAME	ISSUED TO
Exchange Enrollment Agent	AD FS RA
Web Server	AD FS RA
Exchange Enrollment Agent	NDES

CERTIFICATE TEMPLATE NAME	ISSUED TO
Web Server	NDES
CEP Encryption	NDES

If box **2a** reads **GP** and box **2b** reads **N/A**, write **AD FS RA** in box **5b** and write the following certificate template names and issuances in box **5c** on your planning worksheet.

CERTIFICATE TEMPLATE NAME	ISSUED TO
Exchange Enrollment Agent	AD FS RA
Web Server	AD FS RA

If box **2a** or **2b** reads modern management, write **NDES** in box **5b** and write the following certificate template names and issuances in box 5c on your planning worksheet.

CERTIFICATE TEMPLATE NAME	ISSUED TO
Exchange Enrollment Agent	NDES
Web Server	NDES
CEP Encryption	NDES

## Cloud

Nearly all deployments of Windows Hello for Business require an Azure account.

If box **1a** on your planning worksheet reads **cloud only** or **hybrid**, write **Yes** in boxes **6a** and **6b** on your planning worksheet.

If box **1a** on your planning worksheet reads **on-premises**, and box **1f** reads **AD FS with third party**, write **No** in box **6a** on your planning worksheet. Otherwise, write **Yes** in box **6a** as you need an Azure account for perconsumption MFA billing. Write **No** in box **6b** on your planning worksheetâ€"on-premises deployments do not use the cloud directory.

Windows Hello for Business does not require an Azure AD premium subscription. However, some dependencies do.

If box 1a on your planning worksheet reads on-premises, write No in box 6c on your planning worksheet.

If box **1a** on your planning worksheet reads **hybrid** and box **1b** reads **key trust**, write **No** in box **6c** on your planning worksheet. You can deploy Windows Hello for Business using the free Azure Active Directory account (additional costs needed for multifactor authentication).

If box **5b** on your planning worksheet reads **AD FS RA**, write **Yes** in box **6c** on your planning worksheet. Enrolling a certificate using the AD FS registration authority requires devices to authenticate to the AD FS server, which requires device writebackâ€"an Azure AD Premium feature.

Modern managed devices do not require an Azure AD premium subscription. By forgoing the subscription, your users must manually enroll devices in the modern management software, such as Intune or a supported third-party MDM.

If boxes **2a** or **2b** read **modern management** and you want devices to automatically enroll in your modern management software, write **Yes** in box **6c** on your planning worksheet. Otherwise, write **No** in box **6c**.

## Congratulations, You're Done

Your Windows Hello for Business planning worksheet should be complete. This guide provided understanding of the components used in the Windows Hello for Business infrastructure and rationalization of why they are used. The worksheet gives you an overview of the requirements needed to continue the next phase of the deployment. With this worksheet, you'II be able to identify key elements of your Windows Hello for Business deployment.

## Windows Hello for Business Deployment Guide

2/7/2018 • 2 min to read • Edit Online

## **Applies to**

- Windows 10
- Windows 10 Mobile

This guide only applies to Windows 10, version 1703 or higher.

Windows Hello for Business is the springboard to a world without passwords. It replaces username and password sign-in to Windows with strong user authentication based on an asymmetric key pair.

This deployment guide is to guide you through deploying Windows Hello for Business, based on the planning decisions made using the Planning a Windows Hello for Business Deployment Guide. It provides you with the information needed to successfully deploy Windows Hello for Business in an existing environment.

## Assumptions

This guide assumes that baseline infrastructure exists which meets the requirements for your deployment. For either hybrid or on-premises deployments, it is expected that you have:

- A well-connected, working network
- Internet access
- Multifactor Authentication Server to support MFA during Windows Hello for Business provisioning
- Proper name resolution, both internal and external names
- Active Directory and an adequate number of domain controllers per site to support authentication
- Active Directory Certificate Services 2012 or later
- One or more workstation computers running Windows 10, version 1703

If you are installing a server role for the first time, ensure the appropriate server operating system is installed, updated with the latest patches, and joined to the domain. This document provides guidance to install and configure the specific roles on that server.

Do not begin your deployment until the hosting servers and infrastructure (not roles) identified in your prerequisite worksheet are configured and properly working.

## Deployment and trust models

Windows Hello for Business has two deployment models: Hybrid and On-premises. Each deployment model has two trust models: *Key trust* or *certificate trust*.

Hybrid deployments are for enterprises that use Azure Active Directory. On-premises deployments are for enterprises who exclusively use on-premises Active Directory. Remember that the environments that use Azure Active Directory must use the hybrid deployment model for all domains in that forest.

The trust model determines how you want users to authenticate to the on-premises Active Directory:

- The key-trust model is for enterprises who do not want to issue end-entity certificates to their users and have an adequate number of 2016 domain controllers in each site to support authentication.
- The certificate-trust model is for enterprise that do want to issue end-entity certificates to their users and have

the benefits of certificate expiration and renewal, similar to how smart cards work today.

• The certificate trust model also supports enterprises which are not ready to deploy Windows Server 2016 Domain Controllers.

Following are the various deployment guides included in this topic:

- Hybrid Key Trust Deployment
- Hybrid Certificate Trust Deployment
- On Premises Key Trust Deployment
- On Premises Certificate Trust Deployment

## Provisioning

Windows Hello for Business provisioning begins immediately after the user has signed in, after the user profile is loaded, but before the user receives their desktop. Windows only launches the provisioning experience if all the prerequisite checks pass. You can determine the status of the prerequisite checks by viewing the **User Device Registration** in the **Event Viewer** under **Applications and Services Logs\Microsoft\Windows**.

## Hybrid Azure AD joined Key Trust Deployment

2/7/2018 • 1 min to read • Edit Online

## **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

Windows Hello for Business replaces username and password sign-in to Windows with strong user authentication based on asymmetric key pair. The following deployment guide provides the information needed to successfully deploy Windows Hello for Business in a hybrid key trust scenario.

It is recommended that you review the Windows Hello for Business planning guide prior to using the deployment guide. The planning guide helps you make decisions by explaining the available options with each aspect of the deployment and explains the potential outcomes based on each of these decisions. You can review the planning guide and download the planning worksheet.

This deployment guide provides guidance for new deployments and customers who are already federated with Office 365. These two scenarios provide a baseline from which you can begin your deployment.

## New Deployment Baseline

The new deployment baseline helps organizations who are moving to Azure and Office 365 to include Windows Hello for Business as part of their deployments. This baseline is good for organizations who are looking to deploy proof of concepts as well as IT professionals who want to familiarize themselves Windows Hello for Business by deploying a lab environment.

This baseline provides detailed procedures to move your environment from an on-premises only environment to a hybrid environment using Windows Hello for Business to authenticate to Azure Active Directory and to your on-premises Active Directory using a single Windows sign-in.

You're next step is to familiarize yourself with the prerequisites needed for the deployment. Many of the prerequisites will be new for organizations and individuals pursuing the new deployment baseline. Organizations and individuals starting from the federated baseline will likely be familiar with most of the prerequisites, but should validate they are using the proper versions that include the latest updates.

## Prerequistes

- 1. Overview (You are here)
- 2. Prerequistes
- 3. New Installation Baseline
- 4. Configure Directory Synchronization
- 5. Configure Azure Device Registration

- 6. Configure Windows Hello for Business settings
- 7. Sign-in and Provision

## Hybrid Key trust Windows Hello for Business Prerequisites

4/9/2018 • 4 min to read • Edit Online

## **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

Hybrid environments are distributed systems that enable organizations to use on-premises and Azure-based identities and resources. Windows Hello for Business uses the existing distributed system as a foundation on which organizations can provide two-factor authentication that provides a single sign-in like experience to modern resources.

The distributed systems on which these technologies were built involved several pieces of on-premises and cloud infrastructure. High-level pieces of the infrastructure include:

- Directories
- Public Key Infrastucture
- Directory Synchronization
- Federation
- MultiFactor Authetication
- Device Registration

## Directories

Hybrid Windows Hello for Business needs two directories: on-premises Active Directory and a cloud Azure Active Directory. The minimum required domain functional and forest functional levels for Windows Hello for Business deployment is Windows Server 2008 R2. The

A hybrid Windows Hello for Busines deployment needs an Azure Active Directory subscription. The hybrid key trust deployment, does not need a premium Azure Active Directory subscription.

You can deploy Windows Hello for Business in any environment with Windows Server 2008 R2 or later domain controllers. However, the key trust deployment needs an *adequate* number of Windows Server 2016 domain controllers at each site where users authenticate using Windows Hello for Business. Read the Planning an adequate number of Windows Server 2016 Domain Controllers for Windows Hello for Business deployments to learn more.

Review these requirements and those from the Windows Hello for Business planning guide and worksheet. Based on your deployment decisions you may need to upgrade your on-premises Active Directory or your Azure Active Directory subscription to meet your needs.

### **Section Review**

- Active Directory Domain Functional Level
- Active Directory Forest Functional Level
- Domain Controller version
- Azure Active Directory subscription
- Correct subscription for desired features and outcomes

## Public Key Infrastructure

The Windows Hello for Business deployment depends on an enterprise public key infrastructure as trust anchor for authentication. Domain controllers for hybrid deployments need a certificate in order for Windows 10 devices to trust the domain controller.

Key trust deployments do not need client issued certificates for on-premises authentication. Active Directory user accounts are automatically configured for public key mapping by Azure AD Connect synchronizing the public key of the registered Windows Hello for Business credential to an attribute on the user's Active Directory object.

The minimum required enterprise certificate authority that can be used with Windows Hello for Business is Windows Server 2012.

#### IMPORTANT

For Azure AD joined device to authenticate to and use on-premises resources, ensure you:

- Install the root certificate authority certificate for your organization in the user's trusted root certifcate store.
- Publish your certificate revocation list to a location that is available to Azure AD joined devices, such as a web-based url.

### **Section Review**

• Windows Server 2012 Issuing Certificate Authority

## **Directory Synchronization**

The two directories used in hybrid deployments must be synchronized. You need Azure Active Directory Connect to synchronize user accounts in the on-premises Active Directory with Azure Active Directory.

Organizations using older directory synchronization technology, such as DirSync or Azure AD sync need to upgrade to Azure AD Connect.

## **Section Review**

- Azure Active Directory Connect directory synchronization
- Upgrade from DirSync
- Upgrade from Azure AD Sync

## Federation with Azure

You can deploy Windows Hello for Business key trust in non-federated and federated environments. For nonfederated environments, key trust deployments work in environments that have deployed Password Synchronization with Azure AD Connect and Azure Active Directory Pass-through-Authentication. For federated environments, you can deploy Windows Hello for Business key trust using Active Directory Federation Services (AD FS) 2012 R2 or later.

## **Section Review**

- Non-federated environments
- Federated environments

## Multifactor Authentication

Windows Hello for Business is a strong, two-factor credential the helps organizations reduce their dependency on passwords. The provisioning process lets a user enroll in Windows Hello for Business using their username and password as one factor, but needs a second factor of authentication.

Hybrid Windows Hello for Business deployments can use Azureâ€<sup>™</sup>s Multifactor Authentication service or they can use multifactor authentication provides by Windows Server 2012 R2 or later Active Directory Federation Services, which includes an adapter model that enables third parties to integrate their multifactor authentication into AD FS.

## **Section Review**

- Azure MFA Service
- Windows Server 2016 AD FS and Azure (optional, if federated)
- Windows Server 2016 AD FS and third party MFA Adapter (optional, if federated)

## **Device Registration**

Organizations wanting to deploy hybrid key trust need thier domain joined devices to register to Azure Active Directory. Just as a computer has an identity in Active Directory, that same computer has an identity in the cloud. This ensures that only approved computers are used with that Azure Active Directory. Each computer registers its identity in Azure Active Directory.

## Section Checklist

• Device Registration with Azure Device Registration

## **Next Steps**

Follow the Windows Hello for Business hybrid key trust deployment guide. For proof-of-concepts, labs, and new installations, choose the **New Installation Basline**.

For environments transitioning from on-premises to hybrid, start with **Configure Azure Directory Syncrhonization**.

For federerated and non-federated environments, start with Configure Windows Hello for Business settings.

- 1. Overview
- 2. Prerequistes (You are here)
- 3. New Installation Baseline
- 4. Configure Directory Synchronization
- 5. Configure Azure Device Registration
- 6. Configure Windows Hello for Business settings
- 7. Sign-in and Provision

# Windows Hello for Business Key Trust New Installation

4/9/2018 • 5 min to read • Edit Online

## **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

Windows Hello for Business involves configuring distributed technologies that may or may not exist in your current infrastructure. Hybrid key trust deployments of Windows Hello for Business rely on these technolgies

- Active Directory
- Public Key Infrastructure
- Azure Active Directory
- Active Directory Federation Services

New installations are considerably more involved than existing implementations because you are building the entire infrastructure. Microsoft recommends you review the new installation baseline to validate your exsting envrionment has all the needed configurations to support your hybrid certificate trust Windows Hello for Business deployment. If your environment meets these needs, you can read the Configure Directory Synchronization section to prepare your Windows Hello for Business deployment by configuring directory synchronization.

The new installation baseline begins with a basic Active Directory deployment and enterprise PKI.

## Active Directory

This document expects you have Active Directory deployed with an *adequate* number of Windows Server 2016 domain controllers for each site. Read the Planning an adequate number of Windows Server 2016 Domain Controllers for Windows Hello for Business deployments to learn more.

Lab environments and isolated proof of concepts may want to limit the number of domain controllers. The purpose of these environments is to experiment and learn. Reducing the number of domain controllers can prevent troubleshooting issue, such as Active Directory replication, which is unrelated to activity's goal.

### **Section Review**

- An adequate number of Windows Server 2016 domain controllers
- Minimum Windows Server 2008 R2 domain and forest functional level
- Functional networking, name resolution, and Active Directory replication

## Public Key Infrastructure

Windows Hello for Business must have a public key infrastructure regardless of the deployment or trust model. All trust models depend on the domain controllers having a certificate. The certificate serves as a root of trust for clients to ensure they are not communicating with a rogue domain controller.

This guide assumes most enterprises have an existing public key infrastructure. Windows Hello for Business depends on a Windows enterprise public key infrastructure running the Active Directory Certificate Services role from Windows Server 2012 or later.

#### Lab-based public key infrastructure

The following instructions may be used to deploy simple public key infrastructure that is suitable for a lab environment.

Sign-in using *Enterprise Admin* equivalent credentials on Windows Server 2012 or later server where you want the certificate authority installed.

#### NOTE

Never install a certificate authority on a domain controller in a production environment.

- 1. Open an elevated Windows PowerShell prompt.
- 2. Use the following command to install the Active Directory Certificate Services role.

Add-WindowsFeature Adcs-Cert-Authority -IncludeManageTools

3. Use the following command to configure the Certificate Authority using a basic certificate authority configuration.

Install-AdcsCertificateAuthority

## Configure a Production Public Key Infrastructure

If you do not have an existing public key infrastructure, please review Certification Authority Guidance from Microsoft TechNet to properly design your infrastructure. Then, consult the Test Lab Guide: Deploying an AD CS Two-Tier PKI Hierarchy for instructions on how to configure your public key infrastructure using the information from your design session.

#### **IMPORTANT**

For Azure AD joined device to authenticate to and use on-premises resources, ensure you:

- Install the root certificate authority certificate for your organization in the user's trusted root certificate store.
- Publish your certificate revocation list to a location that is available to Azure AD joined devices, such as a web-based url.

#### **Section Review**

- Miniumum Windows Server 2012 Certificate Authority.
- Enterprise Certificate Authority.
- Functioning public key infrastructure.
- Root certifcate authority certificate (Azure AD Joined devices).
- Highly available certificate revoication list (Azure AD Joined devices).

## Azure Active Directory

You've prepared your Active Directory. Hybrid Windows Hello for Business deployment needs Azure Active Directory to host your cloud-based identities.

The next step of the deployment is to follow the Creating an Azure AD tenant process to provision an Azure tenant for your organization.

#### **Section Review**

- Review the different ways to establish an Azure Active Directory tenant.
- Create an Azure Active Directory Tenant.
- Purchase the appropriate Azure Active Directory subscription or licenses, if necessary.

## Multifactor Authentication Services

Windows Hello for Business uses multifactor authentication during provisioning and during user initiated PIN reset scenarios, such as when a user forgets their PIN. There are two preferred multifactor authentication configurations with hybrid deploymentsâ€"Azure MFA and AD FS using Azure MFA or a third-party MFA adapter

Review the What is Azure Multi-Factor Authentication topic to familiarize yourself its purpose and how it works.

#### Azure Multi-Factor Authentication (MFA) Cloud

#### **IMPORTANT**

As long as your users have licenses that include Azure Multi-Factor Authentication, there's nothing that you need to do to turn on Azure MFA. You can start requiring two-step verification on an individual user basis. The licenses that enable Azure MFA are:

- Azure Multi-Factor Authentication
- Azure Active Directory Premium
- Enterprise Mobility + Security

If you have one of these subscriptions or licenses, skip the Azure MFA Adapter section.

#### Azure MFA Provider

If your organization uses Azure MFA on a per-consumption model (no licenses), then review the Create a Multifactor Authentication Provider section to create an Azure MFA Authentication provider and associate it with your Azure tenant.

#### **Configure Azure MFA Settings**

Once you have created your Azure MFA authentication provider and associated it with an Azure tenant, you need to configure the multi-factor authentication settings. Review the Configure Azure Multi-Factor Authentication settings section to configure your settings.

#### Azure MFA User States

After you have completed configuring your Azure MFA settings, you want to review configure User States to understand user states. User states determine how you enable Azure MFA for your users.

#### Azure MFA via ADFS

Alternatively, you can configure Windows Server 2016 Active Directory Federation Services (AD FS) to provide additional multi-factor authentication. To configure, read the Configure AD FS 2016 and Azure MFA section.

#### **Section Review**

- Review the overview and uses of Azure Multifactor Authentication.
- Review your Azure Active Directory subscription for Azure Multifactor Authentication.
- Create an Azure Multifactor Authentication Provider, if necessary.
- Configure Azure Multufactor Authentiation features and settings.
- Understand the different User States and their effect on Azure Multifactor Authentication.
- Consider using Azure Multifactor Authentication or a third-party multifactor authentication provider with Windows Server Active Directory Federation Services, if necessary.

#### **Configure Azure Device Registration**

- 1. Overview
- 2. Prerequistes
- 3. New Installation Baseline (You are here)
- 4. Configure Directory Synchronization
- 5. Configure Azure Device Registration
- 6. Configure Windows Hello for Business settings
- 7. Sign-in and Provision

# Configure Directory Synchronization for Hybrid key trust Windows Hello for Business

2/7/2018 • 1 min to read • Edit Online

## **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

You are ready to configure directory synchronization for your hybrid environment. Hybrid Windows Hello for Business deployment needs both a cloud and an on-premises identity to authenticate and access resources in the cloud or on-premises.

## Deploy Azure AD Connect

Next, you need to synchronizes the on-premises Active Directory with Azure Active Directory. To do this, first review the Integrating on-prem directories with Azure Active Directory and hardware and prerequisites needed and then download the software.

- 1. Overview
- 2. Prerequistes
- 3. New Installation Baseline
- 4. Configure Directory Synchronization (You are here)
- 5. Configure Azure Device Registration
- 6. Configure Windows Hello for Business settings
- 7. Sign-in and Provision

## Configure Device Registration for Hybrid key trust Windows Hello for Business

2/7/2018 • 1 min to read • Edit Online

## **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

You are ready to configure device registration for your hybrid environment. Hybrid Windows Hello for Business deployment needs device registration to enable proper device authentication.

#### NOTE

Before proceeding, you should familiarize yourself with device regisration concepts such as:

- Azure AD registered devices
- Azure AD joined devices
- Hybrid Azure AD joined devices

You can learn about this and more by reading Introduction to Device Management in Azure Active Directory.

## Configure Azure for Device Registration

Begin configuring device registration to support Hybrid Windows Hello for Business by configuring device registration capabilities in Azure AD.

To do this, follow the **Configure device settings** steps under Setting up Azure AD Join in your organization

Next, follow the guidance on the How to configure hybrid Azure Active Directory joined devices page. In the **Configuration steps** section, identify you configuration at the top of the table (either **Windows current and password hash sync** or **Windows current and federation**) and perform only the steps identified with a checkmark.

- 1. Overview
- 2. Prerequistes
- 3. New Installation Baseline
- 4. Configure Directory Synchronization
- 5. Configure Azure Device Registration (You are here)
- 6. Configure Windows Hello for Business settings
- 7. Sign-in and Provision

# Configure Hybrid Windows Hello for Business key trust settings

2/7/2018 • 1 min to read • Edit Online

## **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

You are ready to configure your hybrid key trust environment for Windows Hello for Business.

#### IMPORTANT

Ensure your environment meets all the prerequistes before proceeding. Review the New Installation baseline section of this deployment document to learn how to prepare your environment for your Windows Hello for Business deployment.

The configuration for Windows Hello for Business is grouped in four categories. These categories are:

- Active Directory
- Azure AD Connect
- Public Key Infrastructure
- Group Policy

For the most efficent deployment, configure these technologies in order beginning with the Active Directory configuration



- 1. Overview
- 2. Prerequistes
- 3. New Installation Baseline
- 4. Configure Directory Synchronization
- 5. Configure Azure Device Registration
- 6. Configure Windows Hello for Business settings (You are here)
- 7. Sign-in and Provision

## Hybrid Windows Hello for Business Provisioning

2/7/2018 • 2 min to read • Edit Online

## **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

## Provisioning

The Windows Hello for Business provisioning begins immediately after the user has signed in, after the user profile is loaded, but before the user receives their desktop. Windows only launches the provisioning experience if all the prerequisite checks pass. You can determine the status of the prerequisite checks by viewing the **User Device Registration** in the **Event Viewer** under **Applications and Services Logs\Microsoft\Windows**.



The first thing to validate is the computer has processed device registration. You can view this from the User device registration logs where the check **Device is AAD joined (AADJ or DJ++): Yes** appears. Additionally, you can validate this using the **dsregcmd /status** command from a console prompt where the value for **AzureADJoined** reads **Yes**.

Windows Hello for Business provisioning begins with a full screen page with the title **Setup a PIN** and button with the same name. The user clicks **Setup a PIN**.



The provisioning flow proceeds to the Multi-Factor authentication portion of the enrollment. Provisioning informs the user that it is actively attempting to contact the user through their configured form of MFA. The provisioning process does not proceed until authentication succeeds, fails or times out. A failed or timeout MFA results in an error and asks the user to retry.



After a successful MFA, the provisioning flow asks the user to create and validate a PIN. This PIN must observe any PIN complexity requirements that you deployed to the environment.

		•.	
Windows Set uj	s Security p a PIN		×
Create makes	a PIN to use in place of it easier to sign in to yo	f passwords. Having a PIN our device, apps, and servin	ces.
	•••••	୕	
	OK	Cancel	
		k	

The provisioning flow has all the information it needs to complete the Windows Hello for Business enrollment.

- A successful single factor authentication (username and password at sign-in)
- A device that has successfully completed device registration
- A fresh, successful multi-factor authentication
- A validated PIN that meets the PIN complexity requirements

The remainder of the provisioning includes Windows Hello for Business requesting an asymmetric key pair for the user, preferably from the TPM (or required if explicitly set through policy). Once the key pair is acquired, Windows communicates with Azure Active Directory to register the public key. When key registration completes, Windows Hello for Business provisioning informs the user they can use their PIN to sign-in. The user may close the provisiong application and see their desktop. While the user has completed provisioning, Azure AD Connect syncrhonizes the user's key to Active Directory.

#### IMPORTANT

The minimum time needed to syncrhonize the user's public key from Azure Active Directory to the on-premises Active Directory is 30 minutes. The Azure AD Connect scheduler controls the synchronization interval. **This synchronization latency delays the the user's ability to authenticate and use on-premises resouces until the user's public key has synchronized to Active Directory.** Once synchronized, the user can authenticate and use on-premises resources. Read Azure AD Connect sync: Scheduler to view and adjust the **synchronization cycle** for your organization.

## NOTE

Microsoft is actively investigating ways to reduce the synchronization latency and delays.

- 1. Overview
- 2. Prerequistes
- 3. New Installation Baseline
- 4. Configure Directory Synchronization
- 5. Configure Azure Device Registration
- 6. Configure Windows Hello for Business settings
- 7. Sign-in and Provision(You are here)

## Hybrid Azure AD joined Certificate Trust Deployment

2/7/2018 • 2 min to read • Edit Online

## **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

Windows Hello for Business replaces username and password sign-in to Windows with strong user authentication based on asymmetric key pair. The following deployment guide provides the information needed to successfully deploy Windows Hello for Business in a hybrid certificate trust scenario.

It is recommended that you review the Windows Hello for Business planning guide prior to using the deployment guide. The planning guide helps you make decisions by explaining the available options with each aspect of the deployment and explains the potential outcomes based on each of these decisions. You can review the planning guide and download the planning worksheet.

This deployment guide provides guidance for new deployments and customers who are already federated with Office 365. These two scenarios provide a baseline from which you can begin your deployment.

## New Deployment Baseline

The new deployment baseline helps organizations who are moving to Azure and Office 365 to include Windows Hello for Business as part of their deployments. This baseline is good for organizations who are looking to deploy proof of concepts as well as IT professionals who want to familiarize themselves Windows Hello for Business by deploying a lab environment.

This baseline provides detailed procedures to move your environment from an on-premises only environment to a hybrid environment using Windows Hello for Business to authenticate to Azure Active Directory and to your on-premises Active Directory using a single Windows sign-in.

## Federated Baseline

The federated baseline helps organizations that have completed their federation with Azure Active Directory and Office 365 and enables them to introduce Windows Hello for Business into their hybrid environment. This baseline exclusively focuses on the procedures needed to add Azure Device Registration and Windows Hello for Business to an existing hybrid deployment.

Regardless of the baseline you choose, you're next step is to familiarize yourself with the prerequisites needed for the deployment. Many of the prerequisites will be new for organizations and individuals pursuing the new deployment baseline. Organizations and individuals starting from the federated baseline will likely be familiar with most of the prerequisites, but should validate they are using the proper versions that include the latest updates.

## Prerequistes

- 1. Overview (You are here)
- 2. Prerequistes
- 3. New Installation Baseline
- 4. Device Registration
- 5. Configure Windows Hello for Business settings
- 6. Sign-in and Provision

## Hybrid Windows Hello for Business Prerequisites

4/9/2018 • 4 min to read • Edit Online

## **Applies to**

Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

Hybrid environments are distributed systems that enable organizations to use on-premises and Azure-based identities and resources. Windows Hello for Business uses the existing distributed system as a foundation on which organizations can provide two-factor authentication that provides a single sign-in like experience to modern resources.

The distributed systems on which these technologies were built involved several pieces of on-premises and cloud infrastructure. High-level pieces of the infrastructure include:

- Directories
- Public Key Infrastucture
- Directory Synchronization
- Federation
- MultiFactor Authetication
- Device Registration

## Directories

Hybrid Windows Hello for Business needs two directories: on-premises Active Directory and a cloud Azure Active Directory. The minimum required domain controller, domain functional level, and forest functional level for Windows Hello for Business deployment is Windows Server 2008 R2.

A hybrid Windows Hello for Busines deployment needs an Azure Active Directory subscription. Different deployment configurations are supported by different Azure subscriptions. The hybrid-certificate trust deployment needs an Azure Active Directory premium subscription because it uses the device write-back synchronization feature. Other deployments, such as the hybrid key-trust deployment, may not require Azure Active Directory premium subscription.

Windows Hello for Business can be deployed in any environment with Windows Server 2008 R2 or later domain controllers. Azure device registration and Windows Hello for Business require the Windows Server 2016 Active Directory schema.

Review these requirements and those from the Windows Hello for Business planning guide and worksheet. Based on your deployment decisions you may need to upgrade your on-premises Active Directory or your Azure Active Directory subscription to meet your needs.

### **Section Review**

- Active Directory Domain Functional Level
- Active Directory Forest Functional Level
- Domain Controller version
- Windows Server 2016 Schema
- Azure Active Directory subscription

• Correct subscription for desired features and outcomes

## Public Key Infrastructure

The Windows Hello for Business deployment depends on an enterprise public key infrastructure as trust anchor for authentication. Domain controllers for hybrid deployments need a certificate in order for Windows 10 devices to trust the domain controller.

Certificate trust deployments need an enterprise public key infrastructure and a certificate registration authority to issue authentication certificates to users. When using Group Policy, hybrid certificate trust deployment use the Windows Server 2016 Active Directory Federation Server (AS FS) as a certificate registration authority.

The minimum required enterprise certificate authority that can be used with Windows Hello for Business is Windows Server 2012.

## **Section Review**

- Windows Server 2012 Issuing Certificate Authority
- Windows Server 2016 Active Directory Federation Services

## **Directory Synchronization**

The two directories used in hybrid deployments must be synchronized. You need Azure Active Directory Connect to synchronize user accounts in the on-premises Active Directory with Azure Active Directory.

Organizations using older directory synchronization technology, such as DirSync or Azure AD sync need to upgrade to Azure AD Connect

## **Section Review**

- Azure Active Directory Connect directory synchronization
- Upgrade from DirSync
- Upgrade from Azure AD Sync

## Federation

Federating your on-premises Active Directory with Azure Active Directory ensures all identities have access to all resources regardless if they reside in cloud or on-premises. Windows Hello for Business hybrid certificate trust needs Windows Server 2016 Active Directory Federation Services. All nodes in the AD FS farm must run the same version of AD FS. Additionally, you need to configure your AD FS farm to support Azure registered devices.

The AD FS farm used with Windows Hello for Business must be Windows Server 2016 with minimum update of KB4088889 (14393.2155). If your AD FS farm is not running the AD FS role with updates from Windows Server 2016, then read Upgrading to AD FS in Windows Server 2016

## **Section Review**

- Windows Server 2016 Active Directory Federation Services
- Minimum update of KB4088889 (14393.2155)

## Multifactor Authentication

Windows Hello for Business is a strong, two-factor credential the helps organizations reduce their dependency on passwords. The provisioning process lets a user enroll in Windows Hello for Business using their username and password as one factor. but needs a second factor of authentication.

Hybrid Windows Hello for Business deployments can use Azure's Multifactor Authentication service or they can use multifactor authentication provides by Windows Server 2016 Active Directory Federation Services, which includes an adapter model that enables third parties to integrate their multifactor authentication into AD FS.

## **Section Review**

- Azure MFA Service
- Windows Server 2016 AD FS and Azure
- Windows Server 2016 AD FS and third party MFA Adapter

## **Device Registration**

Organizations wanting to deploy hybrid certificate trust need thier domain joined devices to register to Azure Active Directory. Just as a computer has an identity in Active Directory, that same computer has an identity in the cloud. This ensures that only approved computers are used with that Azure Active Directory. Each computer registers its identity in Azure Active Directory.

Hybrid certificate trust deployments need the device write back feature. Authentication to the Windows Server 2016 Active Directory Federation Services needs both the user and the computer to authenticate. Typically the users are synchronized, but not devices. This prevents AD FS from authenticating the computer and results in Windows Hello for Business certificate enrollment failures. For this reason, Windows Hello for Business deployments need device writeback, which is an Azure Active Directory premium feature.

## **Section Checklist**

- Azure Active Directory Device writeback
- Azure Active Directory Premium subscription

## **Next Steps**

Follow the Windows Hello for Business hybrid certificate trust deployment guide. For proof-of-concepts, labs, and new installations, choose the **New Installation Basline**.

If your environment is already federated, but does not include Azure device registration, choose **Configure Azure Device Registration**.

If your environment is already federated and supports Azure device registration, choose **Configure Windows Hello for Business settings**.

