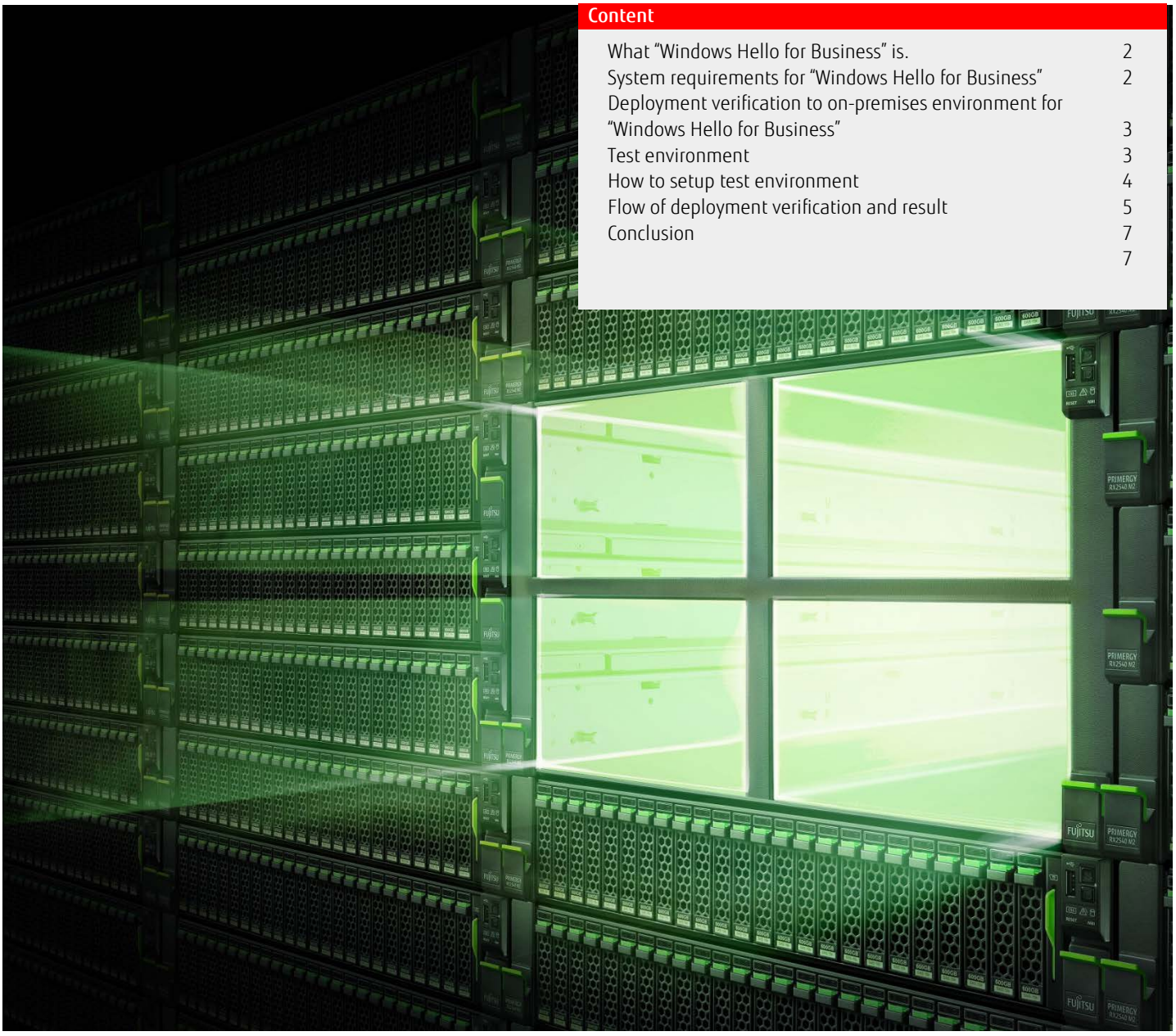
"Windows Hello for Business" makes IT systems more secure and simple by providing "Password-Free Login".

On-Premise deployment using Fujitsu Server PRIMERGY



Content

Introduction

Information leakage has serious effects on company and it can be severe business damage for the company. Therefore, risk management for information security is very important. Today many IT systems using ID and password for user authentication. However there are challenges in authentication via ID and password. For example, vulnerability of IT systems may surface if some users set an easy password. On the other hand, management costs of user support may increase if users set a complicated password and forget it.