- 1. Overview
- 2. Prerequistes (You are here)
- 3. New Installation Baseline

- 4. Configure Azure Device Registration
- 5. Configure Windows Hello for Business settings
- 6. Sign-in and Provision
# Windows Hello for Business Certificate Trust New Installation

2/7/2018 • 5 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

Windows Hello for Business involves configuring distributed technologies that may or may not exist in your current infrastructure. Hybrid certificate trust deployments of Windows Hello for Business rely on these technolgies

- Active Directory
- Public Key Infrastructure
- Azure Active Directory
- Active Directory Federation Services

New installations are considerably more involved than existing implementations because you are building the entire infrastructure. Microsoft recommends you review the new installation baseline to validate your existing envrionment has all the needed configurations to support your hybrid certificate trust Windows Hello for Business deployment. If your environment meets these needs, you can read the Configure Azure Device Registration section to prepare your Windows Hello for Business deployment by configuring Azure device registration.

The new installation baseline begins with a basic Active Directory deployment and enterprise PKI. This document expects you have Active Directory deployed using Windows Server 2008 R2 or later domain controllers.

## Active Directory

Production environments should follow Active Directory best practices regarding the number and placement of domain controllers to ensure adequate authentication throughout the organization.

Lab environments and isolated proof of concepts may want to limit the number of domain controllers. The purpose of these environments is to experiment and learn. Reducing the number of domain controllers can prevent troubleshooting issue, such as Active Directory replication, which is unrelated to activity's goal.

#### **Section Review**

- Minimum Windows Server 2008 R2 domain controllers
- Minimum Windows Server 2008 R2 domain and forest functional level
- Functional networking, name resolution, and Active Directory replication

## Public Key Infrastructure

Windows Hello for Business must have a public key infrastructure regardless of the deployment or trust model. All trust models depend on the domain controllers having a certificate. The certificate serves as a root of trust for clients to ensure they are not communicating with a rogue domain controller. The certificate trust model extends certificate issuance to client computers. During Windows Hello for Business provisioning, the user receives a sign-in certificate. This guide assumes most enterprises have an existing public key infrastructure. Windows Hello for Business depends on a Windows enterprise public key infrastructure running the Active Directory Certificate Services role from Windows Server 2012 or later.

#### Lab-based public key infrastructure

The following instructions may be used to deploy simple public key infrastructure that is suitable for a lab environment.

Sign-in using *Enterprise Admin* equivalent credentials on Windows Server 2012 or later server where you want the certificate authority installed.

#### NOTE

Never install a certificate authority on a domain controller in a production environment.

- 1. Open an elevated Windows PowerShell prompt.
- 2. Use the following command to install the Active Directory Certificate Services role.

```
Add-WindowsFeature Adcs-Cert-Authority -IncludeManageTools
```

3. Use the following command to configure the Certificate Authority using a basic certificate authority configuration.

Install-AdcsCertificateAuthority

## Configure a Production Public Key Infrastructure

If you do have an existing public key infrastructure, please review Certification Authority Guidance from Microsoft TechNet to properly design your infrastructure. Then, consult the Test Lab Guide: Deploying an AD CS Two-Tier PKI Hierarchy for instructions on how to configure your public key infrastructure using the information from your design session.

#### **Section Review**

- Miniumum Windows Server 2012 Certificate Authority.
- Enterprise Certificate Authority.
- Functioning public key infrastructure.

## **Azure Active Directory**

You've prepared your Active Directory. Hybrid Windows Hello for Business deployment needs Azure Active Directory to host your cloud-based identities.

The next step of the deployment is to follow the Creating an Azure AD tenant process to provision an Azure tenant for your organization.

#### **Section Review**

- Review the different ways to establish an Azure Active Directory tenant.
- Create an Azure Active Directory Tenant.
- Purchase the appropriate Azure Active Directory subscription or licenses, if necessary.

### Multifactor Authentication Services

Windows Hello for Business uses multifactor authentication during provisioning and during user initiated PIN reset scenarios, such as when a user forgets their PIN. There are two preferred multifactor authentication configurations with hybrid deployments—Azure MFA and AD FS using Azure MFA

Review the What is Azure Multi-Factor Authentication topic to familiarize yourself its purpose and how it works.

#### Azure Multi-Factor Authentication (MFA) Cloud

#### IMPORTANT

As long as your users have licenses that include Azure Multi-Factor Authentication, there's nothing that you need to do to turn on Azure MFA. You can start requiring two-step verification on an individual user basis. The licenses that enable Azure MFA are:

- Azure Multi-Factor Authentication
- Azure Active Directory Premium
- Enterprise Mobility + Security

If you have one of these subscriptions or licenses, skip the Azure MFA Adapter section.

#### Azure MFA Provider

If your organization uses Azure MFA on a per-consumption model (no licenses), then review the Create a Multifactor Authentication Provider section to create an Azure MFA Authentication provider and associate it with your Azure tenant.

#### **Configure Azure MFA Settings**

Once you have created your Azure MFA authentication provider and associated it with an Azure tenant, you need to configure the multi-factor authentication settings. Review the Configure Azure Multi-Factor Authentication settings section to configure your settings.

#### Azure MFA User States

After you have completed configuring your Azure MFA settings, you want to review configure User States to understand user states. User states determine how you enable Azure MFA for your users.

#### Azure MFA via ADFS 2016

Alternatively, you can configure Windows Server 2016 Active Directory Federation Services (AD FS) to provide additional multi-factor authentication. To configure, read the Configure AD FS 2016 and Azure MFA section

#### **Section Review**

- Review the overview and uses of Azure Multifactor Authentication.
- Review your Azure Active Directory subscription for Azure Multifactor Authentication.
- Create an Azure Multifactor Authentication Provider, if necessary.
- Configure Azure Multufactor Authentiation features and settings.
- Understand the different User States and their effect on Azure Multifactor Authentication.
- Consider using Azure Multifactor Authentication or a third-party multifactor authentication provider with Windows Server 2016 Active Directory Federation Services, if necessary.

#### Configure Azure Device Registration

Follow the Windows Hello for Business hybrid certificate trust deployment guide

- 1. Overview
- 2. Prerequistes
- 3. New Installation Baseline (You are here)
- 4. Configure Azure Device Registration
- 5. Configure Windows Hello for Business settings
- 6. Sign-in and Provision

# Configure Device Registration for Hybrid Windows Hello for Business

4/9/2018 • 14 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

You're environment is federated and you are ready to configure device registration for your hybrid environment. Hybrid Windows Hello for Business deployment needs device registration and device write-back to enable proper device authentication.

#### IMPORTANT

If your environment is not federated, review the New Installation baseline section of this deployment document to learn how to federate your environment for your Windows Hello for Business deployment.

Use this three phased approach for configuring device registration.

- 1. Configure devices to register in Azure
- 2. Synchronize devices to on-premises Active Directory
- 3. Configure AD FS to use cloud devices

#### NOTE

Before proceeding, you should familiarize yourself with device regisration concepts such as:

- Azure AD registered devices
- Azure AD joined devices
- Hybrid Azure AD joined devices

You can learn about this and more by reading Introduction to Device Management in Azure Active Directory.

## Configure Azure for Device Registration

Begin configuring device registration to support Hybrid Windows Hello for Business by configuring device registration capabilities in Azure AD.

To do this, follow the Configure device settings steps under Setting up Azure AD Join in your organization

## Configure Active Directory to support Azure device synchronization

Azure Active Directory is now configured for device registration. Next, you need to configure the on-premises Active Directory to support synchronizing hybrid Azure AD joined devices. Begin with upgrading the Active Directory Schema

#### Upgrading Active Directory to the Windows Server 2016 Schema

To use Windows Hello for Business with Hybrid Azure AD joined devices, you must first upgrade your Active

Directory schema to Windows Server 2016.

#### **IMPORTANT**

If you already have a Windows Server 2016 domain controller in your forest, you can skip **Upgrading Active Directory to the Windows Server 2016 Schema** (this section).

#### Identify the schema role domain controller

To locate the schema master role holder, open and command prompt and type:

Netdom query fsmo | findstr -i schema

Administrator: C:\Windows\system32\cmd.exe

 Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\labadmin>netdom query fsmo | findstr -i "schema"
Schema master
 dc1.corp.mstepdemo.net
C:\Users\labadmin>

The command should return the name of the domain controller where you need to adprep.exe. Update the schema locally on the domain controller hosting the Schema master role.

#### Updating the Schema

Windows Hello for Business uses asymmetric keys as user credentials (rather than passwords). During enrollment, the public key is registered in an attribute on the user object in Active Directory. The schema update adds this new attribute to Active Directory.

Manually updating Active Directory uses the command-line utility **adprep.exe** located at **<drive>:\support\adprep** on the Windows Server 2016 DVD or ISO. Before running adprep.exe, you must identify the domain controller hosting the schema master role.

Sign-in to the domain controller hosting the schema master operational role using Enterprise Admin equivalent credentials.

- 1. Open an elevated command prompt.
- 2. Type cd /d x:\support\adprep where x is the drive letter of the DVD or mounted ISO.
- 3. To update the schema, type adprep /forestprep .
- 4. Read the Adprep Warning. Type the letter C\* and press Enter to update the schema.
- 5. Close the Command Prompt and sign-out.

#### NOTE

If you installed Azure AD Connect prior to upgrading the schema, you will need to re-run the Azure AD Connect installation and refresh the on-premises AD schema to ensure the synchronization rule for msDS-KeyCredentialLink is configured.

#### **Setup Active Directory Federation Services**

If you are new to AD FS and federation services, you should review Understanding Key AD FS Concepts to prior to designing and deploying your federation service. Review the AD FS Design guide to plan your federation service.

Once you have your AD FS design ready, review Deploying a Federation Server farm to configure AD FS in your environment.

#### **IMPORTANT**

During your AD FS deployment, skip the **Configure a federation server with Device Registration Service** and the **Configure Corporate DNS for the Federation Service and DRS** procedures.

The AD FS farm used with Windows Hello for Business must be Windows Server 2016 with minimum update of KB4088889 (14393.2155). If your AD FS farm is not running the AD FS role with updates from Windows Server 2016, then read Upgrading to AD FS in Windows Server 2016

#### **ADFS Web Proxy**

Federation server proxies are computers that run AD FS software that have been configured manually to act in the proxy role. You can use federation server proxies in your organization to provide intermediary services between an Internet client and a federation server that is behind a firewall on your corporate network. Use the Setting of a Federation Proxy checklist to configure AD FS proxy servers in your environment.

#### **Deploy Azure AD Connect**

Next, you need to synchronizes the on-premises Active Directory with Azure Active Directory. To do this, first review the Integrating on-prem directories with Azure Active Directory and hardware and prerequisites needed and then download the software.

When you are ready to install, follow the **Configuring federation with AD FS** section of Custom installation of Azure AD Connect. Select the **Federation with AD FS** option on the **User sign-in** page. At the **AD FS Farm** page, select the use an existing option and click **Next**.

#### Create AD objects for AD FS Device Authentication

If your AD FS farm is not already configured for Device Authentication (you can see this in the AD FS Management console under Service -> Device Registration), use the following steps to create the correct AD DS objects and configuration.



#### NOTE

The below commands require Active Directory administration tools, so if your federation server is not also a domain controller, first install the tools using step 1 below. Otherwise you can skip step 1.

 Run the Add Roles & Features wizard and select feature Remote Server Administration Tools -> Role Administration Tools -> AD DS and AD LDS Tools -> Choose both the Active Directory module for Windows PowerShell and the AD DS Tools.



1. On your AD FS primary server, ensure you are logged in as AD DS user with Enterprise Admin (EA ) privileges and open an elevated Windows PowerShell prompt. Then, run the following commands:



2. On the pop-up window click **Yes**.

#### NOTE

If your AD FS service is configured to use a GMSA account, enter the account name in the format "domain\accountname\$"

PS C:\Users\Administrator> Import-Modu	le activedirectory
PS C:\Users\Administrator> Initialize-	ADDeviceRegistration -ServiceAccountName "Contoso\A
	🛃 This command will prepare — 🗆 🗙
	Do you want to continue with this operation?
	Yes Ves to All No to All Suspend

The above PSH creates the following objects:

- RegisteredDevices container under the AD domain partition
- Device Registration Service container and object under Configuration --> Services --> Device Registration Configuration
- Device Registration Service DKM container and object under Configuration --> Services --> Device Registration Configuration

Executing precheck tests Verifying the target computer is joined to a domain	^
Executing prerequisite tests Populating Device Registration Service setup settings	
Performing configuration Setting mfa access control policy to Device Registration Relying Party trust	
	$\sim$

1. Once this is done, you will see a successful completion message.

PS C:\Users\Administrator> Import-Module activedirectory									
PS C:\Users\Administrator> Initialize-ADDeviceRegistration -ServiceAccountName "Contoso\A									
Message	Context	Status							
The configuration completed successfully.	. DeploymentSucceede	d Success							
PS C:\Users\Administrator>									

#### Create Service Connection Point (SCP) in Active Directory

If you plan to use Windows 10 domain join (with automatic registration to Azure AD) as described here, execute the following commands to create a service connection point in AD DS

1. Open Windows PowerShell and execute the following:

PS C:>Import-Module -Name "C:\Program Files\Microsoft Azure Active Directory Connect\AdPrep\AdSyncPrep.psm1"

#### NOTE

If necessary, copy the AdSyncPrep.psm1 file from your Azure AD Connect server. This file is located in Program Files/Microsoft Azure Active Directory Connect\AdPrep

📙   🛃 📕 🖛   Ad	Prep			-	_		×
File Home	Share	View					~ ?
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$	« Mic	crosoft Azure Active Directory Connect > AdPrep	~ č	Search AdPrep			Q
✓		Name	Date modified	Туре	Size		
E. Desktop	*	AdSyncPrep	5/25/2016 4:58 PM	Windows PowerS		34 KB	
👆 Downloads	A						
🗄 Documents	*						
Pictures	*						
> 💻 This PC							
> 🥔 Network							
4.2							
i item						8	

1. Provide your Azure AD global administrator credentials

PS C:>\$aadAdminCred = Get-Cree	dential									
PS C:\Users\Administrator> \$aadAdminCred = Get-Credential cmdlet Get-Credential at command pipeline position 1 Supply values for the following parameters:										
	cmdlet Get-Credentia	al at command pipe ?	×							
		G								
	Supply values for the	following parameters:								
	<u>U</u> ser name:	billmath@bmathcontoso.c	· ✓							
	Password:	•••••								
		ОК С	ancel							

1. Run the following PowerShell command

PS C:>Initialize-ADSyncDomainJoinedComputerSync	-AdConnectorAccount	[AD	connector	account	name]	-
AzureADCredentials <pre>\$aadAdminCred</pre>						

Where the [AD connector account name] is the name of the account you configured in Azure AD Connect when adding your on-premises AD DS directory.

The above commands enable Windows 10 clients to find the correct Azure AD domain to join by creating the serviceConnectionpoint object in AD DS.

#### Prepare AD for Device Write Back

To ensure AD DS objects and containers are in the correct state for write back of devices from Azure AD, do the following.

1. Open Windows PowerShell and execute the following:

PS C:>Initialize-ADSyncDeviceWriteBack -DomainName <AD DS domain name> -AdConnectorAccount [AD connector account name]

Where the [AD connector account name] is the name of the account you configured in Azure AD Connect when adding your on-premises AD DS directory in domain\accountname format

The above command creates the following objects for device write back to AD DS, if they do not exist already, and allows access to the specified AD connector account name

- RegisteredDevices container in the AD domain partition
- Device Registration Service container and object under Configuration --> Services --> Device Registration Configuration

#### Enable Device Write Back in Azure AD Connect

If you have not done so before, enable device write back in Azure AD Connect by running the wizard a second time and selecting **"Customize Synchronization Options"**, then checking the box for device write back and selecting the forest in which you have run the above cmdlets

### Configure AD FS to use Azure registered devices

#### Configure issuance of claims

In a federated Azure AD configuration, devices rely on Active Directory Federation Services (AD FS) or a 3rd party on-premises federation service to authenticate to Azure AD. Devices authenticate to get an access token to register against the Azure Active Directory Device Registration Service (Azure DRS).

Windows current devices authenticate using Integrated Windows Authentication to an active WS-Trust endpoint (either 1.3 or 2005 versions) hosted by the on-premises federation service.

#### NOTE

When using AD FS, either **adfs/services/trust/13/windowstransport** or **adfs/services/trust/2005/windowstransport** must be enabled. If you are using the Web Authentication Proxy, also ensure that this endpoint is published through the proxy. You can see what end-points are enabled through the AD FS management console under **Service > Endpoints**.

If you don't have AD FS as your on-premises federation service, follow the instructions of your vendor to make sure they support WS-Trust 1.3 or 2005 end-points and that these are published through the Metadata Exchange file (MEX).

The following claims must exist in the token received by Azure DRS for device registration to complete. Azure DRS will create a device object in Azure AD with some of this information which is then used by Azure AD Connect to associate the newly created device object with the computer account on-premises.

- http://schemas.microsoft.com/ws/2012/01/accounttype
- http://schemas.microsoft.com/identity/claims/onpremobjectguid
- http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid

If you have more than one verified domain name, you need to provide the following claim for computers:

http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid

If you are already issuing an ImmutableID claim (e.g., alternate login ID) you need to provide one corresponding claim for computers:

• http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID

In the following sections, you find information about:

- The values each claim should have
- How a definition would look like in AD FS

The definition helps you to verify whether the values are present or if you need to create them.

#### NOTE

If you don't use AD FS for your on-premises federation server, follow your vendor's instructions to create the appropriate configuration to issue these claims.

#### Issue account type claim

http://schemas.microsoft.com/ws/2012/01/accounttype - This claim must contain a value of **DJ**, which identifies the device as a domain-joined computer. In AD FS, you can add an issuance transform rule that looks like this:

```
@RuleName = "Issue account type for domain-joined computers"
c:[
   Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
   Value =~ "-515$",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(
   Type = "http://schemas.microsoft.com/ws/2012/01/accounttype",
   Value = "DJ"
);
```

#### Issue objectGUID of the computer account on-premises

http://schemas.microsoft.com/identity/claims/onpremobjectguid - This claim must contain the **objectGUID** value of the on-premises computer account. In AD FS, you can add an issuance transform rule that looks like this:

```
@RuleName = "Issue object GUID for domain-joined computers"
c1:[
   Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
   Value =~ "-515$",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
88
c2:[
   Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
1
=> issue(
   store = "Active Directory",
   types = ("http://schemas.microsoft.com/identity/claims/onpremobjectguid"),
   query = ";objectguid;{0}",
   param = c2.Value
);
```

#### Issue objectSID of the computer account on-premises

http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid - This claim must contain the the **objectSid** value of the on-premises computer account. In AD FS, you can add an issuance transform rule that looks like this:

```
@RuleName = "Issue objectSID for domain-joined computers"
c1:[
   Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
   Value =~ "-515$",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
&&&
c2:[
   Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(claim = c2);
```

#### Issue issuerID for computer when multiple verified domain names in Azure AD

http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid - This claim must contain the Uniform Resource Identifier (URI) of any of the verified domain names that connect with the on-premises federation service (AD FS or 3rd party) issuing the token. In AD FS, you can add issuance transform rules that look like the ones below in that specific order after the ones above. Please note that one rule to explicitly issue the rule for users is necessary. In the rules below, a first rule identifying user vs. computer authentication is added.

```
@RuleName = "Issue account type with the value User when its not a computer"
NOT EXISTS(
[
    Type == "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value == "DJ"
1
)
\Rightarrow add(
   Type = "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value = "User"
);
@RuleName = "Capture UPN when AccountType is User and issue the IssuerID"
c1:[
    Type == "http://schemas.xmlsoap.org/claims/UPN"
]
&&
c2:[
   Type == "http://schemas.microsoft.com/ws/2012/01/accounttype",
   Value == "User"
1
=> issue(
   Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid",
   Value = regexreplace(
   c1.Value,
    ".+@(?<domain>.+)",
   "http://${domain}/adfs/services/trust/"
    )
);
@RuleName = "Issue issuerID for domain-joined computers"
c:[
    Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
   Value =~ "-515$",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
1
=> issue(
    Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid",
    Value = "http://<verified-domain-name>/adfs/services/trust/"
);
```

- \$<domain> is the AD FS service URL
- <verified-domain-name> is a placeholder you need to replace with one of your verified domain names in Azure
  AD

For more details about verified domain names, see Add a custom domain name to Azure Active Directory. To get a list of your verified company domains, you can use the Get-MsolDomain cmdlet.

#### Issue ImmutableID for computer when one for users exist (e.g. alternate login ID is set)

http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID - This claim must contain a valid value for computers. In AD FS, you can create an issuance transform rule as follows:

```
@RuleName = "Issue ImmutableID for computers"
c1:[
    Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
   Value =~ "-515$",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
88
c2:[
    Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
1
=> issue(
    store = "Active Directory",
    types = ("http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"),
   query = ";objectguid;{0}",
   param = c2.Value
);
```

#### Helper script to create the AD FS issuance transform rules

The following script helps you with the creation of the issuance transform rules described above.

```
$multipleVerifiedDomainNames = $false
$immutableIDAlreadyIssuedforUsers = $false
$oneOfVerifiedDomainNames = 'example.com' # Replace example.com with one of your verified domains
$rule1 = '@RuleName = "Issue account type for domain-joined computers"
c:[
    Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
   Value =~ "-515$".
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
1
=> issue(
   Type = "http://schemas.microsoft.com/ws/2012/01/accounttype",
   Value = "DJ"
);'
$rule2 = '@RuleName = "Issue object GUID for domain-joined computers"
c1:[
    Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
   Value =~ "-515$",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
&&
c2:[
    Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
1
=> issue(
   store = "Active Directory",
   types = ("http://schemas.microsoft.com/identity/claims/onpremobjectguid"),
   query = ";objectguid;{0}",
    param = c2.Value
);'
```

```
$rule3 = '@RuleName = "Issue objectSID for domain-joined computers"
c1:[
   Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
   Value =~ "-515$",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
1
&&
c2:[
    Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid",
    Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
1
=> issue(claim = c2);'
$rule4 = ''
if ($multipleVerifiedDomainNames -eq $true) {
$rule4 = '@RuleName = "Issue account type with the value User when it is not a computer"
NOT EXISTS(
[
    Type == "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value == "DJ"
]
)
\Rightarrow add(
   Type = "http://schemas.microsoft.com/ws/2012/01/accounttype",
    Value = "User"
);
@RuleName = "Capture UPN when AccountType is User and issue the IssuerID"
c1:[
    Type == "http://schemas.xmlsoap.org/claims/UPN"
]
&&
c2:[
    Type == "http://schemas.microsoft.com/ws/2012/01/accounttype",
   Value == "User"
1
=> issue(
   Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid",
   Value = regexreplace(
   c1.Value.
    ".+@(?<domain>.+)",
    "http://${domain}/adfs/services/trust/"
    )
);
@RuleName = "Issue issuerID for domain-joined computers"
c:[
    Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
    Value =~ "-515$",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
1
=> issue(
   Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid",
    Value = "http://' + $oneOfVerifiedDomainNames + '/adfs/services/trust/"
);'
}
$rule5 = ''
if ($immutableIDAlreadyIssuedforUsers -eq $true) {
$rule5 = '@RuleName = "Issue ImmutableID for computers"
c1:[
    Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
   Value =~ "-515$",
   Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
&&
c2:[
   Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname".
```

```
Issuer =~ "^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$"
]
=> issue(
   store = "Active Directory",
   types = ("http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"),
   query = ";objectguid;{0}",
   param = c2.Value
);'
}
$existingRules = (Get-ADFSRelyingPartyTrust -Identifier
urn:federation:MicrosoftOnline).IssuanceTransformRules
$updatedRules = $existingRules + $rule1 + $rule2 + $rule3 + $rule4 + $rule5
$crSet = New-ADFSClaimRuleSet -ClaimRule $updatedRules
Set-AdfsRelyingPartyTrust -TargetIdentifier urn:federation:MicrosoftOnline -IssuanceTransformRules
$crSet.ClaimRulesString
```

#### Remarks

. . . .

- This script appends the rules to the existing rules. Do not run the script twice because the set of rules would be added twice. Make sure that no corresponding rules exist for these claims (under the corresponding conditions) before running the script again.
- If you have multiple verified domain names (as shown in the Azure AD portal or via the Get-MsolDomains cmdlet), set the value of **\$multipleVerifiedDomainNames** in the script to **\$true**. Also make sure that you remove any existing issuerid claim that might have been created by Azure AD Connect or via other means. Here is an example for this rule:

```
c:[Type == "http://schemas.xmlsoap.org/claims/UPN"]
=> issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid", Value =
regexreplace(c.Value, ".+@(?<domain>.+)", "http://${domain}/adfs/services/trust/"));
```

• If you have already issued an **ImmutableID** claim for user accounts, set the value of **\$immutableIDAlreadyIssuedforUsers** in the script to **\$true**.

#### **Configure Device Authentication in AD FS**

Using an elevated PowerShell command window, configure AD FS policy by executing the following command

PS C:>Set-AdfsGlobalAuthenticationPolicy -DeviceAuthenticationEnabled \$true -DeviceAuthenticationMethod All

#### Check your configuration

For your reference, below is a comprehensive list of the AD DS devices, containers and permissions required for device write-back and authentication to work

- object of type ms-DS-DeviceContainer at CN=RegisteredDevices,DC=<domain>
  - read access to the AD FS service account
  - read/write access to the Azure AD Connect sync AD connector account
- Container CN=Device Registration Configuration,CN=Services,CN=Configuration,DC=<domain>
- Container Device Registration Service DKM under the above container

2 ADSI Edit					3	_		×
File Action View Help								
🗢 🔿 🔀 📰 🗶 🗐 😡 🕞 🛛 🗊								
<ul> <li>Configuration [DC1.contoso.com]</li> </ul>	^	Name	Class	Disting	Actions			
CN=Configuration,DC=contoso,DC=com		CN=Device Registration Ser	container	CN=De	CN=Device Registration Co 🔺			
CN=DisplaySpecifiers		CN=Device Registration Ser	msDS-Devic	CN=De	More Actions			•
CN=Extended-Rights					NOTE /	ACCION 3		,
CN=ForestUpdates								
CN=Partitions								
CN=Physical Locations								
✓ CN=Services								
CN=AuthN Policy Configuration								
CN=Claims Configuration								
✓								
CN=Device Registration Service DKM								
CN=CryptoPolicy								
> CN=DeviceRegistrationService								
CN=Device Registration Services								
CN=Group Key Distribution Service								
CN=Mcrosoft SPP								
CN=NetServices								
CN-Public Key Services								
CN=RRAS								
CN=Shadow Principal Configuration								
CN=Windows NT								
CN-Sites	¥	<		>				

- object of type serviceConnectionpoint at CN=<guid>, CN=Device Registration Configuration,CN=Services,CN=Configuration,DC=<domain>
  - read/write access to the specified AD connector account name on the new object
- object of type msDS-DeviceRegistrationServiceContainer at CN=Device Registration Services,CN=Device Registration Configuration,CN=Services,CN=Configuration,DC=<domain>
- object of type msDS-DeviceRegistrationService in the above container

Configure Windows Hello for Business settings

# Follow the Windows Hello for Business hybrid certificate trust deployment guide

- 1. Overview
- 2. Prerequistes
- 3. New Installation Baseline
- 4. Configure Azure Device Registration (You are here)
- 5. Configure Windows Hello for Business settings
- 6. Sign-in and Provision

# Configure Windows Hello for Business

2/7/2018 • 1 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

You're environment is federated and you are ready to configure your hybrid environment for Windows Hello for business using the certificate trust model.

#### IMPORTANT

If your environment is not federated, review the New Installation baseline section of this deployment document to learn how to federate your environment for your Windows Hello for Business deployment.

The configuration for Windows Hello for Business is grouped in four categories. These categories are:

- Active Directory
- Public Key Infrastructure
- Active Directory Federation Services
- Group Policy

For the most efficent deployment, configure these technologies in order beginning with the Active Directory configuration

CONFIGURE ACTIVE DIRECTORY

Follow the Windows Hello for Business hybrid certificate trust deployment guide

- 1. Overview
- 2. Prerequistes
- 3. New Installation Baseline
- 4. Configure Azure Device Registration
- 5. Configure Windows Hello for Business settings (You are here)
- 6. Sign-in and Provision

# Hybrid Windows Hello for Business Provisioning

4/9/2018 • 3 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Hybrid deployments for Windows 10, version 1703 or higher.

# Provisioning

The Windows Hello for Business provisioning begins immediately after the user has signed in, after the user profile is loaded, but before the user receives their desktop. Windows only launches the provisioning experience if all the prerequisite checks pass. You can determine the status of the prerequisite checks by viewing the **User Device Registration** in the **Event Viewer** under **Applications and Services Logs\Microsoft\Windows**.



The first thing to validate is the computer has processed device registration. You can view this from the User device registration logs where the check **Device is AAD joined (AADJ or DJ++): Yes** appears. Additionally, you can validate this using the **dsregcmd /status** command from a console prompt where the value for **AzureADJoined** reads **Yes**.

Windows Hello for Business provisioning begins with a full screen page with the title **Setup a PIN** and button with the same name. The user clicks **Setup a PIN**.



The provisioning flow proceeds to the Multi-Factor authentication portion of the enrollment. Provisioning informs the user that it is actively attempting to contact the user through their configured form of MFA. The provisioning process does not proceed until authentication succeeds, fails or times out. A failed or timeout MFA results in an error and asks the user to retry.



After a successful MFA, the provisioning flow asks the user to create and validate a PIN. This PIN must observe any PIN complexity requirements that you deployed to the environment.

		•.	
Windows	Security		×
Set up	o a PIN		
Create a makes it	a PIN to use in place of t easier to sign in to yo	f passwords. Having a PIN our device, apps, and services.	
ų.	•••••		
	•••••		
	ОК	Cancel	1
		k	

The provisioning flow has all the information it needs to complete the Windows Hello for Business enrollment.

- A successful single factor authentication (username and password at sign-in)
- A device that has successfully completed device registration
- A fresh, successful multi-factor authentication
- A validated PIN that meets the PIN complexity requirements

The remainder of the provisioning includes Windows Hello for Business requesting an asymmetric key pair for the user, preferably from the TPM (or required if explicitly set through policy). Once the key pair is acquired, Windows communicates with Azure Active Directory to register the public key. AAD Connect syncrhonizes the user's key to the on-prem Active Directory.

#### **IMPORTANT**

The following is the enrollment behavior prior to Windows Server 2016 update KB4088889 (14393.2155).

The minimum time needed to synchronize the user's public key from Azure Active Directory to the on-premises Active Directory is 30 minutes. The Azure AD Connect scheduler controls the synchronization interval. **This synchronization latency delays the the user's ability to authenticate and use on-premises resouces until the user's public key has synchronized to Active Directory.** Once synchronized, the user can authenticate and use on-premises resources. Read Azure AD Connect sync: Scheduler to view and adjust the **synchronization cycle** for your organization.

#### NOTE

Windows Server 2016 update KB4088889 (14393.2155) provides synchronous certificate enrollment during hybrid certificate trust provisioning. With this update, users no longer need to wait for Azure AD Connect to sync their public key on-premises. Users enroll their certificate during provisioning and can use the certificate for sign-in immediately after completeling the provisioning.

After a successful key registration, Windows creates a certificate request using the same key pair to request a certificate. Windows send the certificate request to the AD FS server for certificate enrollment.

The AD FS registration authority verifies the key used in the certificate request matches the key that was previously registered. On a successful match, the AD FS registration authority signs the certificate request using its enrollment agent certificate and sends it to the certificate authority.

The certificate authority validates the certificate was signed by the registration authority. On successful validation of the signature, it issues a certificate based on the request and returns the certificate to the AD FS registration authority. The registration authority returns the certificate to Windows where it then installs the certificate in the current user's certificate store. Once this process completes, the Windows Hello for Business provisioning workflow informs the user they can use their PIN to sign-in through the Windows Action Center.

# Follow the Windows Hello for Business hybrid certificate trust deployment guide

- 1. Overview
- 2. Prerequistes
- 3. New Installation Baseline
- 4. Configure Azure Device Registration
- 5. Configure Windows Hello for Business policy settings
- 6. Sign-in and Provision(You are here)â€f

# On Premises Key Trust Deployment

2/7/2018 • 1 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

Windows Hello for Business replaces username and password sign-in to Windows with strong user authentication based on asymmetric key pair. The following deployment guide provides the information needed to successfully deploy Windows Hello for Business in an existing environment.

Below, you can find all the infromation you need to deploy Windows Hello for Business in a key trust model in your on-premises environment:

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings

# Validate Active Directory prerequisites

2/7/2018 • 1 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

Key trust deployments need an adequate number of 2016 domain controllers to ensure successful user authentication with Windows Hello for Business. To learn more about domain controller planning for key trust deployments, read the Windows Hello for Business planning guide, the Planning an adequate number of Windows Server 2016 Domain Controllers for Windows Hello for Business deployments section.

The key registration process for the On-prem deployment of Windows Hello for Business needs the Windows Server 2016 Active Directory schema. The key-trust model receives the schema extension when the first Windows Server 2016 domain controller is added to the forest. The minimum required domain functional and forest functional levels for Windows Hello for Business deployment is Windows Server 2008 R2.

# Create the Windows Hello for Business Users Security Global Group

The Windows Hello for Business Users group is used to make it easy to deploy Windows Hello for Business in phases. You assign Group Policy permissions to this group to simplify the deployment by simply adding the users to the group. This provides users with the proper permissions to provision Windows Hello for Business.

Sign-in a domain controller or management workstation with Domain Admin equivalent credentials.

- 1. Open Active Directory Users and Computers.
- 2. Click View and click Advanced Features.
- 3. Expand the domain node from the navigation pane.
- 4. Right-click the Users container. Click New. Click Group.
- 5. Type Windows Hello for Business Users in the Group Name text box.
- 6. Click **OK**.

# Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites (You are here)
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings

# Validate and Configure Public Key Infrastructure

2/7/2018 • 12 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

Windows Hello for Business must have a public key infrastructure regardless of the deployment or trust model. All trust models depend on the domain controllers having a certificate. The certificate serves as a root of trust for clients to ensure they are not communicating with a rogue domain controller.

# Deploy an enterprise certificate authority

This guide assumes most enterprise have an existing public key infrastructure. Windows Hello for Business depends on a Windows enterprise public key infrastructure running the Active Directory Certificate Services role from Windows Server 2012 or later.

#### Lab-based public key infrastructure

The following instructions may be used to deploy simple public key infrastructure that is suitable for a lab environment.

Sign-in using *Enterprise Admin* equivalent credentials on Windows Server 2012 or later server where you want the certificate authority installed.

#### NOTE

Never install a certificate authority on a domain controller in a production environment.

- 1. Open an elevated Windows PowerShell prompt.
- 2. Use the following command to install the Active Directory Certificate Services role.

```
Add-WindowsFeature Adcs-Cert-Authority -IncludeManagementTools
```

3. Use the following command to configure the Certificate Authority using a basic certificate authority configuration.

Install-AdcsCertificationAuthority

### Configure a Production Public Key Infrastructure

If you do have an existing public key infrastructure, please review Certification Authority Guidance from Microsoft TechNet to properly design your infrastructure. Then, consult the Test Lab Guide: Deploying an AD CS Two-Tier PKI Hierarchy for instructions on how to configure your public key infrastructure using the information from your design session.

#### **Configure Domain Controller Certificates**

Clients need to trust domain controllers and the best way to do this is to ensure each domain controller has a Kerberos Authentication certificate. Installing a certificate on the domain controller enables the Key Distribution Center (KDC) to prove its identity to other members of the domain. This provides clients a root of trust external to the domain—namely the enterprise certificate authority.

Domain controllers automatically request a domain controller certificate (if published) when they discover an enterprise certificate authority is added to Active Directory. However, certificates based on the Domain Controller and Domain Controller Authentication certificate templates do not include the KDC Authentication object identifier (OID), which was later added to the Kerberos RFC. Therefore, domain controllers need to request a certificate based on the Kerberos Authentication certificate template.

By default, the Active Directory Certificate Authority provides and publishes the Kerberos Authentication certificate template. However, the cryptography configuration included in the provided template is based on older and less performant cryptography APIs. To ensure domain controllers request the proper certificate with the best available cryptography, use the Kerberos Authentication certificate template as a baseline to create an updated domain controller certificate template.

Sign-in to a certificate authority or management workstations with Domain Admin equivalent credentials.

- 1. Open the **Certificate Authority** management console.
- 2. Right-click **Certificate Templates** and click **Manage**.
- 3. In the **Certificate Template Console**, right-click the **Kerberos Authentication** template in the details pane and click **Duplicate Template**.
- 4. On the Compatibility tab, clear the Show resulting changes check box. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Authority list. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Recipient list.
- On the General tab, type Domain Controller Authentication (Kerberos) in Template display name. Adjust the validity and renewal period to meet your enterprise's needs. Notelf you use different template names, you'll need to remember and substitute these names in different portions of the lab.
- 6. On the **Subject** tab, select the **Build from this Active Directory information** button if it is not already selected. Select **None** from the **Subject name format** list. Select **DNS name** from the **Include this information in alternate subject** list. Clear all other items.
- 7. On the **Cryptography** tab, select **Key Storage Provider** from the **Provider Category** list. Select **RSA** from the **Algorithm name** list. Type **2048** in the **Minimum key size** text box. Select **SHA256** from the **Request hash** list. Click **OK**.
- 8. Close the console.

#### Superseding the existing Domain Controller certificate

Many domain controllers may have an existing domain controller certificate. The Active Directory Certificate Services provides a default certificate template from domain controllers—the domain controller certificate template. Later releases provided a new certificate template—the domain controller authentication certificate template. These certificate templates were provided prior to update of the Kerberos specification that stated Key Distribution Centers (KDCs) performing certificate authentication needed to include the KDC Authentication extension.

The Kerberos Authentication certificate template is the most current certificate template designated for domain controllers and should be the one you deploy to all your domain controllers (2008 or later). The autoenrollment feature in Windows enables you to effortlessly replace these domain controller certificates. You can use the following configuration to replace older domain controller certificates with a new certificate using the Kerberos Authentication certificate template.

Sign-in to a certificate authority or management workstations with Enterprise Admin equivalent credentials.

- 1. Open the Certificate Authority management console.
- 2. Right-click Certificate Templates and click Manage.
- In the Certificate Template Console, right-click the Domain Controller Authentication (Kerberos) (or the name of the certificate template you created in the previous section) template in the details pane and click Properties.
- 4. Click the Superseded Templates tab. Click Add.
- 5. From the **Add Superseded Template** dialog, select the **Domain Controller** certificate template and click **OK**. Click **Add**.
- 6. From the **Add Superseded Template** dialog, select the **Domain Controller Authentication** certificate template and click **OK**.
- 7. From the Add Superseded Template dialog, select the Kerberos Authentication certificate template and click OK.
- 8. Add any other enterprise certificate templates that were previously configured for domain controllers to the **Superseded Templates** tab.
- 9. Click OK and close the Certificate Templates console.

The certificate template is configured to supersede all the certificate templates provided in the certificate templates superseded templates list. However, the certificate template and the superseding of certificate templates is not active until you publish the certificate template to one or more certificate authorities.

#### Configure an Internal Web Server Certificate template

Windows 10 clients use the https protocol when communicating with Active Directory Federation Services. To meet this need, you must issue a server authentication certificate to all the nodes in the Active Directory Federation Services farm. On-premises deployments can use a server authentication certificate issued by their enterprise PKI. You must configure a server authentication certificate template so the host running the Active Directory Federation Service can request the certificate.

Sign-in to a certificate authority or management workstations with Domain Admin equivalent credentials.

- 1. Open the Certificate Authority management console.
- 2. Right-click Certificate Templates and click Manage.
- 3. In the **Certificate Template Console**, right-click the **Web Server** template in the details pane and click **Duplicate Template**.
- 4. On the Compatibility tab, clear the Show resulting changes check box. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Authority list. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Recipient list.
- 5. On the **General** tab, type **Internal Web Server** in **Template display name**. Adjust the validity and renewal period to meet your enterprise's needs.

**Note:** If you use different template names, you'll need to remember and substitute these names in different portions of the lab.

- 6. On the Request Handling tab, select Allow private key to be exported.
- 7. On the **Subject** tab, select the **Supply in the request** button if it is not already selected.
- 8. On the **Security** tab, Click **Add**. Type **Domain Computers** in the **Enter the object names to select** box. Click **OK**. Select the **Allow** check box next to the **Enroll** permission.
- 9. On the **Cryptography** tab, select **Key Storage Provider** from the **Provider Category** list. Select **RSA** from the **Algorithm name** list. Type **2048** in the **Minimum key size** text box. Select **SHA256** from the **Request hash** list. Click **OK**.
- 10. Close the console.

#### **Unpublish Superseded Certificate Templates**

The certificate authority only issues certificates based on published certificate templates. For defense in depth security, it is a good practice to unpublish certificate templates that the certificate authority is not configured to

issue. This includes the pre-published certificate template from the role installation and any superseded certificate templates.

The newly created domain controller authentication certificate template supersedes previous domain controller certificate templates. Therefore, you need to unpublish these certificate templates from all issuing certificate authorities.

Sign-in to the certificate authority or management workstation with *Enterprise Admin* equivalent credentials.

- 1. Open the **Certificate Authority** management console.
- 2. Expand the parent node from the navigation pane.
- 3. Click **Certificate Templates** in the navigation pane.
- 4. Right-click the **Domain Controller** certificate template in the content pane and select **Delete**. Click **Yes** on the **Disable certificate templates** window.
- 5. Repeat step 4 for the **Domain Controller Authentication** and **Kerberos Authentication** certificate templates.

#### Publish Certificate Templates to the Certificate Authority

The certificate authority may only issue certificates for certificate templates that are published to that certificate authority. If you have more than one certificate authority and you want that certificate authority to issue certificates based on a specific certificate template, then you must publish the certificate template to all certificate authorities that are expected to issue the certificate.

Sign-in to the certificate authority or management workstations with an Enterprise Admin equivalent credentials.

- 1. Open the **Certificate Authority** management console.
- 2. Expand the parent node from the navigation pane.
- 3. Click **Certificate Templates** in the navigation pane.
- 4. Right-click the Certificate Templates node. Click New, and click Certificate Template to issue.
- 5. In the **Enable Certificates Templates** window, select the **Domain Controller Authentication (Kerberos)**, and **Internal Web Server** templates you created in the previous steps. Click **OK** to publish the selected certificate templates to the certificate authority.
- 6. If you published the Domain Controller Authentication (Kerberos) certificate template, then you should unpublish the certificate templates you included in the superseded templates list.
  - To unpublish a certificate template, right-click the certificate template you want to unpublish in the details pane of the Certificate Authority console and select **Delete**. Click **Yes** to confirm the operation.
- 7. Close the console.

#### **Configure Domain Controllers for Automatic Certificate Enrollment**

Domain controllers automatically request a certificate from the domain controller certificate template. However, the domain controller is unaware of newer certificate templates or superseded configurations on certificate templates. To continue automatic enrollment and renewal of domain controller certificates that understand newer certificate template and superseded certificate template configurations, create and configure a Group Policy object for automatic certificate enrollment and link the Group Policy object to the Domain Controllers OU.

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. Expand the domain and select the Group Policy Object node in the navigation pane.
- 3. Right-click Group Policy object and select New
- 4. Type Domain Controller Auto Certificate Enrollment in the name box and click **OK**.
- 5. Right-click the **Domain Controller Auto Certificate Enrollment** Group Policy object and click **Edit**.
- 6. In the navigation pane, expand **Policies** under **Computer Configuration**.
- 7. Expand Windows Settings, Security Settings, and click Public Key Policies.

- 8. In the details pane, right-click Certificate Services Client Auto-Enrollment and select Properties.
- 9. Select Enabled from the Configuration Model list.
- 10. Select the **Renew expired certificates**, **update pending certificates**, and **remove revoked certificates** check box.
- 11. Select the Update certificates that use certificate templates check box.
- 12. Click OK. Close the Group Policy Management Editor.

#### Deploy the Domain Controller Auto Certificate Enrollment Group Policy Object

Sign-in to a domain controller or management workstations with Domain Admin equivalent credentials.

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. In the navigation pane, expand the domain and expand the node that has your Active Directory domain name. Right-click the **Domain Controllers** organizational unit and click **Link an existing GPO...**
- 3. In the **Select GPO** dialog box, select **Domain Controller Auto Certificate Enrollment** or the name of the domain controller certificate enrollment Group Policy object you previously created and click **OK**.

#### Validating your work

Windows Hello for Business is a distributed system, which on the surface appears complex and difficult. The key to a successful Windows Hello for Business deployment is to validate phases of work prior to moving to the next phase.

You want to confirm your domain controllers enroll the correct certificates and not any unnecessary (superseded) certificate templates. You need to check each domain controller that autoenrollment for the computer occurred.

#### Use the Event Logs

Windows Server 2012 and later include Certificate Lifecycle events to determine the lifecycles of certificates for both users and computers. Using the Event Viewer, navigate to the CertificateServices-Lifecycles-System event log under Application and Services/Microsoft/Windows.

Look for an event indicating a new certificate enrollment (autoenrollment). The details of the event include the certificate template on which the certificate was issued. The name of the certificate template used to issue the certificate should match the certificate template name included in the event. The certificate thumbprint and EKUs for the certificate are also included in the event. The EKU needed for proper Windows Hello for Business authentication is Kerberos Authentication, in addition to other EKUs provide by the certificate template.

Certificates superseded by your new domain controller certificate generate an archive event in the CertificateServices-Lifecycles-System event. The archive event contains the certificate template name and thumbprint of the certificate that was superseded by the new certificate.

#### **Certificate Manager**

You can use the Certificate Manager console to validate the domain controller has the properly enrolled certificate based on the correct certificate template with the proper EKUs. Use **certIm.msc** to view certificate in the local computers certificate stores. Expand the **Personal** store and view the certificates enrolled for the computer. Archived certificates do not appear in Certificate Manager.

#### Certutil.exe

You can use **certutil.exe** to view enrolled certificates in the local computer. Certutil shows enrolled and archived certificates for the local computer. From an elevated command prompt, run <u>certutil -q -store my</u> to view locally enrolled certificates.

To view detailed information about each certificate in the store, use certutil -q -v -store my to validate automatic certificate enrollment enrolled the proper certificates.

#### Troubleshooting

Windows triggers automatic certificate enrollment for the computer during boot, and when Group Policy updates. You can refresh Group Policy from an elevated command prompt using gpupdate /force. Alternatively, you can forcefully trigger automatic certificate enrollment using certreq -autoenroll -q from an elevated command prompt.

Use the event logs to monitor certificate enrollment and archive. Review the configuration, such as publishing certificate templates to issuing certificate authority and the allow auto enrollment permissions.

# Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure (You are here)
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings

# Prepare and Deploy Windows Server 2016 Active Directory Federation Services

4/9/2018 • 19 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

Windows Hello for Business works exclusively with the Active Directory Federation Service role included with Windows Server 2016 and requires an additional server update. The on-prem key trust deployment uses Active Directory Federation Services roles for key registration and device registration.

The following guidance describes deploying a new instance of Active Directory Federation Services 2016 using the Windows Information Database as the configuration database, which is ideal for environments with no more than 30 federation servers and no more than 100 relying party trusts.

If your environment exceeds either of these factors or needs to provide SAML artifact resolution, token replay detection, or needs Active Directory Federation Services to operate in a federated provider role, then your deployment needs to use a SQL for your configuration database. To deploy the Active Directory Federation Services using SQL as its configuration database, please review the Deploying a Federation Server Farm checklist.

If your environment has an existing instance of Active Directory Federation Services, then you'll need to upgrade all nodes in the farm to Windows Server 2016 along with the Windows Server 2016 update. If your environment uses Windows Internal Database (WID) for the configuration database, please read Upgrading to AD FS in Windows Server 2016 using a WID database to upgrade your environment. If your environment uses SQL for the configuration database, please read Upgrading to AD FS in windows Server 2016 using a WID database to AD FS in Windows Server 2016 with SQL Server to upgrade your environment.

Ensure you apply the Windows Server 2016 Update to all nodes in the farm after you have successfully completed the upgrade.

A new Active Directory Federation Services farm should have a minimum of two federation servers for proper load balancing, which can be accomplished with an external networking peripherals, or with using the Network Load Balancing Role included in Windows Server.

Prepare the Active Directory Federation Services deployment by installing and updating two Windows Server 2016 Servers. Ensure the update listed below is applied to each server before continuing.

## Update Windows Server 2016

Sign-in the federation server with *local admin* equivalent credentials.

- Ensure Windows Server 2016 is current by running Windows Update from Settings. Continue this process until no further updates are needed. If you're not using Windows Update for updates, please review the Windows Server 2016 update history page to make sure you have the latest updates available installed.
- 2. Ensure the latest server updates to the federation server includes KB4088889 (14393.2155).

#### IMPORTANT

The above referenced updates are mandatory for Windows Hello for Business all on-premises deployment and hybrid certificate trust deployments for domain joined computers.

### Enroll for a TLS Server Authentication Certificate

Key trust Windows Hello for Business on-premises deployments need a federation server for device registration and key registration. Typically, a federation service is an edge facing role. However, the federation services and instance used with the on-premises deployment of Windows Hello for Business does not need Internet connectivity.

The AD FS role needs a server authentication certificate for the federation services, but you can use a certificate issued by your enterprise (internal) certificate authority. The server authentication certificate should have the following names included in the certificate if you are requesting an individual certificate for each node in the federation farm:

- Subject Name: The internal FQDN of the federation server (the name of the computer running AD FS)
- Subject Alternate Name: Your federation service name, such as *fs.corp.contoso.com* (or an appropriate wildcard entry such as \*.corp.contoso.com)

You configure your federation service name when you configure the AD FS role. You can choose any name, but that name must be different than the name of the server or host. For example, you can name the host server **adfs** and the federation service **fs**. The FQDN of the host is adfs.corp.contoso.com and the FQDN of the federation service is fs.corp.contoso.com.

You can, however, issue one certificate for all hosts in the farm. If you chose this option, then leave the subject name blank, and include all the names in the subject alternate name when creating the certificate request. All names should include the FQDN of each host in the farm and the federation service name.

When creating a wildcard certificate, it is recommended that you mark the private key as exportable so that the same certificate can be deployed across each federation server and web application proxy within your AD FS farm. Note that the certificate must be trusted (chain to a trusted root CA). Once you have successfully requested and enrolled the server authentication certificate on one node, you can export the certificate and private key to a PFX file using the Certificate Manager console. You can then import the certificate on the remaining nodes in the AD FS farm.

Be sure to enroll or import the certificate into the AD FS server's computer certificate store. Also, ensure all nodes in the farm have the proper TLS server authentication certificate.

#### Internal Server Authentication Certificate Enrollment

Sign-in the federation server with domain admin equivalent credentials.

- 1. Start the Local Computer Certificate Manager (certlm.msc).
- 2. Expand the **Personal** node in the navigation pane.
- 3. Right-click Personal. Select All Tasks and Request New Certificate.
- 4. Click Next on the Before You Begin page.
- 5. Click Next on the Select Certificate Enrollment Policy page.
- 6. On the Request Certificates page, Select the Internal Web Server check box.
- 7. Click the More information is required to enroll for this certificate. Click here to configure settings link

I		certlm - [Certifi	cates - Local Con	nputer\Personal\Ce	rtificates]			
Rec	cycle Bin	File Action Vie	i la 🔜	?				
		Certificates - Lo	cal Computer	Issued To	^	Issued By	Ex	
		<ul> <li>Personal</li> <li>Certificat</li> </ul>	ec.	🙀 fed.corp.mste	pdemo.net	corp-CA-CA	12	
			Certificate Prop	erties			×	
	🔄 Certificate Enrollment		🔥 Subject G	eneral Extensions	Private Key Certi	fication Authority Signature		
	Request Certificates		The subject of can enter info can be used in	a certificate is the u rmation about the t a certificate.	user or computer t ypes of subject na	o which the certificate is iss me and alternative name va	ued. You Ilues that	
	You can request the following type click Enroll.	es of certificates. Sele	Subject of cert The user or co	tificate mputer that is recei	ving the certificat	2		100
	Active Directory Enrollment Po	olicy	Type:					
	Computer	🤹 ST	Common na	me 🗸	Add >			
	🗹 Internal Web Server	sı) sı	Value:		< Remove			
	A More information is re-	quired to enroll for th	adfs.corp.co	ntoso.com		-		Contraction of the
			Alternative na	me:				
			Туре:					
			DNS	~				
			fs corp cont	oso com	Add >			A STATE
	Show all templates		iscorp.com	oso.com	< Remove			
B								
						OK Cancel	Apply	
		1						
	، باللكور	×	>				>	ows Server 2016 Datacenter
							_	ease_inmarket.161208-2252 6:11 AM
	, P 🗆 🧲 📒			<b>a</b>			E E	1/27/2017

- 8. Under Subject name, select Common Name from the Type list. Type the FQDN of the computer hosting the Active Directory Federation Services role and then click Add. Under Alternative name, select DNS from the Type list. Type the FQDN of the name you will use for your federation services (fs.corp.contoso.com). The name you use here MUST match the name you use when configuring the Active Directory Federation Services server role. Click Add. Click OK when finished.
- 9. Click Enroll.

A server authentication certificate should appear in the computer's Personal certificate store.

## Deploy the Active Directory Federation Service Role

The Active Directory Federation Service (AD FS) role provides the following services to support Windows Hello for Business on-premises deployments.

- Device registration
- Key registration

#### IMPORTANT

Finish the entire AD FS configuration on the first server in the farm before adding the second server to the AD FS farm. Once complete, the second server receives the configuration through the shared configuration database when it is added the AD FS farm.

Windows Hello for Business depends on proper device registration. For on-premises key trust deployments, Windows Server 2016 AD FS handles device and key registration.

Sign-in the federation server with *Enterprise Admin* equivalent credentials.

- 1. Start Server Manager. Click Local Server in the navigation pane.
- 2. Click Manage and then click Add Roles and Features.
- 3. Click Next on the Before you begin page.
- 4. On the Select installation type page, select Role-based or feature-based installation and click Next.
- 5. On the **Select destination server** page, choose **Select a server from the server pool**. Select the federation server from the **Server Pool** list. Click **Next**.
- 6. On the Select server roles page, select Active Directory Federation Services. Click Next.
- 7. Click Next on the Select features page.
- 8. Click Next on the Active Directory Federation Service page.
- 9. Click **Install** to start the role installation.

### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm the AD FS farm uses the correct database configuration.
- Confirm the AD FS farm has an adequate number of nodes and is properly load balanced for the anticipated load.
- Confirm **all** AD FS servers in the farm have the latest updates.
- Confirm all AD FS servers have a valid server authentication certificate
  - The subject of the certificate is the common name (FQDN) of the host or a wildcard name.
  - The alternate name of the certificate contains a wildcard or the FQDN of the federation service

# Device Registration Service Account Prerequisite

The service account used for the device registration server depends on the domain controllers in the environment.

#### NOTE

Follow the procedures below based on the domain controllers deployed in your environment. If the domain controller is not listed below, then it is not supported for Windows Hello for Business.

#### Windows Server 2012 or later Domain Controllers

Windows Server 2012 or later domain controllers support Group Managed Service Accounts—the preferred way to deploy service accounts for services that support them. Group Managed Service Accounts, or GMSA have security advantages over normal user accounts because Windows handles password management. This means the password is long, complex, and changes periodically. The best part of GMSA is all this happens automatically. AD FS supports GMSA and should be configured using them for additional defense in depth security.

GSMA uses the Microsoft Key Distribution Service that is located on Windows Server 2012 or later domain controllers. Windows uses the Microsoft Key Distribution Service to protect secrets stored and used by the GSMA. Before you can create a GSMA, you must first create a root key for the service. You can skip this if your environment already uses GSMA.

#### Create KDS Root Key

Sign-in a domain controller with Enterprise Admin equivalent credentials.

- 1. Start an elevated Windows PowerShell console.
- 2. Type Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)

#### Windows Server 2008 or 2008 R2 Domain Controllers

Windows Server 2008 and 2008 R2 domain controllers do not host the Microsoft Key Distribution Service, nor do they support Group Managed Service Accounts. Therefore, you must use create a normal user account as a service account where you are responsible for changing the password on a regular basis.

#### **Create an AD FS Service Account**

Sign-in a domain controller or management workstation with Domain Admin equivalent credentials.

- 1. Open Active Directory Users and Computers.
- 2. Right-click the Users container, Click New. Click User.
- 3. In the **New Object User** window, type **adfssvc** in the **Full name** text box. Type **adfssvc** in the **User logon name** text box. Click **Next**.
- 4. Enter and confirm a password for the **adfssvc** user. Clear the **User must change password at next logon** checkbox.
- 5. Click **Next** and then click **Finish**.

# Configure the Active Directory Federation Service Role

#### IMPORTANT

Follow the procedures below based on the domain controllers deployed in your environment. If the domain controller is not listed below, then it is not supported for Windows Hello for Business.

#### Windows Server 2016, 2012 R2 or later Domain Controllers

Use the following procedures to configure AD FS when your environment uses **Windows Server 2012 or later Domain Controllers**. If you are not using Windows Server 2012 or later Domain Controllers, follow the procedures under the Configure the Active Directory Federation Service Role (Windows Server 2008 or 2008R2 Domain Controllers) section.

Sign-in the federation server with *Domain Admin* equivalent credentials. These procedures assume you are configuring the first federation server in a federation server farm.

#### 1. Start Server Manager.

2. Click the notification flag in the upper right corner. Click **Configure federation services on this server**.

Dashboard	For adfs		Post-deployment Co	ontigura	TASKS 👻 X		TASKS 💌
Local Server All Servers	Computer name Domain	adfs corp	Configuration requin Federation Services a Configure the federa	red for Active I at ADFS ation service o	Directory n this server.		Never Download updates o
AD FS File and Storage Services		0	Feature installation			ites	loday at 6:46 AM
	Windows Firewall Remote management Remote Desktop	Dom Enab Disal	Configuration requir adfs.corp.mstepdem Add Roles and Featu	ed. Installation io.net. ires	n succeeded on	ics Configuration	Real-Time Protection Settings On
	NIC Teaming Ethernet	Disal 10.0.	Task Details				(UTC-08:00) Pacific T Not activated
	Operating system version Hardware information	Microsoft Microsoft	it Windows Server 2016 [ it Corporation Virtual Ma	Datacenter achine	Processors Installed memory (R Total disk space	RAM)	Intel(R) Xeon(R) CPU 1.43 GB 40 GB
	Operating system version Hardware information	Microsoft Microsoft	't Windows Server 2016 [ 't Corporation Virtual Ma	Datacenter achine	Processors Installed memory (R Total disk space	RAM)	Intel(R) Xeon(R) CPU 1.43 GB 40 GB
	Operating system version Hardware information	Microsoft Microsoft	't Windows Server 2016 [ 't Corporation Virtual Ma	Datacenter achine	Processors Installed memory (R Total disk space	(AM)	Intel(R) Xeon(R) CPU 1.43 GB 40 GB TASKS ▼
	Operating system version Hardware information	Microsoft Microsoft	it Windows Server 2016 I it Corporation Virtual Ma (iii) • (R) •	Datacenter achine	Processors Installed memory (R Total disk space	RAM)	Intel(R) Xeon(R) CPU 1.43 GB 40 GB TASKS ▼
	Operating system version Hardware information	Microsoft Microsoft y Source	it Windows Server 2016 [ t Corporation Virtual Ma (III)	Datacenter schine	Processors Installed memory (R Total disk space	<b>L</b> (AM)	Intel(R) Xeon(R) CPU 1.43 GB 40 GB TASKS •
	Operating system version Hardware information <b>EVENTS</b> All events   16 total <i>Filter</i> Server Name ID Severi ADFS 642 Warning	Microsoft Microsoft y Source g ESENT	it Windows Server 2016 I it Corporation Virtual Ma (ii) • (iii) • (iii) •	Datacenter achine Log Application	Processors Installed memory (R Total disk space	AM)	Intel(R) Xeon(R) CPU 1.43 GB 40 GB TASKS O dows

- 3. On the Welcome page, click Create the first federation server farm and click Next.
- 4. Click Next on the Connect to Active Directory Domain Services page.
- On the Specify Service Properties page, select the recently enrolled or imported certificate from the SSL Certificate list. The certificate is likely named after your federation service, such as *fs.corp.contoso.com* or *fs.contoso.com*.
- 6. Select the federation service name from the Federation Service Name list.
- 7. Type the Federation Service Display Name in the text box. This is the name users see when signing in. Click **Next**.
- 8. On the **Specify Service Account** page, select **Create a Group Managed Service Account**. In the **Account Name** box, type **adfssvc**.
- 9. On the Specify Configuration Database page, select Create a database on this server using Windows Internal Database and click Next.
- 10. On the Review Options page, click Next.
- 11. On the Pre-requisite Checks page, click Configure.
- 12. When the process completes, click **Close**.

#### Windows Server 2008 or 2008 R2 Domain Controllers

Use the following procedures to configure AD FS when your environment uses **Windows Server 2008 or 2008 R2 Domain Controllers**. If you are not using Windows Server 2008 or 2008 R2 Domain Controllers, follow the procedures under the Configure the Active Directory Federation Service Role (Windows Server 2012 or later Domain Controllers) section.

Sign-in the federation server with *Domain Admin* equivalent credentials. These instructions assume you are configuring the first federation server in a federation server farm.

#### 1. Start Server Manager.

2. Click the notification flag in the upper right corner. Click **Configure federation services on this server**.



3. On the **Welcome** page, click **Create the first federation server farm** and click **Next**.

- 4. Click Next on the Connect to Active Directory Domain Services page.
- On the Specify Service Properties page, select the recently enrolled or imported certificate from the SSL Certificate list. The certificate is likely named after your federation service, such as fs.corp.mstepdemo.net or fs.mstepdemo.net.
- 6. Select the federation service name from the Federation Service Name list.
- 7. Type the Federation Service Display Name in the text box. This is the name users see when signing in. Click **Next**.
- 8. On the Specify Service Account page, Select Use an existing domain user account or group Managed Service Account and click Select.
  - In the **Select User or Service Account** dialog box, type the name of the previously created AD FS service account (example adfssvc) and click **OK**. Type the password for the AD FS service account and click **Next**.
- 9. On the Specify Configuration Database page, select Create a database on this server using Windows Internal Database and click Next.
- 10. On the Review Options page, click Next.
- 11. On the Pre-requisite Checks page, click Configure.
- 12. When the process completes, click **Close**.
- 13. Do not restart the AD FS server. You will do this later.

#### Add the AD FS Service account to the KeyAdmins group

The KeyAdmins global group provides the AD FS service with the permissions needed to perform key registration.

Sign-in a domain controller or management workstation with Domain Admin equivalent credentials.

- 1. Open Active Directory Users and Computers.
- 2. Click the Users container in the navigation pane.
- 3. Right-click KeyAdmins in the details pane and click Properties.
- 4. Click the Members tab and click Add...
- 5. In the Enter the object names to select text box, type adfssvc. Click OK.
- 6. Click OK to return to Active Directory Users and Computers.
- 7. Click OK to return to Active Directory Users and Computers.
- 8. Change to server hosting the AD FS role and restart it.

# Configure the Device Registration Service

Sign-in the federation server with *Enterprise Admin* equivalent credentials. These instructions assume you are configuring the first federation server in a federation server farm.