To solve these challenges, you can use biometric authentication called "Windows Hello for Business*1" as one of the security feature of Windows Server 2016 and Windows 10. The feature will be available with the update which will be available in future*2. In this paper, Fujitsu used a private module*2 which is provided by Microsoft.

Fujitsu verified deployment of the feature within "on-premises" environment using Fujitsu Server PRIMERGY RX2540 M2 and LIFEBOOK E736.

NOTE:

*1 Windows 10 has a feature called "Windows Hello" which provides biometric authentication, however, it requires user login by using "Azure AD" or "Microsoft account". It could not login to AD DS (Active Directory Domain Service) which is used by company conventionally.

*2 Update program is pre-release version provided by Microsoft. It may not work the way a final version of the module will. Microsoft may change it for the final, commercial version. It is released as KB4022723 (June 27, 2017).

What "Windows Hello for Business" is.

Conventional authentication and management via ID and password have some challenges below.

- User may set an easy password which may cause potential vulnerability.
- User may set complicated password and forget it, or put a memo which includes written password besides their PC in order not to forget it.
- User may set the same password across some systems.
- User's password leaked by phishing or user's password leaked by server hacking.

For years these challenges have annoyed IT administrators who manage user accounts in their company. To solve above challenges, you can use biometric authentication solution called "Windows Hello for Business" as one of the security feature of Windows Server 2016 and Windows 10.

With "Windows Hello for Business", you can use biological information such as fingerprint, iris and face instead of password.

At the time of Windows Server 2016 released, Azure AD was a mandatory requirement for "Windows Hello for Business". However you will be able to configure "Windows Hello for Business" without Azure AD in future. You can deploy secure IT system by using biometric authentication which is integrated with on-premises AD accounts.

System requirements for "Windows Hello for Business"

System requirements for "Windows Hello for Business" are as follows.

Table 1 System requirements for "Windows Hello for Business*3"

Roll	System requirements	
Active Directory Domain Services	Key-based authentication	Windows Server 2016
	Certificate-based authentication	Windows Server 2008 R2 or later + Windows Server 2016 schema extension
	Domain Functional Level / Forest Functional Level	Windows Server 2008 R2 or later
Active Directory Certificate Services	Windows Server 2012 or later	
Active Directory Federation Services	Windows Server 2016 + **update program (pre-release module)*4**	
Client	Windows 10 + Creators Update	

NOTE:

*3 There are 2 kinds of authentication, key-based or certificate-based. The requirements depend on the authentication which you use.

*4 Update program is pre-release version provided by Microsoft. It may not work the way a final version of the module will. Microsoft may change it for the final, commercial version. It is released as KB4022723 (June 27, 2017).

Deployment verification to on-premises environment for "Windows Hello for Business"

Fujitsu verified deployment of the feature within "on-premises" environment using Fujitsu Server PRIMERGY RX2540 M2 and LIFEBOOK E736 with the cooperation of Microsoft.

Test environment

For the deployment verification, you can use key-based and fingerprint authentication as biometric authentication. "Windows Hello for business" requires Active Directory Domain Services ("AD DS"), Active Directory Certificate Services ("AD CS") and Active Directory Federation Services ("AD FS") roles of Windows Server 2016. To create the test environment, you can prepare one virtual machine for each role. For client, you can use LIFEBOOK E736 which equipped fingerprint sensor and supported Windows Hello. Figure 1 below shows the test environment. In addition, Table 2 and Table 3 shows configuration of server, client and virtual machines.