- 1. Open the AD FS management console.
- 2. In the navigation pane, expand **Service**. Click **Device Registration**.
- 3. In the details pane, click **Configure Device Registration**.
- 4. In the Configure Device Registration dialog, click OK.

### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm you followed the correct procedures based on the domain controllers used in your deployment
  - Windows Server 2016, 2012 R2 or Windows Server 2012 R2
  - Windows Server 2008 or Windows Server 2008 R2
- Confirm you have the correct service account based on your domain controller version.
- Confirm you properly installed the AD FS role on your Windows Server 2016 based on the proper sizing of

your federation, the number of relying parties, and database needs.

- Confirm you used a certificate with the correct names as the server authentication certificate
  - Record the expiration date of the certificate and set a renewal reminder at least six weeks before it expires that includes the:
    - Certificate serial number
    - Certificate thumbprint
    - Common name of the certificate
    - Subject alternate name of the certificate
    - Name of the physical host server
    - The issued date
    - The expiration date
    - Issuing CA Vendor (if a third-party certificate)
- Confirm you added the AD FS service account to the KeyAdmins group.
- Confirm you enabled the Device Registration service.

# Additional Federation Servers

Organizations should deploy more than one federation server in their federation farm for high-availability. You should have a minimum of two federation services in your AD FS farm, however most organizations are likely to have more. This largely depends on the number of devices and users using the services provided by the AD FS farm.

#### Server Authentication Certificate

Each server you add to the AD FS farm must have a proper server authentication certificate. Refer to the Enroll for a TLS Server Authentication Certificate section of this document to determine the requirements for your server authentication certificate. As previously stated, AD FS servers used exclusively for on-premises deployments of Windows Hello for Business can use enterprise server authentication certificates rather than server authentication certificates issued by public certificate authorities.

#### Install Additional Servers

Adding federation servers to the existing AD FS farm begins with ensuring the server are fully patched, to include Windows Server 2016 Update needed to support Windows Hello for Business deployments (https://aka.ms/whfbadfs1703). Next, install the Active Directory Federation Service role on the additional servers and then configure the server as an additional server in an existing farm.

# Load Balance AD FS Federation Servers

Many environments load balance using hardware devices. Environments without hardware load-balancing capabilities can take advantage the network load-balancing feature included in Windows Server to load balance the AD FS servers in the federation farm. Install the Windows Network Load Balancing feature on all nodes participating in the AD FS farm that should be load balanced.

#### Install Network Load Balancing Feature on AD FS Servers

Sign-in the federation server with Enterprise Admin equivalent credentials.

- 1. Start Server Manager. Click Local Server in the navigation pane.
- 2. Click Manage and then click Add Roles and Features.
- 3. Click Next On the Before you begin page.
- 4. On the Select installation type page, select Role-based or feature-based installation and click Next.
- 5. On the **Select destination server** page, chose **Select a server from the server pool**. Select the federation server from the **Server Pool** list. Click **Next**.

- 6. On the **Select server roles** page, click **Next**.
- 7. Select Network Load Balancing on the Select features page.
- 8. Click Install to start the feature installation

Dashboard	For adfs	5	TAS	KS 💌
Local Server All Servers AD FS	Add Roles and Features Wizard	и	X	AM Ites o
File and Storage Se	Select features Before You Begin	Select one or more features to install on the selected server.	DESTINATION SERVER adfs.corp.contoso.com	ction
	Installation Type Server Selection Server Roles Features	Features  LPR Port Monitor Management OData IIS Extension Media Foundation Media Foundation	Description Network Load Balancing (NLB) distributes traffic across several servers, using the TCP/IP networking protocol. NLB is particularly useful	ific Ti
	Confirmation Results	Multipath I/O     Multipath I/O     MultiPoint Connector     MultiPoint Connector     Peer Name Resolution Protocol     Quality Windows Audio Video Experience     RAS Connection Manager Administration Kit (CMA     Remote Assistance     Remote Differential Compression     Multipath Remote Assistance	for ensuring that stateless applications, such as Web servers running Internet Information Services (IIS), are scalable by adding additional servers as the load increases.	1) i7-6 >
		Cover HTP Proxy     Setup and Boot Event Collection     Simple TCP/IP Services     SMB 1.0/CIFS File Sharing Support (Installed)     SMB Bandwidth Limit     SMTP Server		•

#### Configure Network Load Balancing for AD FS

Before you can load balance all the nodes in the AD FS farm, you must first create a new load balance cluster. Once you have created the cluster, then you can add new nodes to that cluster.

Sign-in a node of the federation farm with *Admin* equivalent credentials.

1. Open Network Load Balancing Manager from Administrative Tools.



- 2. Right-click Network Load Balancing Clusters, and then click New Cluster.
- 3. To connect to the host that is to be a part of the new cluster, in the **Host** text box, type the name of the host, and then click **Connect**.

Recycle Bin				
영 Network Load Balanc File Cluster Host Of 만-츐 Network Load Bala	ing Manager New Cluster : Connect Connect to one host that is to be part of the r Host: adfs	new cluster and select the cluster interface	-      X     vbnet mask     Oluster mov	
	Connection status Connected Interfaces available for configuring a new clu	ster Interface IP		
Log En Date 1 0001 4/16/2017	Lthemet	10.0.20.1		
0002 4/16/2017	< Back	Next > Cancel Help	- - 	
<b>:                                    </b>	2 🔖 💷 🏄	Fortes	Activate Winc Go to Settings to a Wir sting purposes only. Build 14393	JOWS activate Windows. Idows Server 2016 Datacenter Brs1_release_sec.170327-1835 ☐ 48 4/16/2017

4. Select the interface that you want to use with the cluster, and then click **Next**. (The interface hosts the virtual IP address and receives the client traffic to load balance.)

- 5. In **Host Parameters**, select a value in **Priority (Unique host identifier)**. This parameter specifies a unique ID for each host. The host with the lowest numerical priority among the current members of the cluster handles all of the cluster's network traffic that is not covered by a port rule. Click **Next**.
- In Cluster IP Addresses, click Add and type the cluster IP address that is shared by every host in the cluster. NLB adds this IP address to the TCP/IP stack on the selected interface of all hosts that are chosen to be part of the cluster. Click Next.

File       Custer       Hot Ouster : Cluster IP Addresses         Image: Cluster Hot Ouster for Addresses are shared by every member of the cluster for load balancing.       Unet mask:       Quster more than the file of the cluster for load balancing.         Image: Cluster       Image: Cluster in the file of the cluster for load balancing.       Image: Cluster in the file of the cluster for load balancing.       Image: Cluster in the file of the cluster for load balancing.         Image: Cluster       Image: Cluster in the file of the cluster for load balancing.       Image: Cluster in the file of the cluster for load balancing.         Image: Cluster       Image: Cluster in the file of the cluster for load balancing.       Image: Cluster in the file of the cluster for load balancing.         Image: Cluster in the file of the cluster for load balancing.       Image: Cluster in the file of the cluster for load balancing.         Image: Cluster in the file of the cluster for load balancing.       Image: Cluster in the file of the cluster for load balancing.         Image: Cluster in the file of the cluster for load balancing.       Image: Cluster in the file of the cluster for load balancing.         Image: Cluster in the file of the cluster in the cluster in the file of the cluster in	Recycle Bin	g Manager	
Log En Date 001 4/16/2017 0002 4/16/2017           	File Cluster Host Of	lew Cluster : Cluster IP Addresses       >         The cluster IP addresses are shared by every member of the cluster for load balancing.       Im firm         The firm       IIP Address       >         Ouster       IPv4 address:       IIPv4 address:         IP address:       10 . 0 . 20 . 100       Subnet mask:       255 . 255 . 0 . 0         Odd IPv6 address:       IIPv6 address:       IIPv6 address:       IIPv6 address:         IPv6 address:       IIPv6 addresse:       IIPv6 addresse:       IIPv6 addresse:	Cluster mov
For testing purposes only. Build 1/303 rs1 release ser 170327-19	Log En Date 0001 4/16/2017 0002 4/16/2017	OK Cancel ove	Activate Windows Go to Settings to activate Windows. Windows Server 2016 TDatacente

7. In **Cluster Parameters**, select values in **IP Address** and **Subnet mask** (for IPv6 addresses, a subnet mask value is not needed). Type the full Internet name that users will use to access this NLB cluster.

Network Load Balanci File Cluster Host O           Image: Cluster Host O	ng Manager New Cluster : Cluster Parameters	- □ ×
⊞ gg ivelwork Load dan	Cluster IP configuration IP address: 10.0.20.100 Subnet mask: 255.255.0.0 Full Internet name: fs.corp.contoso.com Network address: 02bf-0a-00-14-64 Cluster operation mode © Unicast ○ IGMP multicast	ubnet mask Cluster mo
Log En Date 0001 4/16/2017 0002 4/16/2017	< Back Next > Cancel	Help

- 8. In **Cluster operation mode**, click **Unicast** to specify that a unicast media access control (MAC) address should be used for cluster operations. In unicast mode, the MAC address of the cluster is assigned to the network adapter of the computer, and the built-in MAC address of the network adapter is not used. We recommend that you accept the unicast default settings. Click **Next**.
- 9. In Port Rules, click Edit to modify the default port rules to use port 443.

8			
Recycle Bir			
	🎬   🛃 📕 🗕	Shortcut Tools Application Tools Administrative Tools	— — X
	🧔 Network Load Balancing Mana	Jer	- 🗆 × 🗹 😮
	File Cluster Host O	Add/Edit Port Rule	× ×
	Berner Load Bar	Cluster IP address or ☑ All Port range From: 443 ♀ To: 443 ♀ Protocols ● ICP ○ UDP ○ Both Filtering mode ● Multiple host Affinity: ○ None ● Single ○ Network □ Timgout(in minutes): 0 ♀	ubnet mask Cluster mo ity ie B B B B B B B B B B B B B
	Cog En Date 0001 4/16/2017 0002 4/16/2017	Single host     2       Disable this port range     0K	inc
	24 items 1 item selected 1.	Task Scheduler 7/16/2016 6:18 AM	Shortcut 2 KB Activate Wind FF Go to Settings to activate Windows. Windows Server 2016 Datacenter for testing purposes only. Build 14393/rs1_release_sec.170327-1835
-	e 🗋 🤶 🗊 ک	🎭 😐 🧔	문 4 <mark>x 4/16/2017</mark> 다

#### **Additional AD FS Servers**

- 1. To add more hosts to the cluster, right-click the new cluster, and then click Add Host to Cluster.
- 2. Configure the host parameters (including host priority, dedicated IP addresses, and load weight) for the additional hosts by following the same instructions that you used to configure the initial host. Because you are adding hosts to an already configured cluster, all the cluster-wide parameters remain the same.



## Configure DNS for Device Registration

Sign-in the domain controller or administrative workstation with Domain Admin equivalent credentials. You'll need the Federation service name to complete this task. You can view the federation service name by clicking **Edit Federation Service Properties** from the **Action** pan of the **AD FS** management console, or by using
(Get-AdfsProperties).Hostname. (PowerShell) on the AD FS server.

- 1. Open the **DNS Management** console.
- 2. In the navigation pane, expand the domain controller name node and Forward Lookup Zones.
- 3. In the navigation pane, select the node that has the name of your internal Active Directory domain name.
- 4. In the navigation pane, right-click the domain name node and click New Host (A or AAAA).
- In the name box, type the name of the federation service. In the IP address box, type the IP address of your federation server. Click Add Host.
- 6. Close the DNS Management console

## Configure the Intranet Zone to include the federation service

The Windows Hello provisioning presents web pages from the federation service. Configuring the intranet zone to include the federation service enables the user to authenticate to the federation service using integrated authentication. Without this setting, the connection to the federation service during Windows Hello provisioning prompts the user for authentication.

#### **Create an Intranet Zone Group Policy**

Sign-in the domain controller or administrative workstation with Domain Admin equivalent credentials

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. Expand the domain and select the Group Policy Object node in the navigation pane.
- 3. Right-click Group Policy object and select New
- 4. Type Intranet Zone Settings in the name box and click OK.
- 5. In the content pane, right-click the Intranet Zone Settings Group Policy object and click Edit.
- 6. In the navigation pane, expand **Policies** under **Computer Configuration**.
- 7. Expand Administrative Templates > Windows Component > Internet Explorer > Internet Control Panel, and select Security Page.
- 8. In the content pane, double-click **Site to Zone Assignment List**. Click **Enable**.
- Click Show. In the Value Name column, type the url of the federation service beginning with https. In the Value column, type the number 1. Click OK twice, then close the Group Policy Management Editor.

#### Deploy the Intranet Zone Group Policy object

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. In the navigation pane, expand the domain and right-click the node that has your Active Directory domain name and click **Link an existing GPO...**
- 3. In the **Select GPO** dialog box, select **Intranet Zone Settings** or the name of the Windows Hello for Business Group Policy object you previously created and click **OK**.

### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm all AD FS servers have a valid server authentication certificate
  - The subject of the certificate is the common name (FQDN) of the host or a wildcard name.
  - The alternate name of the certificate contains a wildcard or the FQDN of the federation service
- Confirm the AD FS farm has an adequate number of nodes and is properly load balanced for the anticipated load.
- Confirm **all** AD FS servers in the farm have the latest updates.
- Confirm you restarted the AD FS service.
- Confirm you created a DNS A Record for the federation service and the IP address used is the load-balanced IP address
- Confirm you created and deployed the Intranet Zone settings to prevent double authentication to the federation server.

# Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services (You are here)
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings

# Validate and Deploy Multifactor Authentication Services (MFA)

2/7/2018 • 2 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

Windows Hello for Business requires all users perform an additional factor of authentication prior to creating and registering a Windows Hello for Business credential. Windows Hello for Business deployments use Azure Multi-Factor Authentication (Azure MFA) services for the secondary authentication. On-Premises deployments use Azure MFA server, an on-premises implementation that do not require synchronizing Active Directory credentials to Azure Active Directory.

Azure Multi-Factor Authentication is an easy to use, scalable, and reliable solution that provides a second method of authentication so your users are always protected.

- **Easy to Use** Azure Multi-Factor Authentication is simple to set up and use. The extra protection that comes with Azure Multi-Factor Authentication allows users to manage their own devices. Best of all, in many instances it can be set up with just a few simple clicks.
- **Scalable** Azure Multi-Factor Authentication uses the power of the cloud and integrates with your onpremises AD and custom apps. This protection is even extended to your high-volume, mission-critical scenarios.
- **Always Protected** Azure Multi-Factor Authentication provides strong authentication using the highest industry standards.
- **Reliable** We guarantee 99.9% availability of Azure Multi-Factor Authentication. The service is considered unavailable when it is unable to receive or process verification requests for the two-step verification.

# **On-Premises Azure MFA Server**

On-premises deployments, both key and certificate trust, use the Azure MFA server where the credentials are not synchronized to Azure Active Directory.

#### Infrastructure

A lab or proof-of-concept environment does not need high-availability or scalability. However, a production environment needs both of these. Ensure your environment considers and incorporates these factors, as necessary. All production environments should have a minimum of two MFA serversâ€" one primary and one secondary server. The environment should have a minimum of two User Portal Servers that are load balanced using hardware or Windows Network Load Balancing.

Please follow Download the Azure Multi-Factor Authentication Server to download Azure MFA server.

#### IMPORTANT

Make sure to validate the requirements for Azure MFA server, as outlined in Install and Configure the Azure Multi-Factor Authentication Server before proceeding. Do not use instllation instructions provided in the article.

Once you have validated all the requirements, please proceed to Configure or Deploy Multifactor Authentication Services.

# Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA) (You are here)
- 5. Configure Windows Hello for Business Policy settings

# Configure Windows Hello for Business Policy settings

2/7/2018 • 8 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

You need a Windows 10, version 1703 workstation to run the Group Policy Management Console, which provides the latest Windows Hello for Business and PIN Complexity Group Policy settings. To run the Group Policy Management Console, you need to install the Remote Server Administration Tools for Windows 10. You can download these tools from the Microsoft Download Center. Install the Remote Server Administration Tools for Windows 10 on a computer running Windows 10, version 1703.

Alternatively, you can create copy the .ADMX and .ADML files from a Windows 10, version 1703 to their respective language folder on a Windows Server or you can create a Group Policy Central Store and copy them their respective language folder. See How to create and manage the Central Store for Group Policy Administrative Templates in Windows for more information.

On-premises certificate-based deployments of Windows Hello for Business needs one Group Policy setting: Enable Windows Hello for Business

# Enable Windows Hello for Business Group Policy

The Enable Windows Hello for Business Group Policy setting is the configuration needed for Windows to determine if a user should be attempt to enroll for Windows Hello for Business. A user will only attempt enrollment if this policy setting is configured to enabled.

You can configure the Enable Windows Hello for Business Group Policy setting for computer or users. Deploying this policy setting to computers results in ALL users that sign-in that computer to attempt a Windows Hello for Business enrollment. Deploying this policy setting to a user results in only that user attempting a Windows Hello for Business enrollment. Additionally, you can deploy the policy setting to a group of users so only those users attempt a Windows Hello for Business enrollment. If both user and computer policy settings are deployed, the user policy setting has precedence.

# Create the Windows Hello for Business Group Policy object

The Group Policy object contains the policy settings needed to trigger Windows Hello for Business provisioning and to ensure Windows Hello for Business authentication certificates are automatically renewed.

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. Expand the domain and select the Group Policy Object node in the navigation pane.
- 3. Right-click Group Policy object and select New.
- 4. Type Enable Windows Hello for Business in the name box and click OK.
- 5. In the content pane, right-click the Enable Windows Hello for Business Group Policy object and click Edit.
- 6. In the navigation pane, expand **Policies** under **User Configuration**.
- 7. Expand Administrative Templates > Windows Component, and select Windows Hello for Business.
- 8. In the content pane, double-click Use Windows Hello for Business. Click Enable and click OK.
- 9. Close the Group Policy Management Editor.

# Configure Security in the Windows Hello for Business Group Policy object

The best way to deploy the Windows Hello for Business Group Policy object is to use security group filtering. The enables you to easily manage the users that should receive Windows Hello for Business by simply adding them to a group. This enables you to deploy Windows Hello for Business in phases.

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. Expand the domain and select the Group Policy Object node in the navigation pane.
- 3. Double-click the Enable Windows Hello for Business Group Policy object.
- 4. In the **Security Filtering** section of the content pane, click **Add**. Type *Windows Hello for Business Users* or the name of the security group you previously created and click **OK**.
- 5. Click the **Delegation** tab. Select **Authenticated Users** and click **Advanced**.
- 6. In the **Group or User names** list, select **Authenticated Users**. In the **Permissions for Authenticated Users** list, clear the **Allow** check box for the **Apply Group Policy** permission. Click **OK**.

# Deploy the Windows Hello for Business Group Policy object

The application of the Windows Hello for Business Group Policy object uses security group filtering. This enables you to link the Group Policy object at the domain, ensuring the Group Policy object is within scope to all users. However, the security group filtering ensures only the users included in the *Windows Hello for Business Users* global group receive and apply the Group Policy object, which results in the provisioning of Windows Hello for Business.

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. In the navigation pane, expand the domain and right-click the node that has your Active Directory domain name and click **Link an existing GPO...**
- 3. In the **Select GPO** dialog box, select **Enable Windows Hello for Business** or the name of the Windows Hello for Business Group Policy object you previously created and click **OK**.

Just to reassure, linking the **Windows Hello for Business** Group Policy object to the domain ensures the Group Policy object is in scope for all domain users. However, not all users will have the policy settings applied to them. Only users who are members of the Windows Hello for Business group receive the policy settings. All others users ignore the Group Policy object.

# Other Related Group Policy settings

#### Windows Hello for Business

There are other Windows Hello for Business policy settings you can configure to manage your Windows Hello for Business deployment. These policy settings are computer-based policy setting; so they are applicable to any user that sign-in from a computer with these policy settings.

#### Use a hardware security device

The default configuration for Windows Hello for Business is to prefer hardware protected credentials; however, not all computers are able to create hardware protected credentials. When Windows Hello for Business enrollment encounters a computer that cannot create a hardware protected credential, it will create a software-based credential.

You can enable and deploy the **Use a hardware security device** Group Policy Setting to force Windows Hello for Business to only create hardware protected credentials. Users that sign-in from a computer incapable of creating a hardware protected credential do not enroll for Windows Hello for Business.

Another policy setting becomes available when you enable the Use a hardware security device Group Policy

setting that enables you to prevent Windows Hello for Business enrollment from using version 1.2 Trusted Platform Modules (TPM). Version 1.2 TPMs typically perform cryptographic operations slower than version 2.0 TPMs and are more unforgiven during anti-hammering and PIN lockout activities. Therefore, some organization may want not want slow sign-in performance and management overhead associated with version 1.2 TPMs. To prevent Windows Hello for Business from using version 1.2 TPMs, simply select the TPM 1.2 check box after you enable the Use a hardware security device Group Policy object.

#### **Use biometrics**

Windows Hello for Business provides a great user experience when combined with the use of biometrics. Rather than providing a PIN to sign-in, a user can use a fingerprint or facial recognition to sign-in to Windows, without sacrificing security.

The default Windows Hello for Business enables users to enroll and use biometrics. However, some organization may want more time before using biometrics and want to disable their use until they are ready. To not allow users to use biometrics, configure the **Use biometrics** Group Policy setting to disabled and apply it to your computers. The policy setting disabled all biometrics. Currently, Windows does not provide granular policy setting that enable you to disable specific modalities of biometrics such as allow facial recognition, but disallow fingerprint.

#### **PIN Complexity**

PIN complexity is not specific to Windows Hello for Business. Windows 10 enables users to use PINs outside of Windows Hello for Business. PIN Complexity Group Policy settings apply to all uses of PINs, even when Windows Hello for Business is not deployed.

Windows 10 provides eight PIN Complexity Group Policy settings that give you granular control over PIN creation and management. You can deploy these policy settings to computers, where they affect all users creating PINs on that computer; or, you can deploy these settings to users, where they affect those users creating PINs regardless of the computer they use. If you deploy both computer and user PIN complexity Group Policy settings, the user policy settings have precedence over computer policy settings. Also, this conflict resolution is based on the last applied policy. Windows does not merge the policy settings automatically; however, you can deploy Group Policy to provide to accomplish a variety of configurations. The policy settings included are:

- Require digits
- Require lowercase letters
- Maximum PIN length
- Minimum PIN length
- Expiration
- History
- Require special characters
- Require uppercase letters

In the Windows 10, version 1703, the PIN complexity Group Policy settings have moved to remove misunderstanding that PIN complexity policy settings were exclusive to Windows Hello for Business. The new location of these Group Policy settings is under Administrative Templates\System\PIN Complexity under both the Computer and User Configuration nodes of the Group Policy editor.

### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm you authored Group Policy settings using the latest ADMX/ADML files (from the Widows 10 Creators Editions)
- Confirm you configured the Enable Windows Hello for Business to the scope that matches your deployment (Computer vs. User)
- Confirm you configure the Use Certificate enrollment for on-prem authentication policy setting.

- Confirm you configure automatic certificate enrollment to the scope that matches your deployment (Computer vs. User)
- Confirm you configured the proper security settings for the Group Policy object
  - Removed the allow permission for Apply Group Policy for Domain Users (Domain Users must always have the read permissions)
  - Add the Windows Hello for Business Users group to the Group Policy object and gave the group the allow permission for Apply Group Policy
- Linked the Group Policy object to the correct locations within Active Directory
- Deploy any additional Windows Hello for Business Group Policy setting is a policy separate from the one that enables it for users

# Add users to the Windows Hello for Business Users group

Users must receive the Windows Hello for Business group policy settings and have the proper permission to enroll for the WHFB Authentication certificate. You can provide users with these settings and permissions by adding the group used synchronize users to the Windows Hello for Business Users group. Users and groups that are not members of this group will not attempt to enroll for Windows Hello for Business.

# Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings (You are here)

# On Premises Certificate Trust Deployment

2/27/2018 • 1 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

Windows Hello for Business replaces username and password sign-in to Windows with strong user authentication based on asymmetric key pair. The following deployment guide provides the information needed to successfully deploy Windows Hello for Business in an existing environment.

Below, you can find all the information you will need to deploy Windows Hello for Business in a Certificate Trust Model in your on-premises environment:

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings

# Validate Active Directory prerequisites

2/7/2018 • 2 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

The key registration process for the On-prem deployment of Windows Hello for Business needs the Windows Server 2016 Active Directory schema. The key-trust model receives the schema extension when the first Windows Server 2016 domain controller is added to the forest. The certificate trust model requires manually updating the current schema to the Windows Server 2016 schema. If you already have a Windows Server 2016 domain controller in your forest, you can skip the next step.

Manually updating Active Directory uses the command-line utility **adprep.exe** located at **<drive>:\support\adprep** on the Windows Server 2016 DVD or ISO. Before running adprep.exe, you must identify the domain controller hosting the schema master role.

# Discovering schema role

To locate the schema master role holder, open and command prompt and type:



The command should return the name of the domain controller where you need to adprep.exe. Update the schema locally on the domain controller hosting the Schema master role.

# Updating the Schema

Windows Hello for Business uses asymmetric keys as user credentials (rather than passwords). During enrollment, the public key is registered in an attribute on the user object in Active Directory. The schema update adds this new attribute to Active Directory.

Sign-in to the domain controller hosting the schema master operational role using Enterprise Admin equivalent credentials.

- 1. Open an elevated command prompt.
- 2. Type cd / dx: support adprep where x is the drive letter of the DVD or mounted ISO.
- 3. To update the schema, type adprep /forestprep .
- 4. Read the Adprep Warning. Type the letter **C** and press **Enter** to update the schema.
- 5. Close the Command Prompt and sign-out.

# Create the KeyCredential Admins Security Global Group

The Windows Server 2016 Active Directory Federation Services (AD FS) role registers the public key on the user object during provisioning. You assign write and read permission to this group to the Active Directory attribute to ensure the AD FS service can add and remove keys are part of its normal workflow.

Sign-in a domain controller or management workstation with Domain Admin equivalent credentials.

- 1. Open Active Directory Users and Computers.
- 2. Click View and click Advance Features.
- 3. Expand the domain node from the navigation pane.
- 4. Right-click the Users container. Click New. Click Group.
- 5. Type KeyCredential Admins in the Group Name text box.
- 6. Click **OK**.

# Create the Windows Hello for Business Users Security Global Group

The Windows Hello for Business Users group is used to make it easy to deploy Windows Hello for Business in phases. You assign Group Policy and Certificate template permissions to this group to simplify the deployment by simply adding the users to the group. This provides them the proper permissions to provision Windows Hello for Business and to enroll in the Windows Hello for Business authentication certificate.

Sign-in a domain controller or management workstation with Domain Admin equivalent credentials.

- 1. Open Active Directory Users and Computers.
- 2. Click View and click Advanced Features.
- 3. Expand the domain node from the navigation pane.
- 4. Right-click the **Users** container. Click **New**. Click **Group**.
- 5. Type Windows Hello for Business Users in the Group Name text box.
- 6. Click **OK**.

# Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites (You are here)
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings

# Validate and Configure Public Key Infrastructure

2/7/2018 • 12 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

Windows Hello for Business must have a public key infrastructure regardless of the deployment or trust model. All trust models depend on the domain controllers having a certificate. The certificate serves as a root of trust for clients to ensure they are not communicating with a rogue domain controller. The certificate trust model extends certificate issuance to client computers. During Windows Hello for Business provisioning, the user receives a sign-in certificate.

# Deploy an enterprise certificate authority

This guide assumes most enterprise have an existing public key infrastructure. Windows Hello for Business depends on a Windows enterprise public key infrastructure running the Active Directory Certificate Services role from Windows Server 2012 or later.

#### Lab-based public key infrastructure

The following instructions may be used to deploy simple public key infrastructure that is suitable for a lab environment.

Sign-in using *Enterprise Admin* equivalent credentials on Windows Server 2012 or later server where you want the certificate authority installed.

#### NOTE

Never install a certificate authority on a domain controller in a production environment.

- 1. Open an elevated Windows PowerShell prompt.
- 2. Use the following command to install the Active Directory Certificate Services role.

Add-WindowsFeature Adcs-Cert-Authority -IncludeManagementTools

3. Use the following command to configure the Certificate Authority using a basic certificate authority configuration.

Install-AdcsCertificationAuthority

# Configure a Production Public Key Infrastructure

If you do have an existing public key infrastructure, please review Certification Authority Guidance from Microsoft TechNet to properly design your infrastructure. Then, consult the Test Lab Guide: Deploying an AD CS Two-Tier PKI Hierarchy for instructions on how to configure your public key infrastructure using the information from your design session.

#### **Configure Domain Controller Certificates**

Clients need to trust domain controllers and the best way to do this is to ensure each domain controller has a Kerberos Authentication certificate. Installing a certificate on the domain controller enables the Key Distribution Center (KDC) to prove its identity to other members of the domain. This provides clients a root of trust external to the domain—namely the enterprise certificate authority.

Domain controllers automatically request a domain controller certificate (if published) when they discover an enterprise certificate authority is added to Active Directory. However, certificates based on the Domain Controller and Domain Controller Authentication certificate templates do not include the KDC Authentication object identifier (OID), which was later added to the Kerberos RFC. Therefore, domain controllers need to request a certificate based on the Kerberos Authentication certificate template.

By default, the Active Directory Certificate Authority provides and publishes the Kerberos Authentication certificate template. However, the cryptography configuration included in the provided template is based on older and less performant cryptography APIs. To ensure domain controllers request the proper certificate with the best available cryptography, use the Kerberos Authentication certificate template as a baseline to create an updated domain controller certificate template.

Sign-in to a certificate authority or management workstations with Domain Admin equivalent credentials.

- 1. Open the **Certificate Authority** management console.
- 2. Right-click Certificate Templates and click Manage.
- 3. In the **Certificate Template Console**, right-click the **Kerberos Authentication** template in the details pane and click **Duplicate Template**.
- 4. On the Compatibility tab, clear the Show resulting changes check box. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Authority list. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Recipient list.
- On the General tab, type Domain Controller Authentication (Kerberos) in Template display name. Adjust the validity and renewal period to meet your enterprise's needs.
   Notelf you use different template names, you'll need to remember and substitute these names in different portions of the lab.
- 6. On the Subject tab, select the Build from this Active Directory information button if it is not already selected. Select None from the Subject name format list. Select DNS name from the Include this information in alternate subject list. Clear all other items.
- 7. On the **Cryptography** tab, select **Key Storage Provider** from the **Provider Category** list. Select **RSA** from the **Algorithm name** list. Type **2048** in the **Minimum key size** text box. Select **SHA256** from the **Request hash** list. Click **OK**.
- 8. Close the console.

#### Superseding the existing Domain Controller certificate

Many domain controllers may have an existing domain controller certificate. The Active Directory Certificate Services provides a default certificate template from domain controllers—the domain controller certificate template. Later releases provided a new certificate template—the domain controller authentication certificate template. These certificate templates were provided prior to update of the Kerberos specification that stated Key Distribution Centers (KDCs) performing certificate authentication needed to include the KDC Authentication extension.

The Kerberos Authentication certificate template is the most current certificate template designated for domain controllers and should be the one you deploy to all your domain controllers (2008 or later). The autoenrollment feature in Windows enables you to effortlessly replace these domain controller certificates. You can use the following configuration to replace older domain controller certificates with a new certificate using the Kerberos Authentication certificate template.

Sign-in to a certificate authority or management workstations with *Enterprise Admin* equivalent credentials.

- 1. Open the Certificate Authority management console.
- 2. Right-click Certificate Templates and click Manage.
- In the Certificate Template Console, right-click the Domain Controller Authentication (Kerberos) (or the name of the certificate template you created in the previous section) template in the details pane and click Properties.
- 4. Click the Superseded Templates tab. Click Add.
- 5. From the **Add Superseded Template** dialog, select the **Domain Controller** certificate template and click **OK**. Click **Add**.
- 6. From the **Add Superseded Template** dialog, select the **Domain Controller Authentication** certificate template and click **OK**.
- 7. From the Add Superseded Template dialog, select the Kerberos Authentication certificate template and click OK.
- 8. Add any other enterprise certificate templates that were previously configured for domain controllers to the **Superseded Templates** tab.
- 9. Click OK and close the Certificate Templates console.

The certificate template is configured to supersede all the certificate templates provided in the certificate templates superseded templates list. However, the certificate template and the superseding of certificate templates is not active until you publish the certificate template to one or more certificate authorities.

#### Configure an Internal Web Server Certificate template

Windows 10 clients use the https protocol when communicating with Active Directory Federation Services. To meet this need, you must issue a server authentication certificate to all the nodes in the Active Directory Federation Services farm. On-premises deployments can use a server authentication certificate issued by their enterprise PKI. You must configure a server authentication certificate template so the host running the Active Directory Federation Service can request the certificate.

Sign-in to a certificate authority or management workstations with Domain Admin equivalent credentials.

- 1. Open the Certificate Authority management console.
- 2. Right-click **Certificate Templates** and click **Manage**.
- 3. In the **Certificate Template Console**, right-click the **Web Server** template in the details pane and click **Duplicate Template**.
- On the Compatibility tab, clear the Show resulting changes check box. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Authority list. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Recipient list.
- 5. On the **General** tab, type **Internal Web Server** in **Template display name**. Adjust the validity and renewal period to meet your enterprise's needs.

**Note:** If you use different template names, you'll need to remember and substitute these names in different portions of the lab.

- 6. On the Request Handling tab, select Allow private key to be exported.
- 7. On the **Subject** tab, select the **Supply in the request** button if it is not already selected.
- 8. On the **Security** tab, Click **Add**. Type **Domain Computers** in the **Enter the object names to select** box. Click **OK**. Select the **Allow** check box next to the **Enroll** permission.
- 9. On the **Cryptography** tab, select **Key Storage Provider** from the **Provider Category** list. Select **RSA** from the **Algorithm name** list. Type **2048** in the **Minimum key size** text box. Select **SHA256** from the **Request hash** list. Click **OK**.
- 10. Close the console.

#### **Unpublish Superseded Certificate Templates**

The certificate authority only issues certificates based on published certificate templates. For defense in depth security, it is a good practice to unpublish certificate templates that the certificate authority is not configured to

issue. This includes the pre-published certificate template from the role installation and any superseded certificate templates.

The newly created domain controller authentication certificate template supersedes previous domain controller certificate templates. Therefore, you need to unpublish these certificate templates from all issuing certificate authorities.

Sign-in to the certificate authority or management workstation with *Enterprise Admin* equivalent credentials.

- 1. Open the Certificate Authority management console.
- 2. Expand the parent node from the navigation pane.
- 3. Click Certificate Templates in the navigation pane.
- 4. Right-click the **Domain Controller** certificate template in the content pane and select **Delete**. Click **Yes** on the **Disable certificate templates** window.
- 5. Repeat step 4 for the **Domain Controller Authentication** and **Kerberos Authentication** certificate templates.

#### Publish Certificate Templates to the Certificate Authority

The certificate authority may only issue certificates for certificate templates that are published to that certificate authority. If you have more than one certificate authority and you want that certificate authority to issue certificates based on a specific certificate template, then you must publish the certificate template to all certificate authorities that are expected to issue the certificate.

Sign-in to the certificate authority or management workstations with an Enterprise Admin equivalent credentials.

- 1. Open the Certificate Authority management console.
- 2. Expand the parent node from the navigation pane.
- 3. Click **Certificate Templates** in the navigation pane.
- 4. Right-click the Certificate Templates node. Click New, and click Certificate Template to issue.
- 5. In the **Enable Certificates Templates** window, select the **Domain Controller Authentication (Kerberos)**, and **Internal Web Server** templates you created in the previous steps. Click **OK** to publish the selected certificate templates to the certificate authority.
- 6. If you published the Domain Controller Authentication (Kerberos) certificate template, then you should unpublish the certificate templates you included in the superseded templates list.
  - To unpublish a certificate template, right-click the certificate template you want to unpublish in the details pane of the Certificate Authority console and select **Delete**. Click **Yes** to confirm the operation.
- 7. Close the console.

#### **Configure Domain Controllers for Automatic Certificate Enrollment**

Domain controllers automatically request a certificate from the domain controller certificate template. However, the domain controller is unaware of newer certificate templates or superseded configurations on certificate templates. To continue automatic enrollment and renewal of domain controller certificates that understand newer certificate template and superseded certificate template configurations, create and configure a Group Policy object for automatic certificate enrollment and link the Group Policy object to the Domain Controllers OU.

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. Expand the domain and select the Group Policy Object node in the navigation pane.
- 3. Right-click Group Policy object and select New
- 4. Type Domain Controller Auto Certificate Enrollment in the name box and click OK.
- 5. Right-click the **Domain Controller Auto Certificate Enrollment** Group Policy object and click **Edit**.
- 6. In the navigation pane, expand **Policies** under **Computer Configuration**.
- 7. Expand Windows Settings, Security Settings, and click Public Key Policies.

- 8. In the details pane, right-click Certificate Services Client Auto-Enrollment and select Properties.
- 9. Select Enabled from the Configuration Model list.
- 10. Select the **Renew expired certificates**, **update pending certificates**, and **remove revoked certificates** check box.
- 11. Select the **Update certificates that use certificate templates** check box.
- 12. Click OK. Close the Group Policy Management Editor.

#### Deploy the Domain Controller Auto Certificate Enrollment Group Policy Object

Sign-in to a domain controller or management workstations with Domain Admin equivalent credentials.

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. In the navigation pane, expand the domain and expand the node that has your Active Directory domain name. Right-click the **Domain Controllers** organizational unit and click **Link an existing GPO...**
- 3. In the **Select GPO** dialog box, select **Domain Controller Auto Certificate Enrollment** or the name of the domain controller certificate enrollment Group Policy object you previously created and click **OK**.

#### Validating your work

Windows Hello for Business is a distributed system, which on the surface appears complex and difficult. The key to a successful Windows Hello for Business deployment is to validate phases of work prior to moving to the next phase.

You want to confirm your domain controllers enroll the correct certificates and not any unnecessary (superseded) certificate templates. You need to check each domain controller that autoenrollment for the computer occurred.

#### Use the Event Logs

Windows Server 2012 and later include Certificate Lifecycle events to determine the lifecycles of certificates for both users and computers. Using the Event Viewer, navigate to the CertificateServices-Lifecycles-System event log under Application and Services/Microsoft/Windows.

Look for an event indicating a new certificate enrollment (autoenrollment). The details of the event include the certificate template on which the certificate was issued. The name of the certificate template used to issue the certificate should match the certificate template name included in the event. The certificate thumbprint and EKUs for the certificate are also included in the event. The EKU needed for proper Windows Hello for Business authentication is Kerberos Authentication, in addition to other EKUs provide by the certificate template.

Certificates superseded by your new domain controller certificate generate an archive event in the CertificateServices-Lifecycles-System event. The archive event contains the certificate template name and thumbprint of the certificate that was superseded by the new certificate.

#### **Certificate Manager**

You can use the Certificate Manager console to validate the domain controller has the properly enrolled certificate based on the correct certificate template with the proper EKUs. Use **certIm.msc** to view certificate in the local computers certificate stores. Expand the **Personal** store and view the certificates enrolled for the computer. Archived certificates do not appear in Certificate Manager.

#### Certutil.exe

You can use **certutil.exe** to view enrolled certificates in the local computer. Certutil shows enrolled and archived certificates for the local computer. From an elevated command prompt, run <u>certutil -q -store my</u> to view locally enrolled certificates.

To view detailed information about each certificate in the store, use certutil -q -v -store my to validate automatic certificate enrollment enrolled the proper certificates.

#### Troubleshooting

Windows triggers automatic certificate enrollment for the computer during boot, and when Group Policy updates. You can refresh Group Policy from an elevated command prompt using gpupdate /force. Alternatively, you can forcefully trigger automatic certificate enrollment using certreq -autoenroll -q from an elevated command prompt.

Use the event logs to monitor certificate enrollment and archive. Review the configuration, such as publishing certificate templates to issuing certificate authority and the allow auto enrollment permissions.

# Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure (You are here)
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings

# Prepare and Deploy Windows Server 2016 Active Directory Federation Services

4/9/2018 • 32 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

Windows Hello for Business works exclusively with the Active Directory Federation Service role included with Windows Server 2016 and requires an additional server update. The on-prem certificate trust deployment uses Active Directory Federation Services roles for key registration, device registration, and as a certificate registration authority.

The following guidance describes deploying a new instance of Active Directory Federation Services 2016 using the Windows Information Database as the configuration database, which is ideal for environments with no more than 30 federation servers and no more than 100 relying party trusts.

If your environment exceeds either of these factors or needs to provide SAML artifact resolution, token replay detection, or needs Active Directory Federation Services to operate in a federated provider role, then your deployment needs to use a SQL for your configuration database. To deploy the Active Directory Federation Services using SQL as its configuration database, please review the Deploying a Federation Server Farm checklist.

If your environment has an existing instance of Active Directory Federation Services, then you'll need to upgrade all nodes in the farm to Windows Server 2016 along with the Windows Server 2016 update. If your environment uses Windows Internal Database (WID) for the configuration database, please read Upgrading to AD FS in Windows Server 2016 using a WID database to upgrade your environment. If your environment uses SQL for the configuration database, please read Upgrading to AD FS in Windows Server 2016 with SQL Server to upgrade your environment.

Ensure you apply the Windows Server 2016 Update to all nodes in the farm after you have successfully completed the upgrade.

A new Active Directory Federation Services farm should have a minimum of two federation servers for proper load balancing, which can be accomplished with an external networking peripherals, or with using the Network Load Balancing Role included in Windows Server.

Prepare the Active Directory Federation Services deployment by installing and updating two Windows Server 2016 Servers. Ensure the update listed below is applied to each server before continuing.

### Update Windows Server 2016

Sign-in the federation server with local admin equivalent credentials.

- Ensure Windows Server 2016 is current by running Windows Update from Settings. Continue this process until no further updates are needed. If you're not using Windows Update for updates, please advise the Windows Server 2016 update history page to make sure you have the latest updates available installed.
- 2. Ensure the latest server updates to the federation server includes KB4088889 (14393.2155).

#### IMPORTANT

The above referenced updates are mandatory for Windows Hello for Business all on-premises deployment and hybrid certificate trust deployments for domain joined computers.

## Enroll for a TLS Server Authentication Certificate

Windows Hello for Business on-prem deployments require a federation server for device registration, key registration, and authentication certificate enrollment. Typically, a federation service is an edge facing role. However, the federation services and instance used with the on-prem deployment of Windows Hello for Business does not need Internet connectivity.

The AD FS role needs a server authentication certificate for the federation services, but you can use a certificate issued by your enterprise (internal) certificate authority. The server authentication certificate should have the following names included in the certificate if you are requesting an individual certificate for each node in the federation farm:

- Subject Name: The internal FQDN of the federation server (the name of the computer running AD FS)
- Subject Alternate Name: Your federation service name, such as *fs.corp.contoso.com* (or an appropriate wildcard entry such as \*.corp.contoso.com)

You configure your federation service name when you configure the AD FS role. You can choose any name, but that name must be different than the name of the server or host. For example, you can name the host server **adfs** and the federation service **fs**. The FQDN of the host is adfs.corp.contoso.com and the FQDN of the federation service is fs.corp.contoso.com.

You can; however, issue one certificate for all hosts in the farm. If you chose this option, then leave the subject name blank, and include all the names in the subject alternate name when creating the certificate request. All names should include the FQDN of each host in the farm and the federation service name.

It's recommended that you mark the private key as exportable so that the same certificate can be deployed across each federation server and web application proxy within your AD FS farm. Note that the certificate must be trusted (chain to a trusted root CA). Once you have successfully requested and enrolled the server authentication certificate on one node, you can export the certificate and private key to a PFX file using the Certificate Manager console. You can then import the certificate on the remaining nodes in the AD FS farm.

Be sure to enroll or import the certificate into the AD FS server's computer certificate store. Also, ensure all nodes in the farm have the proper TLS server authentication certificate.

#### **Internal Server Authentication Certificate Enrollment**

Sign-in the federation server with domain admin equivalent credentials.

- 1. Start the Local Computer Certificate Manager (certlm.msc).
- 2. Expand the **Personal** node in the navigation pane.
- 3. Right-click Personal. Select All Tasks and Request New Certificate.
- 4. Click Next on the Before You Begin page.
- 5. Click Next on the Select Certificate Enrollment Policy page.
- 6. On the Request Certificates page, Select the Internal Web Server check box.
- 7. Click the More information is required to enroll for this certificate. Click here to configure settings link

	a	File Action View	ates - Local Con / Help	nputer\Personal\C	ertificates]	_		
Rec	cycle Bin	🧢 🔿 🙍 📰 🗎	1   @ 🕞	?				
		<ul> <li>Certificates - Loca</li> <li>Personal</li> </ul>	l Computer	Issued To	^ epdemo.net	Issued By corp-CA-CA	E	2
		(	Certificate Prop	erties			×	
	🛱 Certificate Enrollment		\Lambda Subject G	eneral Extensions	Private Key Certi	fication Authority Signatur	e	
	Request Certificates	ar of certificater Sele	The subject of can enter infor can be used in Subject of cert	a certificate is the rmation about the a certificate. tificate	user or computer t types of subject na	o which the certificate is i me and alternative name	ssued. You values that	
	click Enroll.	es of certificates, sele	The user or co	mputer that is rece	eiving the certificate	2		
	Active Directory Enrollment Po	olicy	Subject name:					
	Computer	<b>ن</b> ې 51	Common na	me v	Add >			
	Internal Web Server	sı (پَ	Value:		< Remove			
	A More information is re	quired to enroll for th	adfs.corp.co	ntoso.com				
			Alternative na	me:				
			DNS	~				
			Value:		Add >			
	Show all templates		fs.corp.conto	oso.com	< Remove			
						OK Cancel	Apply	
		<	>	<			>	ows Server 2016 Datacente lease_inmarket.161208-225
	P 🗆 🬔 📄	<b>E</b> 🔀					Ę	6:11 AM

- 8. Under Subject name, select Common Name from the Type list. Type the FQDN of the computer hosting the Active Directory Federation Services role and then click Add. Under Alternative name, select DNS from the Type list. Type the FQDN of the name you will use for your federation services (fs.corp.contoso.com). The name you use here MUST match the name you use when configuring the Active Directory Federation Services server role. Click Add. Click OK when finished.
- 9. Click Enroll.

A server authentication certificate should appear in the computer's Personal certificate store.

# Deploy the Active Directory Federation Service Role

The Active Directory Federation Service (AD FS) role provides the following services to support Windows Hello for Business on-premises deployments.

- Device registration
- Key registration
- Certificate registration authority (certificate trust deployments)

#### IMPORTANT

Finish the entire AD FS configuration on the first server in the farm before adding the second server to the AD FS farm. Once complete, the second server receives the configuration through the shared configuration database when it is added the AD FS farm.

Windows Hello for Business depends on proper device registration. For on-premises deployments, Windows Server 2016 AD FS handles device registration.

Sign-in the federation server with Enterprise Admin equivalent credentials.

1. Start Server Manager. Click Local Server in the navigation pane.

- 2. Click Manage and then click Add Roles and Features.
- 3. Click Next on the Before you begin page.
- 4. On the Select installation type page, select Role-based or feature-based installation and click Next.
- 5. On the **Select destination server** page, choose **Select a server from the server pool**. Select the federation server from the **Server Pool** list. Click **Next**.
- 6. On the Select server roles page, select Active Directory Federation Services. Click Next.
- 7. Click **Next** on the **Select features** page.
- 8. Click Next on the Active Directory Federation Service page.
- 9. Click Install to start the role installation.

### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm the AD FS farm uses the correct database configuration.
- Confirm the AD FS farm has an adequate number of nodes and is properly load balanced for the anticipated load.
- Confirm all AD FS servers in the farm have the latest updates.
- Confirm all AD FS servers have a valid server authentication certificate
  - The subject of the certificate is the common name (FQDN) of the host or a wildcard name.
  - The alternate name of the certificate contains a wildcard or the FQDN of the federation service

# Device Registration Service Account Prerequisite

The service account used for the device registration server depends on the domain controllers in the environment.

#### NOTE

Follow the procedures below based on the domain controllers deployed in your environment. If the domain controller is not listed below, then it is not supported for Windows Hello for Business.

#### Windows Server 2012 or later Domain Controllers

Windows Server 2012 or later domain controllers support Group Managed Service Accounts—the preferred way to deploy service accounts for services that support them. Group Managed Service Accounts, or GMSA have security advantages over normal user accounts because Windows handles password management. This means the password is long, complex, and changes periodically. The best part of GMSA is all this happens automatically. AD FS supports GMSA and should be configured using them for additional defense in depth security.

GSMA uses the Microsoft Key Distribution Service that is located on Windows Server 2012 or later domain controllers. Windows uses the Microsoft Key Distribution Service to protect secrets stored and used by the GSMA. Before you can create a GSMA, you must first create a root key for the service. You can skip this if your environment already uses GSMA.

#### Create KDS Root Key

Sign-in a domain controller with Enterprise Admin equivalent credentials.

- 1. Start an elevated Windows PowerShell console.
- 2. Type Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)

#### Windows Server 2008 or 2008 R2 Domain Controllers

Windows Server 2008 and 2008 R2 domain controllers do not host the Microsoft Key Distribution Service, nor do they support Group Managed Service Accounts. Therefore, you must use create a normal user account as a service account where you are responsible for changing the password on a regular basis.

#### **Create an AD FS Service Account**

Sign-in a domain controller or management workstation with Domain Admin equivalent credentials.

- 1. Open Active Directory Users and Computers.
- 2. Right-click the Users container, Click New. Click User.
- 3. In the New Object User window, type adfssvc in the Full name text box. Type adfssvc in the User logon name text box. Click Next.
- 4. Enter and confirm a password for the **adfssvc** user. Clear the **User must change password at next logon** checkbox.
- 5. Click **Next** and then click **Finish**.

## Configure the Active Directory Federation Service Role

#### **IMPORTANT**

Follow the procedures below based on the domain controllers deployed in your environment. If the domain controller is not listed below, then it is not supported for Windows Hello for Business.

#### Windows Server 2012 or later Domain Controllers

Use the following procedures to configure AD FS when your environment uses **Windows Server 2012 or later Domain Controllers**. If you are not using Windows Server 2012 or later Domain Controllers, follow the procedures under the Configure the Active Directory Federation Service Role (Windows Server 2008 or 2008R2 Domain Controllers) section.

Sign-in the federation server with *Domain Admin* equivalent credentials. These procedures assume you are configuring the first federation server in a federation server farm.

#### 1. Start Server Manager.

Click the notification flag in the upper right corner. Click Configure federation services on this server.
 E Server Manager

Dashboard	For adfs	4	Post-deployment Configura	TASKS 💌 🗙		TASKS 💌
Local Server All Servers	Computer name Domain	adfs corp	Configuration required for Activ Federation Services at ADFS Configure the federation service	e Directory on this server.	ites	Never Download updates o Todav at 6:46 AM
File and Storage Services ▷	Windows Firewall Remote management Remote Desktop NIC Teaming Ethernet	Dom Enab Disal Disal 10.0.	Feature installation Configuration required. Installati adfs.corp.mstepdemo.net. Add Roles and Features Task Details	ion succeeded on	ics Configuration	Real-Time Protection Settings On (UTC-08:00) Pacific T Not activated
	Operating system version Hardware information	Microsoft Microsoft	Windows Server 2016 Datacenter Corporation Virtual Machine	Processors Installed memory (RA Total disk space	AM)	Intel(R) Xeon(R) CPU 1.43 GB 40 GB
	EVENTS All events   16 total	م	(ii) ▼ (R) ▼			TASKS 💌

- 3. On the Welcome page, click Create the first federation server farm and click Next.
- 4. Click Next on the Connect to Active Directory Domain Services page.
- On the Specify Service Properties page, select the recently enrolled or imported certificate from the SSL Certificate list. The certificate is likely named after your federation service, such as *fs.corp.contoso.com* or *fs.contoso.com*.
- 6. Select the federation service name from the Federation Service Name list.
- 7. Type the Federation Service Display Name in the text box. This is the name users see when signing in. Click **Next**.
- 8. On the **Specify Service Account** page, select **Create a Group Managed Service Account**. In the **Account Name** box, type **adfssvc**.
- 9. On the Specify Configuration Database page, select Create a database on this server using Windows Internal Database and click Next.
- 10. On the Review Options page, click Next.
- 11. On the Pre-requisite Checks page, click Configure.
- 12. When the process completes, click **Close**.

#### Windows Server 2008 or 2008 R2 Domain Controllers

Use the following procedures to configure AD FS when your environment uses **Windows Server 2008 or 2008 R2 Domain Controllers**. If you are not using Windows Server 2008 or 2008 R2 Domain Controllers, follow the procedures under the Configure the Active Directory Federation Service Role (Windows Server 2012 or later Domain Controllers) section.

Sign-in the federation server with *Domain Admin* equivalent credentials. These instructions assume you are configuring the first federation server in a federation server farm.

#### 1. Start Server Manager.



3. On the Welcome page, click Create the first federation server farm and click Next.

- 4. Click Next on the Connect to Active Directory Domain Services page.
- On the Specify Service Properties page, select the recently enrolled or imported certificate from the SSL Certificate list. The certificate is likely named after your federation service, such as fs.corp.mstepdemo.net or fs.mstepdemo.net.
- 6. Select the federation service name from the Federation Service Name list.
- 7. Type the Federation Service Display Name in the text box. This is the name users see when signing in. Click **Next**.
- 8. On the Specify Service Account page, Select Use an existing domain user account or group Managed Service Account and click Select.
  - In the **Select User or Service Account** dialog box, type the name of the previously created AD FS service account (example adfssvc) and click **OK**. Type the password for the AD FS service account and click **Next**.
- 9. On the Specify Configuration Database page, select Create a database on this server using Windows Internal Database and click Next.
- 10. On the **Review Options** page, click **Next**.
- 11. On the **Pre-requisite Checks** page, click **Configure**.
- 12. When the process completes, click **Close**.
- 13. Do not restart the AD FS server. You will do this later.

# Add the AD FS Service account to the KeyCredential Admin group and the Windows Hello for Business Users group

The KeyCredential Admins global group provides the AD FS service with the permissions needed to perform key registration. The Windows Hello for Business group provides the AD FS service with the permissions needed to enroll a Windows Hello for Business authentication certificate on behalf of the provisioning user.

Sign-in a domain controller or management workstation with *Domain Admin* equivalent credentials.

#### 1. Open Active Directory Users and Computers.

- 2. Click the Users container in the navigation pane.
- 3. Right-click KeyCredential Admins in the details pane and click Properties.
- 4. Click the Members tab and click Add...
- 5. In the Enter the object names to select text box, type adfssvc. Click OK.
- 6. Click OK to return to Active Directory Users and Computers.
- 7. Right-click **Windows Hello for Business Users** group
- 8. Click the Members tab and click Add...
- 9. In the Enter the object names to select text box, type adfssvc. Click OK.
- 10. Click OK to return to Active Directory Users and Computers.
- 11. Change to server hosting the AD FS role and restart it.

#### **Configure Permissions for Key Registration**

Key Registration stores the Windows Hello for Business public key in Active Directory. In on-prem deployments, the Windows Server 2016 AD FS server registers the public key with the on-premises Active Directory.

The key-trust model needs Windows Server 2016 domain controllers, which configures the key registration permissions automatically; however, the certificate-trust model does not and requires you to add the permissions manually.

Sign-in a domain controller or management workstations with Domain Admin equivalent credentials.

- 1. Open Active Directory Users and Computers.
- 2. Right-click your domain name from the navigation pane and click **Properties**.
- 3. Click Security (if the Security tab is missing, turn on Advanced Features from the View menu).

- 4. Click Advanced. Click Add. Click Select a principal.
- 5. The Select User, Computer, Service Account, or Group dialog box appears. In the Enter the object name to select text box, type KeyCredential Admins. Click OK.
- 6. In the Applies to list box, select Descendant User objects.
- 7. Using the scroll bar, scroll to the bottom of the page and click **Clear all**.
- 8. In the Properties section, select Read msDS-KeyCredentialLink and Write msDS-KeyCrendentialLink.
- 9. Click **OK** three times to complete the task.

# Configure the Device Registration Service

Sign-in the federation server with *Enterprise Admin* equivalent credentials. These instructions assume you are configuring the first federation server in a federation server farm.

- 1. Open the AD FS management console.
- 2. In the navigation pane, expand Service. Click Device Registration.
- 3. In the details pane, click **Configure Device Registration**.
- 4. In the Configure Device Registration dialog, click OK.

## Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm you followed the correct procedures based on the domain controllers used in your deployment
  - Windows Server 2012 or Windows Server 2012 R2
  - Windows Server 2008 or Windows Server 2008 R2
- Confirm you have the correct service account based on your domain controller version.
- Confirm you properly installed the AD FS role on your Windows Server 2016 based on the proper sizing of your federation, the number of relying parties, and database needs.
- Confirm you used a certificate with the correct names as the server authentication certificate
  - Record the expiration date of the certificate and set a renewal reminder at least six weeks before it expires that includes the:
    - Certificate serial number
    - Certificate thumbprint
    - Common name of the certificate
    - Subject alternate name of the certificate
    - Name of the physical host server
    - The issued date
    - The expiration date
    - Issuing CA Vendor (if a third-party certificate)
- Confirm you granted the AD FS service allow read and write permissions to the ms-DSKeyCredentialLink Active Directory attribute.
- Confirm you enabled the Device Registration service.

# Prepare and Deploy AD FS Registration Authority

A registration authority is a trusted authority that validates certificate request. Once it validates the request, it presents the request to the certificate authority for issuance. The certificate authority issues the certificate, returns it to the registration authority, which returns the certificate to the requesting user. The Windows Hello for Business on-prem certificate-based deployment uses the Active Directory Federation Server (AD FS) as the certificate registration authority.

#### **Configure Registration Authority template**

The certificate registration authority enrolls for an enrollment agent certificate. Once the registration authority verifies the certificate request, it signs the certificate request using its enrollment agent certificate and sends it to the certificate authority. The Windows Hello for Business Authentication certificate template is configured to only issue certificates to certificate requests that have been signed with an enrollment agent certificate. The certificate authority only issues a certificate for that template if the registration authority signs the certificate request.

The registration authority template you configure depends on the AD FS service configuration, which depends on the domain controllers the environment uses for authentication.

#### IMPORTANT

Follow the procedures below based on the domain controllers deployed in your environment. If the domain controller is not listed below, then it is not supported for Windows Hello for Business.

#### Windows 2012 or later domain controllers

Sign-in a certificate authority or management workstations with Domain Admin equivalent credentials.

- 1. Open the Certificate Authority Management console.
- 2. Right-click Certificate Templates and click Manage.
- 3. In the **Certificate Template Console**, right click on the **Exchange Enrollment Agent (Offline request)** template details pane and click **Duplicate Template**.
- On the Compatibility tab, clear the Show resulting changes check box. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Authority list. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Recipient list.
- 5. On the **General** tab, type **WHFB Enrollment Agent** in **Template display name**. Adjust the validity and renewal period to meet your enterprise's needs.
- 6. On the Subject tab, select the Supply in the request button if it is not already selected. Note: The preceding step is very important. Group Managed Service Accounts (GMSA) do not support the Build from this Active Directory information option and will result in the AD FS server failing to enroll the enrollment agent certificate. You must configure the certificate template with Supply in the request to ensure that AD FS servers can perform the automatic enrollment and renewal of the enrollment agent certificate.
- On the Cryptography tab, select Key Storage Provider from the Provider Category list. Select RSA from the Algorithm name list. Type 2048 in the Minimum key size text box. Select SHA256 from the Request hash list.
- 8. On the **Security** tab, click **Add**.
- 9. Click Object Types. Select the Service Accounts check box and click OK.
- 10. Type adfssvc in the Enter the object names to select text box and click OK.
- 11. Click the adfssvc from the Group or users names list. In the Permissions for adfssvc section, In the Permissions for adfssvc section, select the Allow check box for the Enroll permission. Excluding the adfssvc user, clear the Allow check box for the Enroll and Autoenroll permissions for all other items in the Group or users names list if the check boxes are not already cleared. Click OK.
- 12. Close the console.

#### Windows 2008 or 2008R2 domain controllers

Sign-in a certificate authority or management workstations with Domain Admin equivalent credentials.

- 1. Open the Certificate Authority management console.
- 2. Right-click Certificate Templates and click Manage.
- 3. In the Certificate Template console, right-click the Exchange Enrollment Agent template in the details

pane and click **Duplicate Template**.

- On the Compatibility tab, clear the Show resulting changes check box. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Authority list. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Recipient list.
- 5. On the **General** tab, type **WHFB Enrollment Agent** in **Template display name**. Adjust the validity and renewal period to meet your enterprise's needs.
- 6. On the Subject tab, select the Build from this Active Directory information button if it is not already selected. Select Fully distinguished name from the Subject name format list if Fully distinguished name is not already selected. Select the User Principal Name (UPN) check box under Include this information in alternative subject name.
- 7. On the **Cryptography** tab, select **Key Storage Provider** from the **Provider Category** list. Select **RSA** from the **Algorithm name** list. Type **2048** in the **Minimum key size** text box. Select **SHA256** from the **Request hash** list.
- 8. On the Security tab, click Add. Type adfssvc in the Enter the object names to select text box and click OK.
- 9. Click the adfssvc from the Group or users names list. In the Permissions for adfssvc section, select the Allow check box for the Enroll permission. Excluding the adfssvc user, clear the Allow check boxes for the Enroll and Autoenroll permissions for all other items in the Group or users names list if the check boxes are not already cleared. Click OK.
- 10. Close the console.

#### Configure the Windows Hello for Business Authentication Certificate template

During Windows Hello for Business provisioning, the Windows 10, version 1703 client requests an authentication certificate from the Active Directory Federation Service, which requests the authentication certificate on behalf of the user. This task configures the Windows Hello for Business authentication certificate template. You use the name of the certificate template when configuring.

Sign-in a certificate authority or management workstations with Domain Admin equivalent credentials.

- 1. Open the Certificate Authority management console.
- 2. Right-click Certificate Templates and click Manage.
- 3. Right-click the Smartcard Logon template and choose Duplicate Template.
- On the Compatibility tab, clear the Show resulting changes check box. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Authority list. Select Windows Server 2012 or Windows Server 2012 R2 from the Certification Recipient list.
- 5. On the **General** tab, type **WHFB Authentication** in **Template display name**. Adjust the validity and renewal period to meet your enterprise's needs.

**Note:** If you use different template names, you'll need to remember and substitute these names in different portions of the deployment.