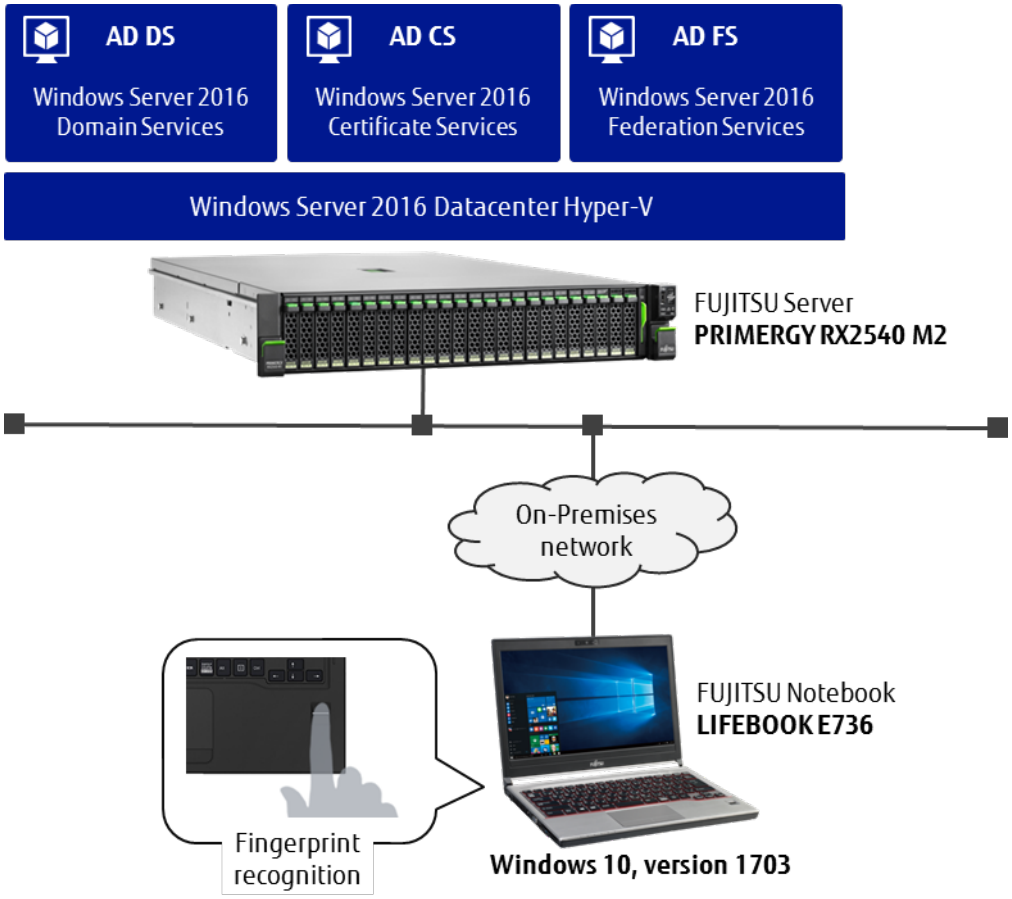


Figure 1 diagram of test environment

Table 2 configuration of physical server/client

Architecture	Physical server	Client
Hardware	PRIMERGY RX2540 M2	LIFEBOOK E736
CPU	Intel Xeon E5-2680 v4	Intel Celeron 3955U
Memory	128 GB	8 GB
HDD	600 GB × 16	500 GB
OS	Microsoft Windows Server 2016 Datacenter	Windows 10 Creators Update, version 1607*5
KB	KB4015438 (March 20, 2017)	KB4016240 (April 25, 2017)

NOTE:

*5 Edition is Windows 10 Pro

Table 3 configuration of virtual machine

Configuration	AD DS	AD CS	AD FS
Generation	Generation 2	Generation 2	Generation 2
CPU	4 core	4 core	4 core
Memory	4 GB	4 GB	4 GB
vHDD	Variable capacity VHDX 127 GB	Variable capacity VHDX 127 GB	Variable capacity VHDX 127 GB
OS	Microsoft Windows Server 2016 Datacenter	Microsoft Windows Server 2016 Datacenter	Microsoft Windows Server 2016 Datacenter
KB	KB4019472 (May 9, 2017)	KB4019472 (May 9, 2017)	KB4019472 (May 9, 2017) **Pre-released module*6**
Roles & Features	Active Directory Domain Services	Active Directory Certificate Services	Active Directory Federation Services

NOTE:

*6 The module is pre-released version provided by Microsoft. It may not work the way a final version of the module will. Microsoft may change it for the final, commercial version. It is released as KB4022723 (June 27, 2017).

How to setup test environment

Outline of test environment is as follows:

<Preparation>

1-1. [on AD DS] Install AD DS
1-2. [on AD DS] Promote the server to a domain controller
1-3. [on AD CS] Install AD CS
1-4. [on AD CS] Configure Enterprise CA
1-5. [on AD FS] Install AD FS
1-6. [on client] Join the domain

<Set up key-based authentication>

2-1. [on AD CS] Set up certificate template for AD FS server
2-2. [on AD DS] Issue KDC certificate
2-3. [on AD FS] Issue AD FS server certificate
2-4. [on AD DS] Set up gMSA (Group Managed Service Accounts)
2-5. [on AD FS] Configure AD FS
2-6. [on AD CS] Configure DNS (Make FS record which configured at 2-5)
2-7. [on AD CS] Add AD FS service account to Key Admins group
2-8. [on AD FS] Activate Device Registration
2-9. [on AD FS] Configure multi factor authentication
=> You can make and use an authentication provider. For this test, Fujitsu customized it based on Microsoft's information. See https://blogs.technet.microsoft.com/cloudpfe/2014/02/01/how-to-create-a-custom-authentication-provider-for-active-directory-federation-services-on-windows-server-2012-r2-part-1/
2-10. [on AD DS] Configure GPO for "Windows Hello for Business"

Flow of deployment verification and result

"Windows Hello for Business" adopts the followings:

1) **two-factor authentication** which authenticates the device registered for AD DS and the PIN registered for client or biological information, and
2) **NGC (Next Generation Credential)** which authenticates private key registered for TPM and public key registered for AD DS (PIN or biometric authentication is used to unlock the TPM).

Key-based authentication flow of on-premises environment is as follows. User needs to register device, PIN and biological information.

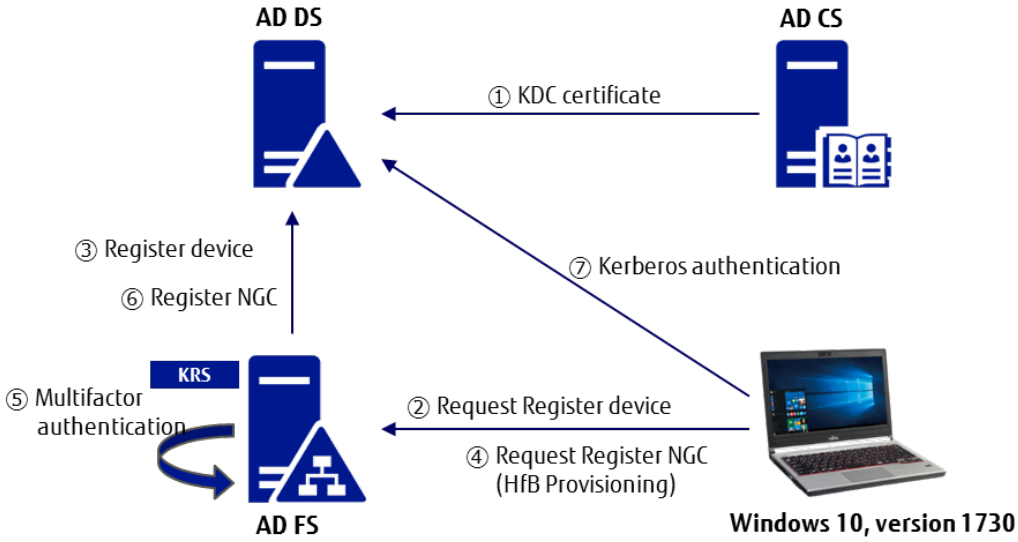


Figure 2 Key-based authentication flow with on-premises environment

At first, you can check the processing of device registration. Since you already setup required configuration in [4.2 How to setup test environment], only required task is to login as a domain user to LIFEBOOK E736 which has already joined the domain. After login to the client, you can input commands [dsregcmd /status] in command prompt. If the device has been registered for AD DS then the value of [EnterpriseJoined] showed "YES". It takes several minutes after first login to the client (see Figure 3).
In our test, the device registration has been started after login to the client and it ended normally.