- 6. On the **Cryptography** tab, select **Key Storage Provider** from the **Provider Category** list. Select **RSA** from the **Algorithm name** list. Type **2048** in the **Minimum key size** text box. Select **SHA256** from the **Request hash** list.
- 7. On the Extensions tab, verify the Application Policies extension includes Smart Card Logon.
- 8. On the **Issuance Requirements** tab, select the This number of authorized signatures check box. Type **1** in the text box.
  - Select Application policy from the Policy type required in signature. Select Certificate Request Agent from in the Application policy list. Select the Valid existing certificate option.
- 9. On the Subject tab, select the Build from this Active Directory information button if it is not already selected. Select Fully distinguished name from the Subject name format list if Fully distinguished name is not already selected. Select the User Principal Name (UPN) check box under Include this information in alternative subject name.
- 10. On the **Request Handling** tab, select the **Renew with same key** check box.
- 11. On the Security tab, click Add. Type Window Hello for Business Users in the Enter the object names to select text box and click OK.
- 12. Click the **Windows Hello for Business Users** from the **Group or users names** list. In the **Permissions for Windows Hello for Business Users** section, select the **Allow** check box for the **Enroll** permission. Excluding the **Windows Hello for Business Users** group, clear the **Allow** check box for the **Enroll** and **Autoenroll** permissions for all other entries in the **Group or users names** section if the check boxes are not already cleared. Click **OK**.
- 13. If you previously issued Windows Hello for Business sign-in certificates using Configuration Manger and are switching to an AD FS registration authority, then on the **Superseded Templates** tab, add the previously used **Windows Hello for Business Authentication** template(s), so they will be superseded by this template for the users that have Enroll permission for this template.
- 14. Click on the **Apply** to save changes and close the console.

#### Mark the template as the Windows Hello Sign-in template

Sign-in to an AD FS Windows Server 2016 computer with Enterprise Admin equivalent credentials.

- 1. Open an elevated command prompt.
- 2. Run certutil -dsTemplate WHFBAuthentication msPKI-Private-Key-Flag +CTPRIVATEKEY\_FLAG\_HELLO\_LOGON\_KEY

#### NOTE

If you gave your Windows Hello for Business Authentication certificate template a different name, then replace WHFBAuthentication in the above command with the name of your certificate template. It's important that you use the template name rather than the template display name. You can view the template name on the **General** tab of the certificate template using the Certificate Template management console (certtmpl.msc). Or, you can view the template name using the **Get-CATemplate** ADCS Administration Windows PowerShell cmdlet on our Windows Server 2012 or later certificate authority.

## Publish Enrollment Agent and Windows Hello For Business Authentication templates to the Certificate Authority

Sign-in a certificate authority or management workstations with *Enterprise Admin* equivalent credentials.

- 1. Open the Certificate Authority management console.
- 2. Expand the parent node from the navigation pane.
- 3. Click **Certificate Templates** in the navigation pane.
- 4. Right-click the Certificate Templates node. Click New, and click Certificate Template to issue.
- 5. In the **Enable Certificates Templates** window, select the **WHFB Enrollment Agent** template you created in the previous steps. Click **OK** to publish the selected certificate templates to the certificate authority.
- 6. Publish the **WHFB Authentication** certificate template using step 5.
- 7. Close the console.

#### **Configure the Registration Authority**

Sign-in the AD FS server with Domain Admin equivalent credentials.

- 1. Open a Windows PowerShell prompt.
- 2. Type the following command

Set-AdfsCertificateAuthority -EnrollmentAgent -EnrollmentAgentCertificateTemplate WHFBEnrollmentAgent - WindowsHelloCertificateTemplate WHFBAuthentication

#### NOTE

If you gave your Windows Hello for Business Enrollment Agent and Windows Hello for Business Authentication certificate templates different names, then replace **WHFBEnrollmentAgent** and WHFBAuthentication in the above command with the name of your certificate templates. It's important that you use the template name rather than the template display name. You can view the template name on the **General** tab of the certificate template using the **Certificate Template** management console (certtmpl.msc). Or, you can view the template name using the **Get-CATemplate** ADCS Administration Windows PowerShell cmdlet on a Windows Server 2012 or later certificate authority.

#### **Enrollment Agent Certificate Enrollment**

Active Directory Federation Server used for Windows Hello for Business certificate enrollment perform their own certificate lifecycle management. Once the registration authority is configured with the proper certificate template, the AD FS server attempts to enroll the certificate on the first certificate request or when the service first starts.

Approximately 60 days prior to enrollment agent certificate's expiration, the AD FS service attempts to renew the certificate until it is successful. If the certificate fails to renew, and the certificate expires, the AD FS server will request a new enrollment agent certificate. You can view the AD FS event logs to determine the status of the enrollment agent certificate.

### Additional Federation Servers

Organizations should deploy more than one federation server in their federation farm for high-availability. You should have a minimum of two federation services in your AD FS farm, however most organizations are likely to have more. This largely depends on the number of devices and users using the services provided by the AD FS farm.

#### Server Authentication Certificate

Each server you add to the AD FS farm must have a proper server authentication certificate. Refer to the Enroll for a TLS Server Authentication Certificate section of this document to determine the requirements for your server authentication certificate. As previously stated, AD FS servers used exclusively for on-premises deployments of Windows Hello for Business can use enterprise server authentication certificates rather than server authentication certificates issued by public certificate authorities.

#### Install Additional Servers

Adding federation servers to the existing AD FS farm begins with ensuring the server are fully patched, to include Windows Server 2016 Update needed to support Windows Hello for Business deployments (https://aka.ms/whfbadfs1703). Next, install the Active Directory Federation Service role on the additional servers and then configure the server as an additional server in an existing farm.

## Load Balance AD FS Federation Servers

Many environments load balance using hardware devices. Environments without hardware load-balancing capabilities can take advantage the network load-balancing feature included in Windows Server to load balance the AD FS servers in the federation farm. Install the Windows Network Load Balancing feature on all nodes participating in the AD FS farm that should be load balanced.

#### Install Network Load Balancing Feature on AD FS Servers

Sign-in the federation server with Enterprise Admin equivalent credentials.

- 1. Start Server Manager. Click Local Server in the navigation pane.
- 2. Click Manage and then click Add Roles and Features.
- 3. Click Next On the Before you begin page.

- 4. On the Select installation type page, select Role-based or feature-based installation and click Next.
- 5. On the **Select destination server** page, chose **Select a server from the server pool**. Select the federation server from the **Server Pool** list. Click **Next**.
- 6. On the **Select server roles** page, click **Next**.
- 7. Select Network Load Balancing on the Select features page.
- 8. Click Install to start the feature installation



#### **Configure Network Load Balancing for AD FS**

Before you can load balance all the nodes in the AD FS farm, you must first create a new load balance cluster. Once you have created the cluster, then you can add new nodes to that cluster.

Sign-in a node of the federation farm with Admin equivalent credentials.

1. Open Network Load Balancing Manager from Administrative Tools.

Recycle B	🧔 Network L	oad Balan	icing Manage	r								_		×	
	File Cluster	Host C	Options Hel	р											
	🕀 🙀 Networ	rk Load Ba	alancing Clust	ers	Cluster con	figuratio	n for all known N	NLB clusters							
					Cluster nan	ne		Cluster IP address	3	Cluster IP subne	t mask	Cluster mode			
	Log En Dat	te	Time	Cluster	Host		Description								
	0001 4/1	6/2017 6/2017	11:22:31 A				NLB Manager	session started	<						
	.,.	0,2011					2000 mg rocan	y bound instance.	-						
	]													.:	
												(Filma)	6		
											Action		0.00		
											Go to S	ate vvind lettings to a	ows ctivate '	Window	NS.
												Win	dows Serv	er 2016 D	)atacenter
										For testing pu	irposes on	ly. Build 14393	.rs1_releas	e_sec.17 1:22 AM	0327-1835
		e		2	<b>2</b> 個	<u> </u>						E F	( <u>×</u> ₄,	/16/2017	Ļ

- 2. Right-click **Network Load Balancing Clusters**, and then click **New Cluster**.
- 3.

3.	3. To connect to the host that is to be a and then click <b>Connect</b>	part of the new cluster, in the <b>Host</b> text b	box, type the name of the host,
	Recycle Bin		
	🔕 Network Load Balancing Manager		– 🗆 X
	File Cluster Host O New Cluster :	Connect >	<
	Bernet	adfs Connect Connect Connect Connect Connect Connect Connect Connect Connect adfs Connect Conn	ubnet mask Cluster mov
	Log En Date 0001 4/16/2017 0002 4/16/2017	< Back Next > Cancel Help	
	# P @ C 📄 🗷 🔖	For test	.:: Activate Windows Go to Settings to activate Windows. Windows Server 2016 Datacenter ing purposes only. Build 14393.rs1_release_sec.170327-1835 딸 식 11:33 AM 도 식 1/16/2017
4.	<ol> <li>Select the interface that you want to address and receives the client traffic</li> </ol>	use with the cluster, and then click <b>Next</b> . c to load balance.)	(The interface hosts the virtual IP

- 5. In **Host Parameters**, select a value in **Priority (Unique host identifier)**. This parameter specifies a unique ID for each host. The host with the lowest numerical priority among the current members of the cluster handles all of the cluster's network traffic that is not covered by a port rule. Click **Next**.
- In Cluster IP Addresses, click Add and type the cluster IP address that is shared by every host in the cluster. NLB adds this IP address to the TCP/IP stack on the selected interface of all hosts that are chosen to be part of the cluster. Click Next.

Recycle Bin	ing Manager	
File Cluster Host Of	New Cluster : Cluster IP Addresses       >         The cluster IP addresses are shared by every member of the cluster for load balancing. The firm in a diadress is a standard of the cluster for load balancing.       uster         IP ac       (a) Add IPv4 address:       III (a)	Ubnet mask Cluster mov
Log En Date 1 0001 4/16/2017 0002 4/16/2017 0002 4/16/2017	OK Cancel ove	Activate Windows Go to Settings to activate Windows. Windows Server 2016 Datacente ting purposes only. Build 14393.rs1_release_sec.170327-183:

7. In **Cluster Parameters**, select values in **IP Address** and **Subnet mask** (for IPv6 addresses, a subnet mask value is not needed). Type the full Internet name that users will use to access this NLB cluster.

Log En       Date         0001       4/16/2017	Network Load Balancing     File Cluster Host O     P     P     P     P     P	; Manager Jew Cluster : Cluster Parameters	×	- [	- ×
Log En Date : 0001 4/16/2017 : 0002 4/16/2017 :		Cluster IP configuration IP address: 10.0.20.100 Subnet mask: 255.255.0.0 Full Internet name: Is.corp.contoso.com Network address: 02-bf-0a-00-14-64 Cluster operation mode ① Unicast ① Multicast ① IGMP multicast		ubnet mask	Cluster mov
< Back Next > Cancel Help >	Log En Date 0001 4/16/2017 0002 4/16/2017	< Back Next > Cancel He	lp		,

- 8. In **Cluster operation mode**, click **Unicast** to specify that a unicast media access control (MAC) address should be used for cluster operations. In unicast mode, the MAC address of the cluster is assigned to the network adapter of the computer, and the built-in MAC address of the network adapter is not used. We recommend that you accept the unicast default settings. Click **Next**.
- 9. In Port Rules, click Edit to modify the default port rules to use port 443.

Recycle Bin		
2월   🕑 📑 🖬	Shortcut Tools Application Tools Administrative Tools	X
🥵 Network Load Balancing	Manager	- 🗆 × 🗹 🕐
File Cluster Host O	w Clu Add/Edit Port Rule X X	م
	Define Cluster IP address or  All Pot range From: 443  To: 443  Pot range From: 443  To: 443  Pot range From: 443  To: 443  Pot range Protocols ● ICP ○ UDP ○ Both Filtering mode ● Multiple host Affinity: ○ None ● Single ○ Network Trongout(n minutes): 0  How sight	et mask Cluster mo E G Cluster mo Cluster mo Clust
Log En Date 0001 4/16/2017 0002 4/16/2017	of ee clust O_Single host O_Disable this port range OK Cancel telp	B B B B B B B B B
		B
24 items 1 item sele	ed 1.06 KB	Activate Windows. Go to Settings to activate Windows. Windows Server 2016 Datacenter Process only, Build 14/202 rel, science or 17/2027 1995
#   <th></th> <th>FD05ES ONLY: Build 143993751_Telease_sec.170327-1835 타고 0<sub>8</sub> 11:53 AM 부고 0<sub>8</sub> 4/16/2017</th>		FD05ES ONLY: Build 143993751_Telease_sec.170327-1835 타고 0 <sub>8</sub> 11:53 AM 부고 0 <sub>8</sub> 4/16/2017

#### **Additional AD FS Servers**

- 1. To add more hosts to the cluster, right-click the new cluster, and then click Add Host to Cluster.
- 2. Configure the host parameters (including host priority, dedicated IP addresses, and load weight) for the additional hosts by following the same instructions that you used to configure the initial host. Because you are adding hosts to an already configured cluster, all the cluster-wide parameters remain the same.



## Configure DNS for Device Registration

Sign-in the domain controller or administrative workstation with Domain Admin equivalent credentials. You'll need the Federation service name to complete this task. You can view the federation service name by clicking **Edit Federation Service Properties** from the **Action** pan of the **AD FS** management console, or by using
(Get-AdfsProperties).Hostname. (PowerShell) on the AD FS server.

- 1. Open the DNS Management console.
- 2. In the navigation pane, expand the domain controller name node and Forward Lookup Zones.
- 3. In the navigation pane, select the node that has the name of your internal Active Directory domain name.
- 4. In the navigation pane, right-click the domain name node and click New Host (A or AAAA).
- 5. In the **name** box, type the name of the federation service. In the **IP address** box, type the IP address of your federation server. Click **Add Host**.
- 6. Close the DNS Management console

## Configure the Intranet Zone to include the federation service

The Windows Hello provisioning presents web pages from the federation service. Configuring the intranet zone to include the federation service enables the user to authenticate to the federation service using integrated authentication. Without this setting, the connection to the federation service during Windows Hello provisioning prompts the user for authentication.

#### **Create an Intranet Zone Group Policy**

Sign-in the domain controller or administrative workstation with Domain Admin equivalent credentials

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. Expand the domain and select the Group Policy Object node in the navigation pane.
- 3. Right-click Group Policy object and select New
- 4. Type Intranet Zone Settings in the name box and click OK.
- 5. In the content pane, right-click the Intranet Zone Settings Group Policy object and click Edit.
- 6. In the navigation pane, expand **Policies** under **Computer Configuration**.
- 7. Expand Administrative Templates > Windows Component > Internet Explorer > Internet Control Panel, and select Security Page.
- 8. In the content pane, double-click **Site to Zone Assignment List**. Click **Enable**.
- 9. Click **Show**. In the **Value Name** column, type the url of the federation service beginning with https. In the **Value** column, type the number **1**. Click OK twice, then close the Group Policy Management Editor.

#### Deploy the Intranet Zone Group Policy object

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. In the navigation pane, expand the domain and right-click the node that has your Active Directory domain name and click **Link an existing GPO...**
- 3. In the **Select GPO** dialog box, select **Intranet Zone Settings** or the name of the Windows Hello for Business Group Policy object you previously created and click **OK**.

### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm you configured the correct enrollment agent certificate template based on the type of AD FS service account.
- Confirm only the AD FS service account has the allow enroll permission for the enrollment agent certificate template.
- Consider using an HSM to protect the enrollment agent certificate; however, understand the frequency and quantity of signature operations the enrollment agent server makes and understand the impact it has on overall performance.
- Confirm you properly configured the Windows Hello for Business authentication certificate template—to include:
  - Issuance requirements of an authorized signature from a certificate request agent.
  - The certificate template was properly marked as a Windows Hello for Business certificate template using certutil.exe
  - The Windows Hello for Business Users group, or equivalent has the allow enroll and allow auto enroll permissions
- Confirm all certificate templates were properly published to the appropriate issuing certificate authorities.
- Confirm the AD FS service account has the allow enroll permission for the Windows Hello Business authentication certificate template.
- Confirm the AD FS certificate registration authority is properly configured using the Get-AdfsCertificateAuthority Windows PowerShell cmdlet.
- Confirm you restarted the AD FS service.
- Confirm you properly configured load-balancing (hardware or software).
- Confirm you created a DNS A Record for the federation service and the IP address used is the load-balanced IP address
- Confirm you created and deployed the Intranet Zone settings to prevent double authentication to the federation server.

## Validating your work

You need to verify the AD FS service has properly enrolled for an enrollment agent certificate template. You can verify this is a variety ways, depending on if your service account is a normal user account or if the service account is a group managed service account.

#### **Event Logs**

Use the event logs on the AD FS service to confirm the service account enrolled for an enrollment agent certificate. First, look for the AD FS event ID 443 that confirms certificate enrollment cycle has finished. Once confirmed the AD FS certificate enrollment cycle completed review the CertificateLifecycle-User event log. In this event log, look for event ID 1006, which indicates a new certificate was installed. Details of the event log should show

- The account name under which the certificate was enrolled.
- The action, which should read enroll.
- The thumbprint of the certificate
- The certificate template used to issue the certificate.

#### **Normal Service Account**

When using a normal service account, use the Microsoft Management Console (mmc.exe) and load the Certificate Manager snap-in for the service account and verify.

#### **Group Managed Service Account**

You cannot use the Certificate Manager to view enrolled certificates for group managed service accounts. Use the event log information to confirm the AD FS service account enrolled a certificate. Use certuil.exe to view the details of the certificate now shown in the event log.

Group managed service accounts use user profiles to store user information, which included enrolled certificates. On the AD FS server, use a command prompt and navigate to

 $\label{eq:systemdrive} were \called \calle\ \calle\ \calle\$ 

Each file in this folder represents a certificate in the service account's Personal store (You may need to use DIR /A to view the files in the folder). Match the thumbprint of the certificate from the event log to one of the files in this folder. That file is the certificate. Use the Certutil -q <certificateThumbprintFileName> to view the basic information about the certificate.

For detailed information about the certificate, use Certutil -q -v <certificateThumbprintFileName> .

## Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services (You are here)
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings

## Validate and Deploy Multifactor Authentication Services (MFA)

2/7/2018 • 2 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

Windows Hello for Business requires all users perform multi-factor authentication prior to creating and registering a Windows Hello for Business credential. Windows Hello for Business deployments use Azure Multi-Factor Authentication (Azure MFA) services for the secondary authentication. On-Premises deployments use Azure MFA server, an on-premises implementation that do not require synchronizing Active Directory credentials to Azure Active Directory.

Azure Multi-Factor Authentication is an easy to use, scalable, and reliable solution that provides a second method of authentication so your users are always protected.

- **Easy to Use** Azure Multi-Factor Authentication is simple to set up and use. The extra protection that comes with Azure Multi-Factor Authentication allows users to manage their own devices. Best of all, in many instances it can be set up with just a few simple clicks.
- **Scalable** Azure Multi-Factor Authentication uses the power of the cloud and integrates with your onpremises AD and custom apps. This protection is even extended to your high-volume, mission-critical scenarios.
- **Always Protected** Azure Multi-Factor Authentication provides strong authentication using the highest industry standards.
- **Reliable** We guarantee 99.9% availability of Azure Multi-Factor Authentication. The service is considered unavailable when it is unable to receive or process verification requests for the two-step verification.

### **On-Premises Azure MFA Server**

On-premises deployments, both key and certificate trust, use the Azure MFA server where the credentials are not synchronized to Azure Active Directory.

#### Infrastructure

A lab or proof-of-concept environment does not need high-availability or scalability. However, a production environment needs both of these. Ensure your environment considers and incorporates these factors, as necessary. All production environments should have a minimum of two MFA servers—one primary and one secondary server. The environment should have a minimum of two User Portal Servers that are load balanced using hardware or Windows Network Load Balancing.

Please follow Download the Azure Multi-Factor Authentication Server to download Azure MFA server.

#### IMPORTANT

Make sure to validate the requirements for Azure MFA server, as outlined in Install and Configure the Azure Multi-Factor Authentication Server before proceeding. Do not use instllation instructions provided in the article.

Once you have validated all the requirements, please proceed to Configure or Deploy Multifactor Authentication Services.

## Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA) (You are here)
- 5. Configure Windows Hello for Business Policy settings

# Configure or Deploy Multifactor Authentication Services

3/20/2018 • 33 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

On-premises deployments must use the On-premises Azure MFA Server using the AD FS adapter model Optionally, you can use a third-party MFA server that provides an AD FS Multifactor authentication adapter.

#### TIP

Please make sure you've read Validate and Deploy Multifactor Authentication Services (MFA) before proceeding any further.

### Prerequisites

The Azure MFA Server and User Portal servers have several perquisites and must have connectivity to the Internet.

#### **Primary MFA Server**

The Azure MFA server uses a primary and secondary replication model for its configuration database. The primary Azure MFA server hosts the writeable partition of the configuration database. All secondary Azure MFA servers hosts read-only partitions of the configuration database. All production environment should deploy a minimum of two MFA Servers.

For this documentation, the primary MFA uses the name **mf\*a**\* or **mfa.corp.contoso.com**. All secondary servers use the name **mfa\*n**\* or **mfan.corp.contoso.com**, where *n* is the number of the deployed MFA server.

The primary MFA server is also responsible for synchronizing from Active Directory. Therefore, the primary MFA server should be domain joined and fully patched.

#### **Enroll for Server Authentication**

The communication between the primary MFA server, secondary MFA servers, User Portal servers, and the client is protected using TLS, which needs a server authentication certificate.

Sign-in the primary MFA server with domain admin equivalent credentials.

- 1. Start the Local Computer Certificate Manager (certlm.msc).
- 2. Expand the **Personal** node in the navigation pane.
- 3. Right-click Personal. Select All Tasks and Request New Certificate.
- 4. Click **Next** on the **Before You Begin** page.
- 5. Click Next on the Select Certificate Enrollment Policy page.
- 6. On the Request Certificates page, Select the Internal Web Server check box.
- 7. Click the More information is required to enroll for this certificate. Click here to configure settings link.
- 8. Under **Subject name**, select **Common Name** from the **Type** list. Type the FQDN of the primary MFA server and then click **Add** (mfa.corp.contoso.com). Click **Add**. Click **OK** when finished.
- 9. Click Enroll.

A server authentication certificate should appear in the computer's Personal certificate store.

#### Install the Web Server Role

The Azure MFA server does not require the Web Server role, however, User Portal and the optional Mobile App server communicate with the MFA server database using the MFA Web Services SDK. The MFA Web Services SDK uses the Web Server role.

To install the Web Server (IIS) role, please follow Installing IIS 7 on Windows Server 2008 or Windows Server 2008 R2 or Installing IIS 8.5 on Windows Server 2012 R2 depending on the host Operating System you're going to use.

The following services are required:

- Common Parameters > Default Document.
- Common Parameters > Directory Browsing.
- Common Parameters > HTTP Errors.
- Common Parameters > Static Content.
- Health and Diagnostics > HTTP Logging.
- Performance > Static Content Compression.
- Security > Request Filtering.
- Security > Basic Authentication.
- Management Tools > IIS Management Console.
- Management Tools > IIS 6 Management Compatibility.
- Application Development > ASP.NET 4.5.

#### Update the Server

Update the server using Windows Update until the server has no required or optional updates as the Azure MFA Server software may require one or more of these updates for the installation and software to correctly work. These procedures install additional components that may need to be updated.

#### Configure the IIS Server's Certificate

The TLS protocol protects all the communication to and from the MFA server. To enable this protection, you must configure the default web site to use the previously enrolled server authentication certificate.

Sign in the primary MFA server with *administrator* equivalent credentials.

- 1. From Administrators, Start the Internet Information Services (IIS) Manager console
- 2. In the navigation pane, expand the node with the same name as the local computer. Expand **Settings** and select **Default Web Site**.
- 3. In the Actions pane, click Bindings.
- 4. In the Site Bindings dialog, Click Add.
- 5. In the **Add Site Binding** dialog, select **https** from the **Type** list. In the **SSL certificate** list, select the certificate with the name that matches the FQDN of the computer.
- 6. Click OK. Click Close. From the Action pane, click Restart.

#### Configure the Web Service's Security

The Azure MFA Server service runs in the security context of the Local System. The MFA User Portal gets its user and configuration information from the Azure MFA server using the MFA Web Services. Access control to the information is gated by membership to the Phonefactor Admins security group. You need to configure the Web Service's security to ensure the User Portal and the Mobile App servers can securely communicate to the Azure MFA Server. Also, all User Portal server administrators must be included in the Phonefactor Admins security group.

Sign in the domain controller with *domain administrator* equivalent credentials.

Create Phonefactor Admin group

#### 1. Open Active Directory Users and Computers

2. In the navigation pane, expand the node with the organization's Active Directory domain name. Right-click the

Users container, select New, and select Group.

- 3. In the New Object Group dialog box, type Phonefactor Admins in Group name.
- 4. Click **OK**.

Add accounts to the Phonefactor Admins group

- 1. Open Active Directory Users and Computers.
- 2. In the navigation pane, expand the node with the organization's Active Directory domain name. Select Users. In the content pane. Right-click the **Phonefactors Admin** security group and select **Properties**.
- 3. Click the **Members** tab.
- 4. Click **Add**. Click **Object Types..** In the **Object Types** dialog box, select **Computers** and click **OK**. Enter the following user and/or computers accounts in the **Enter the object names to select** box and then click **OK**.
  - The computer account for the primary MFA Server
  - Group or user account that will manage the User Portal server.

#### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm the hosts of the MFA service has enrolled a server authentication certificate with the proper names.
  - Record the expiration date of the certificate and set a renewal reminder at least six weeks before it expires that includes the:
    - Certificate serial number
    - Certificate thumbprint
    - Common name of the certificate
    - Subject alternate name of the certificate
    - Name of the physical host server
    - $\circ$  The issued date
    - The expiration date
    - Issuing CA Vendor (if a third-party certificate)
- Confirm the Web Services Role was installed with the correct configuration (including Basic Authentication, ASP.NET 4.5, etc).
- Confirm the host has all the available updates from Windows Update.
- Confirm you bound the server authentication certificate to the IIS web site.
- Confirm you created the Phonefactor Admins group.
- Confirm you added the computer account hosting the MFA service to the Phonefactor Admins group and any user account who are responsible for administrating the MFA server or User Portal.

#### **User Portal Server**

The User Portal is an IIS Internet Information Server web site that allows users to enroll in Multi-Factor Authentication and maintain their accounts. A user may change their phone number, change their PIN, or bypass Multi-Factor Authentication during their next sign on. Users will log in to the User Portal using their normal username and password and will either complete a Multi-Factor Authentication call or answer security questions to complete their authentication. If user enrollment is allowed, a user will configure their phone number and PIN the first time they log in to the User Portal. User Portal Administrators may be set up and granted permission to add new users and update existing users.

The User Portal web site uses the user database that is synchronized across the MFA Servers, which enables a design to support multiple web servers for the User Portal and those servers can support internal and external customers. While the user portal web site can be installed directly on the MFA server, it is recommended to install the User Portal on a server separate from the MFA Server to protect the MFA user database, as a layered, defense-in-depth security design.

#### **Enroll for Server Authentication**

Internal and external users use the User Portal to manage their multifactor authentication settings. To protect this communication, you need to enroll all User Portal servers with a server authentication certificate. You can use an enterprise certificate to protect communication to internal User Portal servers.

For external User Portal servers, it is typical to request a server authentication certificate from a public certificate authority. Contact a public certificate authority for more information on requesting a certificate for public use. Follow the procedures below to enroll an enterprise certificate on your User Portal server.

Sign-in the User Portal server with *domain admin* equivalent credentials.

- 1. Start the Local Computer Certificate Manager (certlm.msc).
- 2. Expand the **Personal** node in the navigation pane.
- 3. Right-click Personal. Select All Tasks and Request New Certificate.
- 4. Click Next on the Before You Begin page.
- 5. Click Next on the Select Certificate Enrollment Policy page.
- 6. On the Request Certificates page, Select the Internal Web Server check box.
- 7. Click the More information is required to enroll for this certificate. Click here to configure settings link.
- 8. Under **Subject name**, select **Common Name** from the **Type** list. Type the FQDN of the primary MFA server and then click **Add** (app1.corp.contoso.com).
- 9. Under **Alternative name**, select **DNS** from the **Type** list. Type the FQDN of the name you will use for your User Portal service (mfaweb.corp.contoso.com).
- 10. Click Add. Click OK when finished.
- 11. Click Enroll.

A server authentication certificate should appear in the computer's Personal certificate store.

#### Install the Web Server Role

To do this, please follow the instructions mentioned in the previous Install the Web Server Role section. However, do **not** install Security > Basic Authentication. The user portal server does not requiret this.

#### Update the Server

Update the server using Windows Update until the server has no required or optional updates as the Azure MFA Server software may require one or more of these updates for the installation and software to correctly work. These procedures install additional components that may need to be updated.

#### Configure the IIS Server's Certificate

To do this, please follow the instructions mentioned in the previous Configure the IIS Server's Certificate section.

#### Create WebServices SDK user account

The User Portal and Mobile App web services need to communicate with the configuration database hosted on the primary MFA server. These services use a user account to communicate to authenticate to the primary MFA server. You can think of the WebServices SDK account as a service account used by other servers to access the WebServices SDK on the primary MFA server.

#### 1. Open Active Directory Users and Computers.

- 2. In the navigation pane, expand the node with the organization's Active Directory domain name. Right-click the **Users** container, select **New**, and select **User**.
- 3. In the **New Object User** dialog box, type **PFWSDK\_** in the **First name** and **User logon name** boxes, where is the name of the primary MFA server running the Web Services SDK. Click **Next**.
- 4. Type a strong password and confirm it in the respective boxes. Clear **User must change password at next logon**. Click **Next**. Click **Finish** to create the user account.

#### Add the MFA SDK user account to the Phonefactor Admins group

Adding the WebServices SDK user account to the Phonefactor Admins group provides the user account with the

proper authorization needed to access the configuration data on the primary MFA server using the WebServices SDK.

- 1. Open Active Directory Users and Computers.
- 2. In the navigation pane, expand the node with the organization's Active Directory domain name. Select **Users**. In the content pane. Right-click the **Phonefactors Admin** security group and select Properties.
- 3. Click the Members tab.
- 4. Click **Add**. Click **Object Types..** Type the PFWSDK\_ user name in the **Enter the object names to select** box and then click **OK**.
  - The computer account for the primary MFA Server
  - The Webservices SDK user account
  - Group or user account that will manage the User Portal server.

#### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm the hosts of the user portal are properly configure for load balancing and high-availability.
- Confirm the hosts of the user portal have enrolled a server authentication certificate with the proper names.
  - Record the expiration date of the certificate and set a renewal reminder at least six weeks before it expires that includes the:
    - Certificate serial number
    - Certificate thumbprint
    - Common name of the certificate
    - Subject alternate name of the certificate
    - Name of the physical host server
    - The issued date
    - The expiration date
    - Issuing CA Vendor (if a third-party certificate)
- Confirm the Web Server Role was properly configured on all servers.
- Confirm all the hosts have the latest updates from Windows Update.
- Confirm you created the web service SDK domain account and the account is a member of the Phonefactor Admins group.

## Installing Primary Azure MFA Server

When you install Azure Multi-Factor Authentication Server, you have the following options:

- 1. Install Azure Multi-Factor Authentication Server locally on the same server as AD FS
- 2. Install the Azure Multi-Factor Authentication adapter locally on the AD FS server, and then install Multi-Factor Authentication Server on a different computer (preferred deployment for production environments)

See Configure Azure Multi-Factor Authentication Server to work with AD FS in Windows Server to view detailed installation and configuration options.

Sign-in the federation server with *Domain Admin* equivalent credentials and follow To install and configure the Azure Multi-Factor Authentication server for an express setup with the configuration wizard. You can re-run the authentication wizard by selecting it from the Tools menu on the server.

#### IMPORTANT

Only follow the above mention article to install Azure MFA Server. Once it is intstalled, continue configuration using this article.

#### **Configuring Company Settings**

You need to configure the MFA server with the default settings it applies to each user account when it is imported or synchronized from Active Directory.

Sign-in the primary MFA server with MFA administrator equivalent credentials.

- 1. Start the Multi-Factor Server application
- 2. Click Company Settings.
- 3. On the General Tab, select Fail Authentication from the When internet is not accessible list.
- 4. In User defaults, select Phone Call or Text Message

**Note:** You can use mobile app; however, the configuration is beyond the scope of this document. Read Getting started the MFA Server Mobile App Web Service to configure and use mobile app multi-factor authentication or the Install User Portal topic in the Multi-Factor Server help.