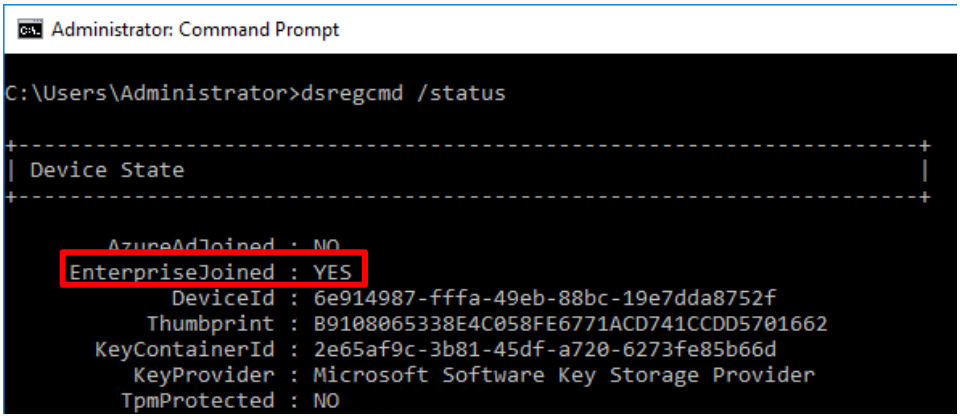


Figure 3 Execution result of command [dsregcmd /status]

Second, you can check the processing of PIN and biological information registration. Once you logout the client, LIFEBOOK E736, and login with domain account which is enabled "Windows Hello for Business" at [2-10] of [4.2 How to setup test environment]. At the moment, neither PIN nor biological information have been registered, therefore, you need to input password string to login to the client (see Figure 4).
After login to the client, you can set up PIN through the screen showed "Your organization requires Windows Hello" (see Figure 5).

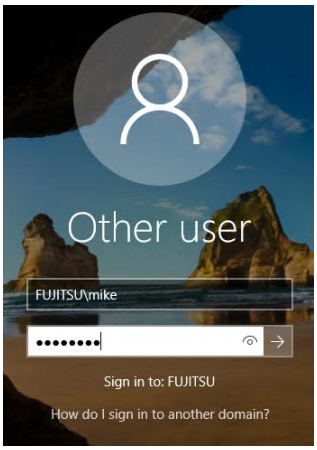


Figure 4 Input password conventionally

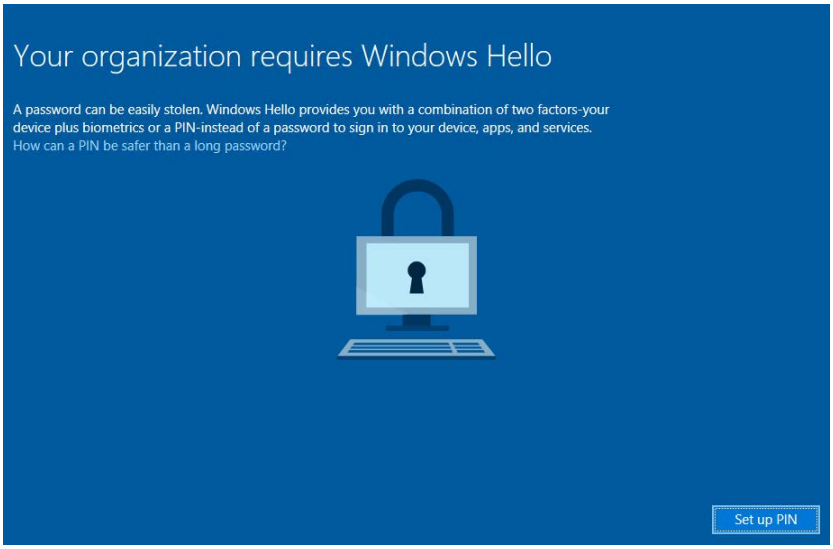


Figure 5 Display shows Windows Hello is required

After Click [Set up PIN], the client starts to communicate with AD FS. In this deployment verification, you can use a customer authentication provider for this test (see [2-9] of [4.2 How to setup test environment]). Then you can register the correct authentication PIN on dialog (see Figure 6). You can login to domain environment and desktop screen will be displayed.