- 5. Select **Enable Global Services** if you want to allow Multi-Factor Authentications to be made to telephone numbers in rate zones that have an associated charge.
- 6. Clear the **User can change phone** check box to prevent users from changing their phone during the Multi-Factor Authentication call or in the User Portal. A consistent configuration is for users to change their phone numbers in Active Directory and let those changes synchronize to the multi-factor server using the Synchronization features in Directory Integration.
- 7. Select **Fail Authentication** from the **When user is disabled** list. Users should provision their account through the user portal.
- 8. Select the appropriate language from the **Phone call language**, **Text message language**, **Mobile app language**, and **OATH token language** lists.
- 9. Under default PIN rules, Select the User can change PIN checkbox to enable users to change their PIN during multi-factor authentication and through the user portal.
- 10. Configure the minimum length for the PIN.
- 11. Select the **Prevent weak PINs** check box to reject weak PINs. A weak PIN is any PIN that could be easily guessed by a hacker: 3 sequential digits, 3 repeating digits, or any 4 digit subset of user phone number are not allowed. If you clear this box, then there are no restrictions on PIN format. For example: User tries to reset PIN to 1235 and is rejected because it's a weak PIN. User will be prompted to enter a valid PIN.
- 12. Select the **Expiration days** check box if you want to expire PINs. If enabled, provide a numeric value representing the number of days the PIN is valid.
- 13. Select the **PIN history** check box if you want to remember previously used PINs for the user. PIN History stores old PINs for each user. Users are not allowed to reset their PIN to any value stored in their PIN History. When cleared, no PIN History is stored. The default value is 5 and range is 1 to 10.

6	Multi-Factor Authentication Server	_ 🗆 X
File View Tools Help		
Image: Weight of the second secon	Company Settings           General         Usemame Resolution         Text Message         OATH Token Text         Reports	Help
OATH Tokens Tags	When interret is not accessible:     Fail Authentication       User defaults       O Phone call       PIN       Text message	
RADIUS IIS Authentication Authentication	Mobile app     Standard       OATH token       Image: Standard	
LDAP Windows Authentication Authentication	User can change phone          Image: Second synchronized with Active Directory         When user is disabled:       Fail Authentication	
	Phone call language:	
Settings	Mobile app language: en: English V	
Email Directory Integration	OATH token language: en: English	
User Portal Web Service SDK	✓ User can change PIN       ✓ Minimum length       ✓ Prevent weak PINs       ✓ Expiration days	
Mobile App Logging	PIN history 5	
	🚝 🚹 R	6:54 PM 6:54 PM 4/23/2017

#### **Configuring Email Settings and Content**

If you are deploying in a lab or proof-of-concept, then you have the option of skipping this step. In a production environment, ideally, you'll want to setup the Azure Multifactor Authentication Server and its user portal web interface prior to sending the email. The email gives your users time to visit the user portal and configure the multifactor settings.

Now that you have imported or synchronized with your Azure Multi-Factor Authentication server, it is advised that you send your users an email that informs them that they have been enrolled in multi-factor authentication.

With the Azure Multi-Factor Authentication Server there are various ways to configure your users for using multifactor authentication. For instance, if you know the users' phone numbers or were able to import the phone numbers into the Azure Multi-Factor Authentication Server from their company's directory, the email will let users know that they have been configured to use Azure Multi-Factor Authentication, provide some instructions on using Azure Multi-Factor Authentication and inform the user of the phone number they will receive their authentications on.

The content of the email will vary depending on the method of authentication that has been set for the user (e.g. phone call, SMS, mobile app). For example, if the user is required to use a PIN when they authenticate, the email will tell them what their initial PIN has been set to. Users are usually required to change their PIN during their first authentication.

If users' phone numbers have not been configured or imported into the Azure Multi-Factor Authentication Server, or users are pre-configured to use the mobile app for authentication, you can send them an email that lets them know that they have been configured to use Azure Multi-Factor Authentication and it will direct them to complete their account enrollment through the Azure Multi-Factor Authentication User Portal. A hyperlink will be included that the user clicks on to access the User Portal. When the user clicks on the hyperlink, their web browser will open and take them to their company's Azure Multi-Factor Authentication User Portal.

By clicking the email icon on the left you can setup the settings for sending these emails. This is where you can enter the SMTP information of your mail server and it allows you to send a blanket wide email by adding a check to the Send mails to users check box.

#### Content

On the Email Content tab, you will see all of the various email templates that are available to choose from. So, depending on how you have configured your users to use multi-factor authentication, you can choose the template that best suits you.

#### Edit the Content Settings

The Azure MFA server does not send emails, even when configured to do so, until you configured the sender information for each email template listed in the Content tab.

Sign-in the primary MFA server with MFA administrator equivalent credentials.

- 1. Open the Multi-Factor Authentication Server console.
- 2. Click Email from the list of icons and click the Email Content tab.
- 3. Select an email template from the list of templates. Click Edit.
- 4. In the **Edit Email** dialog, in the **From** text box, type the email address of the person or group that should appear to have sent the email.

8		Multi-Factor Authentication Server	_ □ >
File View 1	Tools Help		
	<u>8</u> 2	Email Settings Email Content	Hel
Status	Users	Phone Call	
		Edit Email	
OATH Tokens	Tags	Heip B-PIN Type: Phone Call - PIN - New User and the trictation involves so ing on you will continue to	omething you know
		Format: Plain Text v call asking you to enter v tering your PIN and pressi	our PIN followed ng #, the sign on
RADIUS Authentication A	IIS Authentication	Text Me i⊡-One Cc: mtaadmin@corp.contoso.com	
	l.	Subject: Welcome to Multi-Factor Authentication	
LDAP Authentication A	Windows Authentication	Attachment: Browse Ferent phone number. For phone number. For phone number. Ferent phone n	u signing on
<b>1</b>	Ç,	factor authentication involves something you have (your phone). When you sign on, you will password) and something you have (your phone). When you sign on, you will continue to use the same usemame and password. Before your sign on is	tential fraud to
AD FS	Company Settings	complete, you will receive a phone call asking you to enter your PIN followed B→ Two by the pound (#) key to confirm your sign on. If you don't confirm the sign on by entering your PIN and pressing #, the sign on will be denied.	
		Your account has been configured as follows:	
Email	Directory Integration	Phone: <\$phone\$> PIN: <\$pin\$>	
<u> </u>	4	Please reply to this email if this phone number is not correct or you would prefer	
User Portal	Web Service SDK	Mobile / Previous Next Apply Close	
	<i></i>	User Enrollment	
Mobile App	Logging		
		Edit Resend	
	$\mathbf{\Sigma}$		8:53 AM

- 5. Optionally, customize other options in the email template.
- 6. When finished editing the template, Click **Apply**.
- 7. Click **Next** to move to the next email in the list. Repeat steps 4 and 6 to edit the changes.
- 8. Click **Close** when you are done editing the email templates.

#### **Configuring Directory Integration Settings and Synchronization**

Synchronization keeps the Multi-Factor Authentication user database synchronized with the users in Active Directory or another LDAP Lightweight Directory Access Protocol directory. The process is similar to Importing Users from Active Directory, but periodically polls for Active Directory user and security group changes to process. It also provides for disabling or removing users removed from a container or security group and removing users deleted from Active Directory.

It is important to use a different group memberships for synchronizing users from Active Directory and for enabling Windows Hello for Business. Keeping the group memberships separated enables you to synchronize users and configure MFA options without immediately deploying Windows Hello for Business to that user. This deployment approach provides the maximum flexibility, which gives users the ability to configure their settings before they provision Windows Hello for Business. To start provisioning, simply add the group used for synchronization to the Windows Hello for Business Users group (or equivalent if you use custom names).

#### MultiFactorAuthAdSync Service

The MultiFactorAuthAdSync service is a Windows service that performs the periodic polling of Active Directory. It is installed in a Stopped state and is started by the MultiFactorAuth service when configured to run. If you have a multi-server Multi-Factor Authentication configuration, the MultiFactorAuthAdSync may only be run on a single server.

The MultiFactorAuthAdSync service uses the DirSync LDAP server extension provided by Microsoft to efficiently poll for changes. This DirSync control caller must have the "directory get changes" right and DS-Replication-Get-Changes extended control access right. By default, these rights are assigned to the Administrator and LocalSystem accounts on domain controllers. The MultiFactorAuthAdSync service is configured to run as LocalSystem by default. Therefore, it is simplest to run the service on a domain controller. The service can run as an account with lesser permissions if you configure it to always perform a full synchronization. This is less efficient, but requires less account privileges.

#### Settings

Configuring the directory synchronization between Active Directory and the Azure MFA server is easy.

Sign in the primary MFA server with MFA administrator equivalent credentials.

- 1. Open the Multi-Factor Authentication Server console.
- 2. From the Multi-Factor Authentication Server window, click the Directory Integration icon.
- 3. Click the **Synchronization** tab.
- 4. Select Use Active Directory.
- 5. Select **Include trusted domains** to have the Multi-Factor Authentication Server attempt to connect to domains trusted by the current domain, another domain in the forest, or domains involved in a forest trust. When not importing or synchronizing users from any of the trusted domains, clear the checkbox to improve performance.

#### Synchronization

The MFA server uses synchronization items to synchronize users from Active Directory to the MFA server database. Synchronization items enables you to synchronize a collection of users based security groups or Active Directory containers.

You can configure synchronization items based on different criteria and filters. For the purpose of configuring Windows Hello for Business, you need to create a synchronization item based membership of the Windows Hello for Business user group. This ensures the same users who receive Windows Hello for Business policy settings are the same users synchronized to the MFA server (and are the same users with permission to enroll in the certificate). This significantly simplifies deployment and troubleshooting.

See Directory integration between Azure MFA Server and Active Directory for more details.

#### To add a synchronization item

Sign in the primary MFA server with MFA administrator equivalent credentials.

- 1. Open the Multi-Factor Authentication Server console.
- 2. From the Multi-Factor Authentication Server window, click the Directory Integration icon.
- 3. Select the **Synchronization** tab.
- 4. On the **Synchronization** tab, click **Add**.

6			Multi-Factor Auth	entication Serv	rer			D X
File Viev			Add Synchron	ization Item			x	
							<u>Help</u>	Help
٥ð	Domain: corp.contoso.co	om 🗸	Usemame	Name	Email Address	Mobile	Business	
Status	List Search		kakers@corp.contoso	Akers, Kim	kakers@corp.contos			
	View: Security Groups	×						
	KevCredential Admins							
OATH Toke	PhoneFactor Admins							
1	Protected Users BAS and IAS Servers							
	Read-only Domain Controllers							
RADIUS Authenticat	Schema Admins	_						
	WinRMRemoteWMIUsers	=						
		~	<		Ш		>	
LDAP Authenticat	User filter:				<ul> <li>Display users</li> </ul>		1	
Additional	Import: Selected	Security Group - Rec	cursive	¥	Display limit:		1000 🔶	
	Settings Method Defaults Language	Defaults						
AD FS								
	Add new users							
	Update existing users     Disable (Decrementation)			D: U				
Email	Uisable/ Remove users no longer	a member		Disable	¥			
	import prione:	Mobile			*			
	Backup:	Business			¥			
User Porta	Enabled	Only New Users	with Phone Number		¥			
	Send email	New and Update	ed Users		*			
200 E		Assign new P	IN to updated users					
Mobile Ap								
						Add	Close	
							di.	
								4:44 PM
							8 🖥 🕼	4/26/2017

- 5. In the Add Synchronization Item dialog, select Security Groups from the View list.
- 6. Select the group you are using for replication from the list of groups
- 7. Select **Selected Security Groups Recursive** or, select **Security Group** from the **Import** list if you do not plan to nest groups.
- 8. Select Add new users and Update existing users.
- 9. Select Disable/Remove users no longer a member and select Disable from the list.
- 10. Select the attributes appropriate for your environment for **Import phone** and **Backup**.
- 11. Select Enabled and select Only New Users with Phone Number from the list.
- 12. Select Send email and select New and Updated Users.

#### Configure synchronization item defaults

- 1. When creating a new or editing a synchronization item from the Multi-Factor Authentication Server, select the **Method Defaults** tab.
- Select the default second factor authentication method. For example, if the second factor of authentication is a text message, select **Text message**. Select if the direction of text message authentication and if the authentication should use a one-time password or one-time password and PIN (Ensure users are configured to create a PIN if the default second factor of communication requires a PIN).

#### Configure synchronization language defaults

- 1. When creating a new or editing a synchronization item from the Multi-Factor Authentication Server, select the **Language Defaults** tab.
- 2. Select the appropriate default language for these groups of users synchronized by these synchronization item.
- 3. If creating a new synchronization item, click **Add** to save the item. If editing an existing synchronization item, click **Apply** and then click **Close**.

#### TIP

For more information on these settings and the behaviors they control, see Directory integration between Azure MFA Server and Active Directory.

#### Installing the MFA Web Services SDK

The Web Service SDK section allows the administrator to install the Multi-Factor Authentication Web Service SDK. The Web Service SDK is an IIS (Internet Information Server) web service that provides an interface for integrating the full features of the Multi-Factor Authentication Server into most any application. The Web Service SDK uses the Multi-Factor Authentication Server as the data store.

Remember the Web Services SDK is only need on the primary Multi-Factor to easily enable other servers access to the configuration information. The prerequisites section guided you through installing and configuring the items needed for the Web Services SDK, however the installer will validate the prerequisites and make suggest any corrective action needed.

Please follow the instructions under Install the web service SDK to intall the MFA Web Services SDK.

## Install Secondary MFA Servers

Additional MFA servers provided redundancy of the MFA configuration. The MFA server models uses one primary MFA server with multiple secondary servers. Servers within the same group establish communication with the primary server for that group. The primary server replicates to each of the secondary servers. You can use groups to partition the data stored on different servers, for example you can create a group for each domain, forest, or organizational unit.

Follow the same procedures for installing the primary MFA server software for each additional server. Remember that each server must be activated.

Sign in the secondary MFA server with domain administrator equivalent credentials.

1. Once the Multi-Factor Authentication Server console starts, you must configure the current server's replication group membership. You have the option to join an existing group or create a new group. When joining an existing group, the server becomes a secondary server in the existing replication group. When creating a new group, the server becomes the primary server of that replication group. Click **OK**.

**Note:** Group membership cannot be changed after activation. If a server was joined to the wrong group, it must be activated again to join a different group. Please contact support for assistance with deactivating and reactivating a server.

- 2. The console asks you if you want to enable replication by running the **Multi-Server Configuration Wizard**. Click **Yes**.
- 3. In the Multi-Server Configuration Wizard, leave Active Directory selected and clear Certificates. Click Next.
- On the Active Directory page, the wizard determines what configuration is needed to enable replication. Typically, the wizard recommends adding the computer account for the current server to the PhoneFactor Admin group. Click Next to add the computer account to the group.
- 5. On the **Multi-Server Configuration Complete** page, click **Finish** to reboot the computer to update its group membership.

#### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm you downloaded the latest Azure MFA Server from the Azure Portal.
- Confirm the server has Internet connectivity.
- Confirm you installed and activated the Azure MFA Server.

- Confirm your Azure MFA Server configuration meets your organization's needs (Company Settings, Email Settings, etc).
- Confirm you created Directory Synchronization items based on your deployment to synchronize users from Active Directory to the Azure MFA server.
  - For example, you have security groups representing each collection of users that represent a phase of your deployment and a corresponding synchronization item for each of those groups.
- Confirm the Azure MFA server properly communicates with the Azure MFA cloud service by testing multifactor authentication with a newly synchronized user account.
- Confirm you installed the Web Service SDK on the primary MFA server.
- Confirm your MFA servers have adequate redundancy, should you need to promote a secondary server to the primary server.

## Installing the User Portal Server

You previously configured the User Portal settings on the primary MFA server. The User Portal web application communicates to the primary MFA server using the Web Services SDK to retrieve these settings. This configuration is ideal to ensure you can scale up the User Portal application to meet the needs of your internal users.

#### Copying the User Portal Installation file

Sign in the primary MFA server with local administrator equivalent credentials.

- 1. Open Windows Explorer.
- 2. Browse to the C:\Progam Files\MultiFactor Authentication Server folder.
- 3. Copy the MultiFactorAuthenticationUserPortalSetup64.msi file to a folder on the User Portal server.

#### **Configure Virtual Directory name**

Sign in the User Portal server with local administrator equivalent credentials.

- 1. Open Windows Explorer and browse to the folder to which you saved the installation file from the previous step.
- Run the MultiFactorAuthenticationUserPortalSetup64.msi. The installation package asks if you want to download Visual Studio C++ Redistributable for Visual Studio 2015. Click Yes. When prompted, select Save As. The downloaded file is missing its file extension. Save the file with a .exe extension and install the runtime.
- Run the installation package again. The installer package asks about the C++ runtime again; however, this is for the X64 version (the previous prompt was for x86). Click **Yes** to download the installation package and select **Save As** so you can save the downloaded file with a .exe extension. **Install** the run time.
- 4. Run the User Portal installation package. On the Select Installation Address page, use the default settings for Site and Application Pool settings. You can modify the Virtual directory to use a name that is more fitting for the environment, such as mfa (This virtual directory must match the virtual directory specified in the User Portal settings). Click Next.
- 5. Click Close.

#### Edit MFA User Portal config file

Sign in the User Portal server with *local administrator* equivalent credentials.

- 1. Open Windows Explorer and browse to C:\inetpub\wwwroot\MultiFactorAuth (or appropriate directory based on the virtual directory name) and edit the **web.config** file.
- 2. Locate the **USE\_WEB\_SERVICE\_SDK** key and change the value from **false** to **true**.
- Locate the WEB\_SERVICE\_SDK\_AUTHENTICATION\_USERNAME key and set the value to the username of the Web Service SDK account in the PhoneFactor Admins security group. Use a qualified username, like domain\username or machine\username.
- 4. Locate the **WEB\_SERVICE\_SDK\_AUTHENTICATION\_PASSWORD** key and set the value to the password of the

Web Service SDK account in the PhoneFactor Admins security group.

5. Locate the **pfup\_pfwssdk\_PfWsSdk** setting and change the value from

## "http://localhost:4898/PfWsSdk.asmx" to the URL of the Web Service SDK that is running on the Azure Multi-Factor Authentication Server (e.g.

https://computer1.domain.local/MultiFactorAuthWebServiceSdk/PfWsSdk.asmx). Since SSL is used for this connection, refer to the Web Service SDK by server name, not IP address, since the SSL certificate was issued for the server name. If the server name does not resolve to an IP address from the internet-facing server, add an entry to the hosts file on that server to map the name of the Azure Multi-Factor Authentication Server to its IP address. Save the **web.config** file after changes have been made.

#### Create a DNS entry for the User Portal web site

Sign-in the domain controller or administrative workstation with Domain Admin equivalent credentials.

- 1. Open the **DNS Management** console.
- 2. In the navigation pane, expand the domain controller name node and Forward Lookup Zones.
- 3. In the navigation pane, select the node that has the name of your internal Active Directory domain name.
- 4. In the navigation pane, right-click the domain name node and click **New Host (A or AAAA)**.
- In the name box, type the host name of the User Portal, such as *mfaweb* (this name must match the name of the certificate used to secure communication to the User Portal). In the IP address box, type the load balanced IP address of the User Portal. Click Add Host.
- 6. Close the **DNS Management** console.

#### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm the user portal application is properly installed on all user portal hosts
- Confirm the USE\_WEB\_SERVICE\_SDK named value has a value equal to true.
- Confirm the WEB\_SERVICE\_SDK\_AUTHENTICATION\_USERNAME named value has the username of the web service SDK domain account previously created and that the user name is represented as DOMAIN\USERNAME
- Confirm the WEB\_SERVICES\_SDK\_AUTHENTICATION\_PASSWORD named value has the correct password for the web service SDK domain account.
- Confirm the pfup\_pfwssdk\_PfWsSdk named value has value that matches the URL of for the SDK service installed on the primary MFA server.
- Confirm you saved the changes to the web.config file.

#### Validating your work

Windows Hello for Business is a distributed system, which on the surface appears complex and difficult. The key to a successful Windows Hello for Business deployment is to validate phases of work prior to moving to the next phase.

Using a web browser, navigate to the URL provided in the *pf\_up\_pfwssdk\_PfWsSdk* named value in the web.config file of any one of the user portal servers. The URL should be protected by a server authentication certificate and should prompt you for authentication. Authenticate to the web site using the username and password provided in the web.config file. Successful authentication and page view confirms the Web SDK configured on the primary MFA server is correctly configured and ready to work with the user portal.

#### **Configuring the User Portal**

The User Portal section allows the administrator to install and configure the Multi-Factor Authentication User Portal. The User Portal is an IIS Internet Information Server web site that allows users to enroll in Multi-Factor Authentication and maintain their accounts. A user may change their phone number, change their PIN, or bypass Multi-Factor Authentication during their next sign on. Users will log in to the User Portal using their normal username and password and will either complete a Multi-Factor Authentication call or answer security questions to complete their authentication. If user enrollment is allowed, a user will configure their phone number and PIN the first time they log in to the User Portal. User Portal Administrators may be set up and granted permission to add new users and update existing users.

#### Settings

Sign in the primary MFA server with MFA administrator equivalent credentials.

- 1. Open the Multi-Factor Authentication Server console.
- 2. From the Multi-Factor Authentication Server window, click the User Portal icon.

8		Multi-Factor Authentication Server	L-	×
File View	Tools Help			
<b>N</b>	<u>Co</u>	User Portal		Help
O		Settings Administrators Security Questions Passed Sessions Trusted IPs		
Status	Users	Install User Portal		
	1 A	lear Data IIPI		
	42			
UATH Tokens	Tags	Vindows Domain		
	<u> </u>	Allow users to log in		
		Allow user entrollment      Breast factorial and and		
RADIUS Authentication	IIS Authentication			
-30	-50.			
	J.C	Promot for bypass seconds		
LDAP Authentication	Windows Authentication			
	100			
	- Co			
AD FS	Company Settings	Mobile app		
	E/M	OATH token		
		Automatically trigger user's default method		
Email	Directory	✓ Allow users to select language		
	Ellem	Allow users to activate mobile app		
8		Device limit		
User Portal	Web Service	Use security questions for fallback		
	JUK	Questions to answer: 4		
音韻	<b></b>	Allow users to associate third-party OATH token		
Mobile App	Logging	Use OATH token for fallback		
		Session timeout (minutes):		
		Enable logging		
		🚗 📶		6:59 PM
	2		8 E (8	4/23/2017

- 3. On the Settings tab, type the URL your users use to access the User Portal. The URL should begin with https, such as <a href="https://mfaportal.corp.contoso.com/mfa">https://mfaportal.corp.contoso.com/mfa</a>. The Multi-Factor Authentication Server uses this information when sending emails to users.
- 4. Select Allow users to log in and Allow user enrollment check boxes.
- 5. Select Allow users to select method. Select Phone call and select Text message (you can select Mobile app later once you have deployed the Mobile app web service). Select Automatically trigger user's default method.
- 6. Select Allow users to select language.
- 7. Select Use security questions for fallback and select 4 from the Questions to answer list.

#### TIP

For more information on these settings and the behaviors they control, see Deploy the user portal for the Azure Multi-Factor Authentication Server.

#### Administrators

The User Portal Settings tab allows the administrator to install and configure the User Portal.

- 1. Open the Multi-Factor Authentication Server console.
- 2. From the Multi-Factor Authentication Server window, click the User Portal icon.
- 3. On the Administrators tab, Click Add
- 4. In the Add Administrator dialog, Click Select User... to pick a user to install and manage the User Portal. Use the

default permissions.

5. Click Add.

#### TIP

For more information on these settings and the behaviors they control, read the **Multi-Factor Authentication Server Help** content.

#### Security Questions

Security questions for the User Portal may be customized to meet your requirements. The questions defined here will be offered as options for each of the four security questions a user is prompted to configure during their first log on to User Portal. The order of the questions is important since the first four items in the list will be used as defaults for the four security questions.

#### Trusted IPs

The Trusted IPs tab allows you to skip Multi-Factor Authentication for User Portal log ins originating from specific IPs. For example, if users use the User Portal from the office and from home, you may decide you don't want their phones ringing for Multi-Factor Authentication while at the office. For this, you would specify the office subnet as a trusted IP entry.

## Configure the AD FS Server to use the MFA for multifactor authentication

You need to configure the AD FS server to use the MFA server. You do this by Installing the MFA Adapter on the primary AD FS Server.

#### Install the MFA AD FS Adapter

Follow Install a standalone instance of the AD FS adapter by using the Web Service SDK. You should follow this instructions on all AD FS servers. You can find the files needed on the MFA server.

#### Edit the MFA AD FS Adapter config file on all ADFS Servers

Sign in the primary AD FS server with *local administrator* equivalent credentials.

- 1. Open Windows Explorer and browse to C:\inetpub\wwwroot\MultiFactorAuth (or appropriate directory based on the virtual directory name) and edit the MultiFactorAuthenticationAdfsAdapter.config file.
- 2. Locate the USE\_WEB\_SERVICE\_SDK key and change the value from false to true.
- Locate the WEB\_SERVICE\_SDK\_AUTHENTICATION\_USERNAME key and set the value to the username of the Web Service SDK account in the PhoneFactor Admins security group. Use a qualified username, like domain\username or machine\username.
- 4. Locate the **WEB\_SERVICE\_SDK\_AUTHENTICATION\_PASSWORD** key and set the value to the password of the Web Service SDK account in the **PhoneFactor Admins** security group.
- 5. Locate the pfup\_pfwssdk\_PfWsSdk setting and change the value from "http://localhost:4898/PfWsSdk.asmx" to the URL of the Web Service SDK that is running on the Azure Multi-Factor Authentication Server (e.g. https://computer1.domain.local/MultiFactorAuthWebServiceSdk/PfWsSdk.asmx). Since SSL is used for this connection, refer to the Web Service SDK by server name, not IP address, since the SSL certificate was issued for the server name. If the server name does not resolve to an IP address from the internet-facing server, add an entry to the hosts file on that server to map the name of the Azure Multi-Factor Authentication Server to its IP address. Save the MultiFactorAuthenticationAdfsAdapter.config file after changes have been made.

#### Edit the AD FS Adapter Windows PowerShell cmdlet

Sign in the primary AD FS server with *local administrator* equivalent credentials.

Edit the **Register-MultiFactorAuthenticationAdfsAdapter.ps1** script adding -ConfigurationFilePath <path> to

the end of the Register-AdfsAuthenticationProvider command where is the full path to the

#### MultiFactorAuthenticationAdfsAdapter.config file.

#### Run the AD FS Adapter PowerShell cmdlet

Sign in the primary AD FS server with local administrator equivalent credentials.

Run **Register-MultiFactorAuthenticationAdfsAdapter.ps1** script in PowerShell to register the adapter. The adapter is registered as **WindowsAzureMultiFactorAuthentication**.

#### NOTE

You must restart the AD FS service for the registration to take effect.

#### Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm the user portal application is properly installed on all user portal hosts
- Confirm the USE\_WEB\_SERVICE\_SDK named value has a value equal to true.
- Confirm the WEB\_SERVICE\_SDK\_AUTHENTICATION\_USERNAME named value has the username of the web service SDK domain account previously created and that the user name is represented as DOMAIN\USERNAME
- Confirm the WEB\_SERVICES\_SDK\_AUTHENTICATION\_PASSWORD named value has the correct password for the web service SDK domain account.
- Confirm the pfup\_pfwssdk\_PfWsSdk named value has value that matches the URL of for the SDK service installed on the primary MFA server.
- Confirm you saved the changes to the web.config file.
- Confirm you restarted the AD FS Service after completing the configuration.

## Test Multifactor Authentication

Now, you should test your Azure Multi-Factor Authentication server configuration before proceeding any further in the deployment. The AD FS and Azure Multi-Factor Authentication server configurations are complete.

- 1. In the Multi-Factor Authentication server, on the left, click Users.
- 2. In the list of users, select a user that is enabled and has a valid phone number to which you have access.
- 3. Click Test.
- 4. In the **Test User** dialog, provide the user's password to authenticate the user to Active Directory.

The Multi-Factor Authentication server communicates with the Azure MFA cloud service to perform a second factor authentication for the user. The Azure MFA cloud service contacts the phone number provided and asks for the user to perform the second factor authentication configured for the user. Successfully providing the second factor should result in the Multi-factor authentication server showing a success dialog.

## Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings

## Configure Windows Hello for Business Policy settings

2/7/2018 • 10 min to read • Edit Online

#### **Applies to**

• Windows 10

This guide only applies to Windows 10, version 1703 or higher.

You need a Windows 10, version 1703 workstation to run the Group Policy Management Console, which provides the latest Windows Hello for Business and PIN Complexity Group Policy settings. To run the Group Policy Management Console, you need to install the Remote Server Administration Tools for Windows 10. You can download these tools from the Microsoft Download Center. Install the Remote Server Administration Tools for Windows 10 on a computer running Windows 10, version 1703.

Alternatively, you can create copy the .ADMX and .ADML files from a Windows 10, version 1703 to their respective language folder on a Windows Server or you can create a Group Policy Central Store and copy them their respective language folder. See How to create and manage the Central Store for Group Policy Administrative Templates in Windows for more information.

On-premises certificate-based deployments of Windows Hello for Business needs three Group Policy settings:

- Enable Windows Hello for Business
- Use certificate for on-premises authentication
- Enable automatic enrollment of certificates

## Enable Windows Hello for Business Group Policy

The Enable Windows Hello for Business Group Policy setting is the configuration needed for Windows to determine if a user should be attempt to enroll for Windows Hello for Business. A user will only attempt enrollment if this policy setting is configured to enabled.

You can configure the Enable Windows Hello for Business Group Policy setting for computer or users. Deploying this policy setting to computers results in ALL users that sign-in that computer to attempt a Windows Hello for Business enrollment. Deploying this policy setting to a user results in only that user attempting a Windows Hello for Business enrollment. Additionally, you can deploy the policy setting to a group of users so only those users attempt a Windows Hello for Business enrollment. If both user and computer policy settings are deployed, the user policy setting has precedence.

## Use certificate for on-premises authentication

The Use certificate for on-premises authentication Group Policy setting determines if the on-premises deployment uses the key-trust or certificate trust on-premises authentication model. You must configure this Group Policy setting to configure Windows to enroll for a Windows Hello for Business authentication certificate. If you do not configure this policy setting, Windows considers the deployment to use key-trust on-premises authentication, which requires a sufficient number of Windows Server 2016 domain controllers to handle the Windows Hello for Business key-trust authentication requests.

You can configure this Group Policy setting for computer or users. Deploying this policy setting to computers results in ALL users requesting a Windows Hello for Business authentication certificate. Deploying this policy setting to a user results in only that user requesting a Windows Hello for Business authentication certificate.

Additionally, you can deploy the policy setting to a group of users so only those users request a Windows Hello for Business authentication certificate. If both user and computer policy settings are deployed, the user policy setting has precedence.

## Enable automatic enrollment of certificates

Windows Hello for Business provisioning performs the initial enrollment of the Windows Hello for Business authentication certificate. This certificate expires based on the duration configured in the Windows Hello for Business authentication certificate template. The Windows 10, version 1703 certificate auto enrollment was updated to renew these certificates before they expire, which significantly reduces user authentication failures from expired user certificates.

The process requires no user interaction provided the user signs-in using Windows Hello for Business. The certificate is renewed in the background before it expires.

## Create the Windows Hello for Business Group Policy object

The Group Policy object contains the policy settings needed to trigger Windows Hello for Business provisioning and to ensure Windows Hello for Business authentication certificates are automatically renewed.

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. Expand the domain and select the Group Policy Object node in the navigation pane.
- 3. Right-click Group Policy object and select New.
- 4. Type Enable Windows Hello for Business in the name box and click OK.
- 5. In the content pane, right-click the Enable Windows Hello for Business Group Policy object and click Edit.
- 6. In the navigation pane, expand **Policies** under **User Configuration**.
- 7. Expand Administrative Templates > Windows Component, and select Windows Hello for Business.
- 8. In the content pane, double-click Use Windows Hello for Business. Click Enable and click OK.
- 9. Double-click **Use certificate for on-premises authentication**. Click **Enable** and click **OK**. Close the **Group Policy Management Editor**.

## Configure Automatic Certificate Enrollment

- 1. Start the Group Policy Management Console (gpmc.msc).
- 2. Expand the domain and select the Group Policy Object node in the navigation pane.
- 3. Right-click the Enable Windows Hello for Business Group Policy object and click Edit.
- 4. In the navigation pane, expand Policies under User Configuration.
- 5. Expand Windows Settings > Security Settings, and click Public Key Policies.
- 6. In the details pane, right-click Certificate Services Client Auto-Enrollment and select Properties.
- 7. Select Enabled from the Configuration Model list.
- 8. Select the **Renew expired certificates**, **update pending certificates**, and **remove revoked certificates** check box.
- 9. Select the Update certificates that use certificate templates check box.
- 10. Click OK. Close the Group Policy Management Editor.

## Configure Security in the Windows Hello for Business Group Policy object

The best way to deploy the Windows Hello for Business Group Policy object is to use security group filtering. The enables you to easily manage the users that should receive Windows Hello for Business by simply adding them to a group. This enables you to deploy Windows Hello for Business in phases.

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. Expand the domain and select the Group Policy Object node in the navigation pane.
- 3. Double-click the Enable Windows Hello for Business Group Policy object.
- 4. In the **Security Filtering** section of the content pane, click **Add**. Type *Windows Hello for Business Users* or the name of the security group you previously created and click **OK**.
- 5. Click the **Delegation** tab. Select **Authenticated Users** and click **Advanced**.
- 6. In the Group or User names list, select Authenticated Users. In the Permissions for Authenticated Users list, clear the Allow check box for the Apply Group Policy permission. Click OK.

## Deploy the Windows Hello for Business Group Policy object

The application of the Windows Hello for Business Group Policy object uses security group filtering. This enables you to link the Group Policy object at the domain, ensuring the Group Policy object is within scope to all users. However, the security group filtering ensures only the users included in the *Windows Hello for Business Users* global group receive and apply the Group Policy object, which results in the provisioning of Windows Hello for Business.

- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. In the navigation pane, expand the domain and right-click the node that has your Active Directory domain name and click **Link an existing GPO...**
- 3. In the **Select GPO** dialog box, select **Enable Windows Hello for Business** or the name of the Windows Hello for Business Group Policy object you previously created and click **OK**.

Just to reassure, linking the **Windows Hello for Business** Group Policy object to the domain ensures the Group Policy object is in scope for all domain users. However, not all users will have the policy settings applied to them. Only users who are members of the Windows Hello for Business group receive the policy settings. All others users ignore the Group Policy object.

## Other Related Group Policy settings

#### Windows Hello for Business

There are other Windows Hello for Business policy settings you can configure to manage your Windows Hello for Business deployment. These policy settings are computer-based policy setting; so they are applicable to any user that sign-in from a computer with these policy settings.

#### Use a hardware security device

The default configuration for Windows Hello for Business is to prefer hardware protected credentials; however, not all computers are able to create hardware protected credentials. When Windows Hello for Business enrollment encounters a computer that cannot create a hardware protected credential, it will create a software-based credential.

You can enable and deploy the **Use a hardware security device** Group Policy Setting to force Windows Hello for Business to only create hardware protected credentials. Users that sign-in from a computer incapable of creating a hardware protected credential do not enroll for Windows Hello for Business.

Another policy setting becomes available when you enable the **Use a hardware security device** Group Policy setting that enables you to prevent Windows Hello for Business enrollment from using version 1.2 Trusted Platform Modules (TPM). Version 1.2 TPMs typically perform cryptographic operations slower than version 2.0 TPMs and are more unforgiven during anti-hammering and PIN lockout activities. Therefore, some organization may want not want slow sign-in performance and management overhead associated with version 1.2 TPMs. To prevent Windows Hello for Business from using version 1.2 TPMs, simply select the TPM 1.2 check box after you enable the Use a hardware security device Group Policy object.

#### **Use biometrics**

Windows Hello for Business provides a great user experience when combined with the use of biometrics. Rather than providing a PIN to sign-in, a user can use a fingerprint or facial recognition to sign-in to Windows, without sacrificing security.

The default Windows Hello for Business enables users to enroll and use biometrics. However, some organization may want more time before using biometrics and want to disable their use until they are ready. To not allow users to use biometrics, configure the **Use biometrics** Group Policy setting to disabled and apply it to your computers. The policy setting disabled all biometrics. Currently, Windows does not provide granular policy setting that enable you to disable specific modalities of biometrics such as allow facial recognition, but disallow fingerprint.

#### **PIN Complexity**

PIN complexity is not specific to Windows Hello for Business. Windows 10 enables users to use PINs outside of Windows Hello for Business. PIN Complexity Group Policy settings apply to all uses of PINs, even when Windows Hello for Business is not deployed.

Windows 10 provides eight PIN Complexity Group Policy settings that give you granular control over PIN creation and management. You can deploy these policy settings to computers, where they affect all users creating PINs on that computer; or, you can deploy these settings to users, where they affect those users creating PINs regardless of the computer they use. If you deploy both computer and user PIN complexity Group Policy settings, the user policy settings have precedence over computer policy settings. Also, this conflict resolution is based on the last applied policy. Windows does not merge the policy settings automatically; however, you can deploy Group Policy to provide to accomplish a variety of configurations. The policy settings included are:

- Require digits
- Require lowercase letters
- Maximum PIN length
- Minimum PIN length
- Expiration
- History
- Require special characters
- Require uppercase letters

In the Windows 10, version 1703, the PIN complexity Group Policy settings have moved to remove misunderstanding that PIN complexity policy settings were exclusive to Windows Hello for Business. The new location of these Group Policy settings is under Administrative Templates\System\PIN Complexity under both the Computer and User Configuration nodes of the Group Policy editor.

## Review

Before you continue with the deployment, validate your deployment progress by reviewing the following items:

- Confirm you authored Group Policy settings using the latest ADMX/ADML files (from the Widows 10 Creators Editions)
- Confirm you configured the Enable Windows Hello for Business to the scope that matches your deployment (Computer vs. User)
- Confirm you configure the Use Certificate enrollment for on-prem authentication policy setting.
- Confirm you configure automatic certificate enrollment to the scope that matches your deployment (Computer vs. User)
- Confirm you configured the proper security settings for the Group Policy object
  - Removed the allow permission for Apply Group Policy for Domain Users (Domain Users must always have the read permissions)
  - Add the Windows Hello for Business Users group to the Group Policy object and gave the group the

allow permission for Apply Group Policy

- Linked the Group Policy object to the correct locations within Active Directory
- Deploy any additional Windows Hello for Business Group Policy setting is a policy separate from the one that enables it for users

## Add users to the Windows Hello for Business Users group

Users must receive the Windows Hello for Business group policy settings and have the proper permission to enroll for the WHFB Authentication certificate. You can provide users with these settings and permissions by adding the group used synchronize users to the Windows Hello for Business Users group. Users and groups that are not members of this group will not attempt to enroll for Windows Hello for Business.

## Follow the Windows Hello for Business on premises certificate trust deployment guide

- 1. Validate Active Directory prerequisites
- 2. Validate and Configure Public Key Infrastructure
- 3. Prepare and Deploy Windows Server 2016 Active Directory Federation Services
- 4. Validate and Deploy Multifactor Authentication Services (MFA)
- 5. Configure Windows Hello for Business Policy settings (You are here)

## Windows Hello for Business Features

4/9/2018 • 6 min to read • Edit Online

Consider these additional features you can use after your organization deploys Windows Hello for Business.

- Conditional access
- Dynamic lock
- PIN reset
- Privileged credentials

## Conditional access

#### **Requirements:**

- Azure Active Directory
- Hybrid Windows Hello for Business deployment

In a mobile-first, cloud-first world, Azure Active Directory enables single sign-on to devices, apps, and services from anywhere. With the proliferation of devices (including BYOD), work off corporate networks, and 3rd party SaaS apps, IT professionals are faced with two opposing goals:+

- Empower the end users to be productive wherever and whenever
- Protect the corporate assets at any time

To improve productivity, Azure Active Directory provides your users with a broad range of options to access your corporate assets. With application access management, Azure Active Directory enables you to ensure that only the right people can access your applications. What if you want to have more control over how the right people are accessing your resources under certain conditions? What if you even have conditions under which you want to block access to certain apps even for the right people? For example, it might be OK for you if the right people are accessing certain apps from a trusted network; however, you might not want them to access these apps from a network you don't trust. You can address these questions using conditional access.

Read Conditional access in Azure Active Directory to learn more about Conditional Access. Afterwards, read Getting started with conditional access in Azure Active Directory to start deploying Conditional access.

## Dynamic lock

#### **Requirements:**

• Windows 10, version 1703

Dynamic lock enables you to configure Windows 10 devices to automatically lock when bluetooth paired device signal falls below the maximum Recieved Signal Stregnth Indicator (RSSI) value. You configure the dynamic lock policy using Group Policy. You can locate the policy setting at **Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Busines**. The name of the policy is **Configure dynamic lock factors**.

The Group Policy Editor, when the policy is enabled, creates a default signal rule policy with the following value:

#### IMPORTANT

Microsoft recommends using the default values for this policy settings. Measurements are relative based on the varying conditions of each environment. Therefore, the same values may produce different results. Test policy settings in each environment prior to broadly deploying the setting.

```
<rule schemaVersion="1.0">
    </rule schemaVersion="1.0">
    </rule schemaVersion="1.0">
    </rule>
</rule>
```

For this policy setting, the **type** and **scenario** attribute values are static and cannot change. The **classofDevice** attribute defaults Phones and uses the values from the following table

DESCRIPTION	VALUE
Miscellaneous	0
Computer	256
Phone	512
LAN/Network Access Point	768
Audio/Video	1024
Peripheral	1280
Imaging	1536
Wearable	1792
Тоу	2048
Health	2304
Uncategorized	7936

The **rssiMin** attribute value signal indicates the strength needed for the device to be considered "in-range". The default value of **-10** enables a user to move about an average size office or cubicle without triggering Windows to lock the device. The **rssiMaxDelta** has a default value of **-10**, which instruct Windows 10 to lock the device once the signal strength weakens by more than measurement of 10.

RSSI measurements are relative and lower as the bluetooth signals between the two paired devices reduces. Therefore a measurement of 0 is stronger than -10, which is stronger than -60, which is an indicator the devices are moving further apart from each other.

### **PIN** reset

Hybrid Deployments Requirements:

• Azure Active Directory

- Hybrid Windows Hello for Business deployment
- Modern Management Microsoft Intune, or compatible mobile device management (MDM)
- Remote reset Windows 10, version 1703
- Reset above Lock Windows 10, version 1709

The Microsoft PIN reset services enables you to help users who have forgotten their PIN. Using Microsoft Intune or a compatible MDM, you can configure Windows 10 devices to securely use the Microsoft PIN reset service that enables you to remotely push a PIN reset or enables users to reset their forgotten PIN above the lock screen without requiring reenrollment.

#### Onboarding the Microsoft PIN reset service to your Intune tenant

Before you can remotely reset PINs, you must onboard the Microsoft PIN reset service to your Intune or MDM tenant, and configure devices you manage. Follow these instructions to get that set up:

#### Connect Intune with the PIN reset service

- 1. Visit Microsoft PIN Reset Service Integration website, and sign in using the tenant administrator account you use to manage your Intune tenant.
- 2. After you log in, click **Accept** to give consent for the PIN reset service to access your account.

Overview	0 Overview	NAME		SIGN-ON OKL
		СМ	Client MDM	https://localhost/mdm
💕 Quick start	MANAGE	CN	Client NON MDM	
MANAGE	All applications	MP	Microsoft Pin Reset Service Deve	elopme_http://prs-t4.azurewebsites.net
x <sup>R</sup> Users and groups	Application proxy	MP	Microsoft Pin Reset Service Integ	gration https://cred.spserv.microsoft.com
👪 Enterprise applications	ACTIVITY	-		
Registrations	Sign-ins			
🚸 Azure AD Connect	Audit logs			

3. In the Azure portal, you can verify that Intune and the PIN reset service were integrated from the Enterprise applications - All applications blade as shown in the following screenshot:

Micros	oft Pin Reset Service
Integra App publisher	ation r website: cred.spserv.microsoft.com
Microsoft Pi	n Reset Service Integration needs permission to:
<ul> <li>Sign in and</li> </ul>	d read user profile 🛛 🖗
You're signe	d in as:
If you agree, resources fo	this app will have access to the specified r all users in your organization. No one else will be

4. Log in to this website using your Intune tenant admin credentials and, again, choose **Accept** to give consent for the service to access your account.

#### Configure Windows devices to use PIN reset

To configure PIN reset on Windows devices you manage, use an Intune Windows 10 custom device policy to enable the feature. Configure the policy using the following Windows policy configuration service provider (CSP):

#### • For devices - ./Device/Vendor/MSFT/PassportForWork/tenant ID/Policies/EnablePinRecovery

*tenant ID* refers to your Azure Active Directory, Directory ID which you can obtain from the **Properties** page of Azure Active Directory.

Set the value for this CSP to True.

Read the Steps to reset the passcode section to removely reset a PIN on an Intune managed device.

#### **On-premises Deployments**

- \*\* Requirements\*\*
- Active Directory
- On-premises Windows Hello for Business deployment
- Reset from settings Windows 10, version 1703
- Reset above Lock Windows 10, version 1709

On-premises deployments provide users with the ability to reset forgotton PINs either through the settings page or from above the user's lock screen. Users must know or be provider their password for authentication, must perform a second factor of authentication, and then reprovision Windows Hello for Business.

#### IMPORTANT

Users must have corporate network connectivity to domain controllers and the AD FS server to reset their PINs.

#### **Reset PIN from Settings**

- 1. Sign-in to Windows 10, version 1703 or later using an alternate credential.
- 2. Open Settings, click Accounts, click Sign-in options.
- 3. Under PIN, click I forgot my PIN and follow the instructions.

#### Reset PIN above the Lock Screen

- 1. On Windows 10, version 1709, click I forgot my PIN from the Windows Sign-in
- 2. Enter your password and press enter.
- 3. Follow the instructions provided by the provisioning process
- 4. When finished, unlock your desktop using your newly creeated PIN.

#### NOTE

Visit the Frequently Asked Questions section of the Windows Hello for Business page and watch the **What happens when the user forgets their PIN?** video.

## **Privileged Credentials**

#### Requirements

- Hybrid and On-premises Windows Hello for Business deployments
- Domain Joined or Hybird Azure joined devices
- Windows 10, version 1709

The privileged credentials scenario enables administrators to perform elevated, admistrative funcions by enrolling both their non-privileged and privileged credentials on their device.

By design, Windows 10 does not enumerate all Windows Hello for Business users from within a user's session. Using the computer Group Policy setting, Allow enumeration of emulated smart card for all users, you can configure a device to all this enumeration on selected devices.

With this setting, administrative users can sign-in to Windows 10, version 1709 using their non-privileged Windows Hello for Business credentials for normal workflow such as email, but can launch Microsoft Managment Consoles (MMCs), Remote Desktop Services clients, and other applications by selecting **Run as different user** or
**Run as administrator**, selecting the privileged user account, and providing their PIN. Administrators can also take advantage of this feature with command line applications by using **runas.exe** combined with the **/smartcard** argument. This enables administrators to perform their day-to-day operations without needing to sign-in and out, or use fast user switching when alternativing between privileged and non-privileged workloads.

# Multifactor Unlock

3/20/2018 • 9 min to read • Edit Online

## **Requirements:**

- Windows Hello for Business deployment (Hybrid or On-premises)
- Hybird Azure AD joined (Hybrid deployments)
- Domain Joined (on-premises deployments)
- Windows 10, version 1709
- Bluetooth, Bluetooth capable phone optional

Windows, today, natively only supports the use of a single credential (password, PIN, fingerprint, face, etc.) for unlocking a device. Therefore, if any of those credentials are compromised (shoulder surfed), an attacker could gain access to the system.

Windows 10 offers Multifactor device unlock by extending Windows Hello with trusted signals, administrators can configure Windows 10 to request a combination of factors and trusted signals to unlock their devices.

Which organizations can take advanage of Multifactor unlock? Those who:

- Have expressed that PINs alone do not meet their security needs.
- Want to prevent Information Workers from sharing credentials.
- Want their orgs to comply with regulatory two-factor authentication policy.
- Want to retain the familiar Windows logon UX and not settle for a custom solution.

You enable multifactor unlock using Group Policy. The **Configure device unlock factors** policy setting is located under **Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Business**.

## The Basics: How it works

First unlock factor credential provider and Second unlock credential provider are repsonsible for the bulk of the configuration. Each of these components contains a globally unque identifier (GUID) that represents a different Windows credential provider. With the policy setting enabled, users unlock the device using at least one credenital provider from each category before Windows allows the user to proceed to their desktop.

The policy setting has three components:

- First unlock factor credential provider
- Second unlock factor credential provider
- Signal rules for device unlock

## Configuring Unlock Factors

The **First unlock factor credential providers** and **Second unlock factor credential providers** portion of the policy setting each contain a comma separated list of credential providers.

Supported credential providers include:

CREDENTIAL PROVIDER	GUID
PIN	{D6886603-9D2F-4EB2-B667-1971041FA96B}
Fingerprint	{BEC09223-B018-416D-A0AC-523971B639F5}
Facial Recognition	{8AF662BF-65A0-4D0A-A540-A338A999D36F}
Trusted Signal (Phone proximity, Network location)	{27FBDB57-B613-4AF2-9D7E-4FA7A66C21AD}

## NOTE

Multifactor unlock does not support third-party credential providers or credential providers not listed in the above table.

The default credential providers for the First unlock factor credential provider include:

- PIN
- Fingerprint
- Facial Recongition

The default credential providers for the Second unlock factor credential provider include:

- Trusted Signal
- PIN

Configure a comma separated list of credential provider GUIDs you want to use as first and second unlock factors. While a credential provider can appear in both lists, remember that a credential supported by that provider can only satisfy one of the unlock factors. Listed credential providers do not need to be in any specific order.

For example, if you include the PIN and fingerprint credential providers in both first and second factor lists, a user can use their fingerprint or PIN as the first unlock factor. However, whichever factor they used to satisfy the first unlock factor cannot be used to satisfy the second unlock factor. Each factor can therefore be used exactly once. The Trusted Signal provider can *only* be specified as part of the Second unlock factor credential provider list.

## Configure Signal Rules for the Trusted Signal Credential Provider

The **Signal rules for device unlock** setting contains the rules the Trusted Signal credential provider uses to satisfy unlocking the device.

## **Rule element**

You represent signal rules in XML. Each signal rule has an starting and ending **rule** element that contains the **schemaVersion** attribute and value. The current supported scheam version is 1.0. **Example** 

```
<rule schemaVersion="1.0"> </rule>
```

## Signal element

Each rule element has a **signal** element. All signal elements have a **type** element and value. Windows 10, version 1709 supports the **ipConfig** and **bluetooth** type values.

ATTRIBUTE	VALUE
type	"bluetooth" or "ipConfig" (Windows 10, version 1709)

## Bluetooth

You define the bluetooth signal with additional attribute in the signal elment. The bluetooth configuration does not use any other elements. You can end the signal element with short ending tag "/>".

ATTRIBUTE	VALUE	REQUIRED
type	"bluetooth"	yes
scenario	"Authentication"	yes
classOfDevice	"number"	no
rssiMin	"number"	no
rssiMaxDelta	"number"	no

## Example:

```
<rule schemaVersion="1.0">
<signal type="bluetooth" scenario="Authentication" classOfDevice="512" rssiMin="-10" rssiMaxDelta="-10"/>
</rule>
```

The **classofDevice** attribute defaults Phones and uses the values from the following table

DESCRIPTION	VALUE
Miscellaneous	0
Computer	256
Phone	512
LAN/Network Access Point	768
Audio/Video	1024
Peripheral	1280
Imaging	1536
Wearable	1792
Тоу	2048
Health	2304
Uncategorized	7936

The rssiMin attribute value signal indicates the strength needed for the device to be considered "in-range". The

default value of **-10** enables a user to move about an average size office or cubicle without triggering Windows to lock the device. The **rssiMaxDelta** has a default value of **-10**, which instruct Windows 10 to lock the device once the signal strength weakens by more than measurement of 10.

RSSI measurements are relative and lower as the bluetooth signals between the two paired devices reduces. Therefore a measurement of 0 is stronger than -10, which is stronger than -60, which is an indicator the devices are moving further apart from each other.

#### **IMPORTANT**

Microsoft recommends using the default values for this policy settings. Measurements are relative, based on the varying conditions of each environment. Therefore, the same values may produce different results. Test policy settings in each environment prior to broadly deploying the setting. Use the rssiMIN and rssiMaxDelta values from the XML file created by the Group Policy Management Editor or remove both attributes to use the default values.

#### **IP** Configuration

You define IP configuration signals using one or more ipConfiguration elements. Each element has a string value. IpConfiguration elements do not have attributes or nested elements.

#### IPv4Prefix

The IPv4 network prefix represented in Internet standard dotted-decimal notation. A network prefix that uses the Classless Inter-Domain Routing (CIDR) notation is required as part of the network string. A network port must not be present in the network string. A **signal** element may only contain one **ipv4Prefix** element.

#### Example

<ipv4Prefix>192.168.100.0/24</ipv4Prefix>

The assigned IPv4 addresses in the range of 192.168.100.1 to 192.168.100.254 match this signal configuration.

IPv4Gateway

The IPv4 network gateway represented in Internet standard dotted-decimal notation. A network port or prefix must not be present in the network string. A **signal** element may only contain one **ipv4Gateway** element.

## Example

<ipv4Gateway>192.168.100.10</ipv4Gateway>

IPv4DhcpServer

The IPv4 DHCP server represented in Internet standard dotted-decimal notation. A network port or prefix must not be present in the network string. A **signal** element may only contain one **ipv4DhcpServer** element. **Example** 

<ipv4DhcpServer>192.168.100.10</ipv4DhcpServer>

IPv4DnsServer

The IPv4 DNS server represented in Internet standard dotted-decimal notation. A network port or prefix must not be present in the network string. The **signal** element may contain one or more **ipv4DnsServer** elements. **Example:** 

<ipv4DnsServer>192.168.100.10</ipv4DnsServer>

#### IPv6Prefix

The IPv6 network prefix represented in IPv6 network using Internet standard hexadecimal encoding. A network prefix in CIDR notation is required as part of the network string. A network port or scope ID must not be present in the network string. A **signal** element may only contain one **ipv6Prefix** element.

## Example

<ipv6Prefix>21DA:D3::/48</ipv6Prefix>

#### IPv6Gateway

The IPv6 network gateway represented in Internet standard hexadecimal encoding. An IPv6 scope ID may be present in the network string. A network port or prefix must not be present in the network string. A **signal** element may only contain one **ipv6Gateway** element.

### Example

<ipv6Gateway>21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A%2</ipv6Gateway>

#### IPv6DhcpServer

The IPv6 DNS server represented in Internet standard hexadecimal encoding. An IPv6 scope ID may be present in the network string. A network port or prefix must not be present in the network string. A **signal** element may only contain one **ipv6DhcpServer** element.

#### Example

<ipv6DhcpServer>21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A%2</ipv6DhcpServer

#### IPv6DnsServer

The IPv6 DNS server represented in Internet standard hexadecimal encoding. An IPv6 scope ID may be present in the network string. A network port or prefix must not be present in the network string. The **signal** element may contain one or more **ipv6DnsServer** elements.

#### Example

<ipv6DnsServer>21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A%2</ipv6DnsServer>

## d n s Su ffi x

The fully qualified domain name of your organizations internal dns suffix where any part of the fully qualified domain name in this setting exists in the computer's primary dns suffix. The **signal** element may contain one or more **dnsSuffix** elements.

### Example

<dnsSuffix>corp.contoso.com</dnsSuffix>

### Sample Trusted Signal Congfigurations

These examples are wrapped for readability. Once properly formatted, the entire XML contents must be a single line.

#### Example 1

This example configures an IPConfig signal type using Ipv4Prefix, Ipv4DnsServer, and DnsSuffix elements.

```
<rule schemaVersion="1.0">
<signal type="ipConfig">
<ipv4Prefix>10.10.10.0/24</ipv4Prefix>
<ipv4DnsServer>10.10.0.1</ipv4DnsServer>
<ipv4DnsServer>10.10.0.2</ipv4DnsServer>
<dnsSuffix>corp.contoso.com</dnsSuffix>
</signal>
</rule>
```

This example configures an IpConfig signal type using a dnsSuffix element and a bluetooth signal for phones. This configuration is wrapped for reading. Once properly formatted, the entire XML contents must be a single line. This example implies that either the ipconfig **or** the Bluetooth rule must evaluate to true, for the resulting signal evaluation to be true.

## NOTE

Separate each rule element using a comma.

```
<rule schemaVersion="1.0">
    <signal type="ipConfig">
        <dnsSuffix>corp.contoso.com</dnsSuffix>
        </signal>
    </rule>,
    </rule schemaVersion="1.0">
        <signal type="bluetooth" scenario="Authentication" classOfDevice="512" rssiMin="-10" rssiMaxDelta="-10"/>
        </rule>
```

### Example 3

This example configures the same as example 2 using compounding And elements. This example implies that the ipconfig **and** the Bluetooth rule must evaluate to true, for the resulting signal evaluation to be true.

```
<rule schemaVersion="1.0">
<and>
<signal type="ipConfig">
<dnsSuffix>corp.microsoft.com</dnsSuffix>
</signal>
<signal type="bluetooth" scenario="Authentication" classOfDevice="512" rssiMin="-10" rssiMaxDelta="-10"/>
</and>
</rule>
```

## Deploying Multifactor Unlock

#### IMPORTANT

You need to remove all third party credential providers to ensure users cannot unlock their devices if they do not have the required factors. The fall back options are to use passwords or smart cards (both of which could be disabled as needed).

#### How to configure Multifactor Unlock policy settings

You need a Windows 10, version 1709 workstation to run the Group Policy Management Console, which provides the latest Windows Hello for Business Group Policy settings, which includes muiltifactor unlock. To run the Group Policy Management Console, you need to install the Remote Server Administration Tools for Windows 10. You can download these tools from the Microsoft Download Center. Install the Remote Server Administration Tools for Windows 10 on a computer running Windows 10, version 1709.

Alternatively, you can create copy the .ADMX and .ADML files from a Windows 10, version 1703 to their respective language folder on a Windows Server or you can create a Group Policy Central Store and copy them their respective language folder. See How to create and manage the Central Store for Group Policy Administrative Templates in Windows for more information.

### Create the Multifactor Unlock Group Policy object

The Group Policy object contains the policy settings needed to trigger Windows Hello for Business provisioning and to ensure Windows Hello for Business authentication certificates are automatically renewed.

#### IMPORTANT

- PIN must be in at least one of the groups
- Trusted signals **must** be combined with another credential provider
- You cannot use the same unlock factor to satisfy both categories. Therefore, if you include any credential provider in both categories, it means it can satisfy either category, but not both.
- 1. Start the Group Policy Management Console (gpmc.msc)
- 2. Expand the domain and select the Group Policy Object node in the navigation pane.
- 3. Right-click Group Policy object and select New.
- 4. Type *Multifactor Unlock* in the name box and click **OK**.
- 5. In the content pane, right-click the Multifactor Unlock Group Policy object and click Edit.
- 6. In the navigation pane, expand **Policies** under **Computer Configuration**.
- 7. Expand Administrative Templates > Windows Component, and select Windows Hello for Business.



8. In the content pane, double-click **Configure device unlock factors**. Click **Enable**. The **Options** section populates the policy setting with default values.

Se Configure device unlock factors – 🗖 🗙				x					
Configure device	unlock factors			Previous Setting	j Ne	ext Setting	]		
<ul> <li>Not Configured</li> <li>Enabled</li> <li>Disabled</li> </ul>	Comment: Supported on:	At least Window	ws Server or \	Vindows 10					< >
Options:			Help:						
First unlock factor cree {D6886603-9D2F-4EB Second unlock factor {27FBDB57-B613-4AF Signal rules for device <rule schemaversion<="" td=""><td>edential providers 2-B667-1971041FA credential provide 2-9D7E-4FA7A66C e unlock = "1.0"&gt; <signal td="" ty<=""><td>91 ers 2 P</td><td>Configure such as fact first and se specified a a comma s signal type If you enab factor from If you disal continue to For more in linkid=849</td><td>a comma separate e and fingerprint p cond unlock facto s one of the unlock separated list of sig to be verified. The this policy settin n each list to succe ble or do not confi o unlock with exist nformation see: htt 684</td><th>d list of c provider G rs. If the t k factors, nal rules ng, the us ssfully un gure this ing unloc tps://go.r</th><th>redential pro GUIDs, to be u rrusted signal you should a in the form o er will have t ilock. policy setting k options. nicrosoft.cor</th><th>vider ( ised a: provi lso co f xml : o use g, user n/fwli</th><th>3UIDs, ; the der is nfigur for eac one s can nk/?</th><td>e :h</td></signal></td></rule>	edential providers 2-B667-1971041FA credential provide 2-9D7E-4FA7A66C e unlock = "1.0"> <signal td="" ty<=""><td>91 ers 2 P</td><td>Configure such as fact first and se specified a a comma s signal type If you enab factor from If you disal continue to For more in linkid=849</td><td>a comma separate e and fingerprint p cond unlock facto s one of the unlock separated list of sig to be verified. The this policy settin n each list to succe ble or do not confi o unlock with exist nformation see: htt 684</td><th>d list of c provider G rs. If the t k factors, nal rules ng, the us ssfully un gure this ing unloc tps://go.r</th><th>redential pro GUIDs, to be u rrusted signal you should a in the form o er will have t ilock. policy setting k options. nicrosoft.cor</th><th>vider ( ised a: provi lso co f xml : o use g, user n/fwli</th><th>3UIDs, ; the der is nfigur for eac one s can nk/?</th><td>e :h</td></signal>	91 ers 2 P	Configure such as fact first and se specified a a comma s signal type If you enab factor from If you disal continue to For more in linkid=849	a comma separate e and fingerprint p cond unlock facto s one of the unlock separated list of sig to be verified. The this policy settin n each list to succe ble or do not confi o unlock with exist nformation see: htt 684	d list of c provider G rs. If the t k factors, nal rules ng, the us ssfully un gure this ing unloc tps://go.r	redential pro GUIDs, to be u rrusted signal you should a in the form o er will have t ilock. policy setting k options. nicrosoft.cor	vider ( ised a: provi lso co f xml : o use g, user n/fwli	3UIDs, ; the der is nfigur for eac one s can nk/?	e :h
					ОК	Cancel		Appl	у

- 9. Configure first and second unlock factors using the information in the Configure Unlock Factors section.
- 10. If using trusted signals, configure the trusted signals used by the unlock factor using the information in the Configure Signal Rules for the Trusted Signal Credential Provider section.
- 11. Click **Ok** to close the **Group Policy Management Editor**. Use the **Group Policy Management Console** to deploy the newly created Group Policy object to your organization's computers.

## Troubleshooting

Mulitfactor unlock writes events to event log under **Application and Services** Logs\Microsoft\Windows\HelloForBusiness with the category name Device Unlock.

## **Events**

EVENT ID	DETAILS
3520	Unlock attempt initiated
5520	Unlock policy not configured
6520	Warning event
7520	Error event
8520	Success event