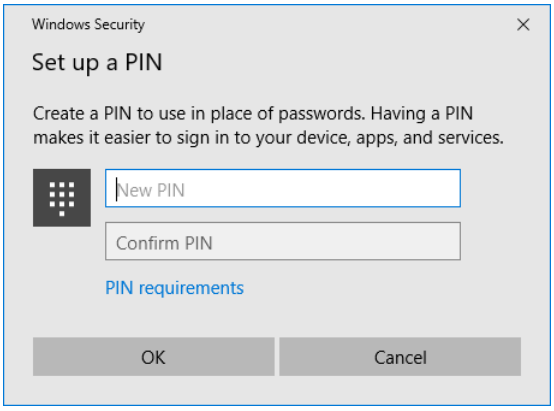


Figure 6 PIN setup dialog

The registration for device and PIN were completed. So after logout the user, you can confirm that the user can select PIN instead of password at login prompt (see Figure 7). In addition, you made sure that we could login to the domain environment using PIN which we have registered at Figure 6.

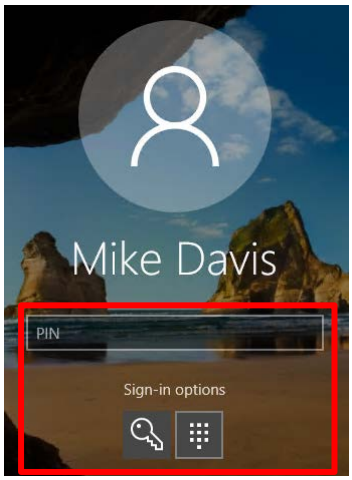


Figure 7 PIN is selectable

Finally, regarding fingerprint registration, this is as well as Windows Hello. You can register fingerprint at [Sign in options] => [Windows Hello] below (see Figure 8).

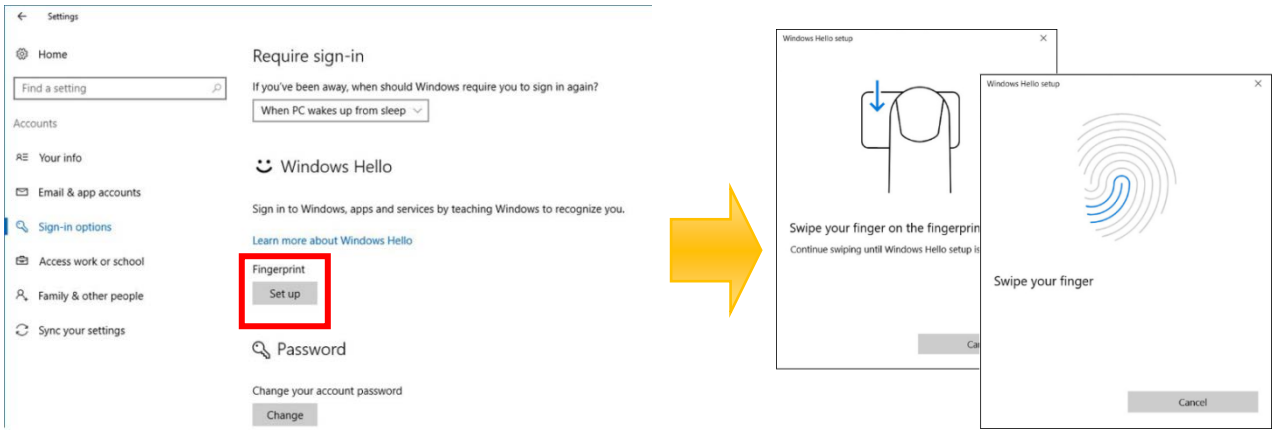


Figure 8 Fingerprint registration

By previous configuration procedures, registration of device, PIN and biological information (fingerprint) have been completed (see Figure 9). Once you logout and check the login screen, you were able to select fingerprint authentication. From the next time, you can login to the domain environment with fingerprint information.

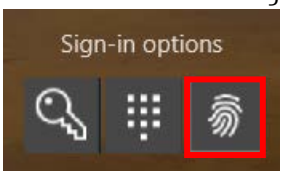


Figure 9 Fingerprint authentication is selectable

Conclusion

Microsoft's latest technology is available through Windows Server 2016 and Windows 10 updates. With the cooperation of Microsoft, Fujitsu evaluated the pre-released version of "Windows Hello for Business" which brings secure and easy-to-manage solution for on-premises environment through biometric authentication. Fujitsu confirmed that with pre-release module you can successfully deploy "Windows Hello for Business" in on-premises environment using PRIMERGY RX2540 M2 and LIFEBOOK E736.

Fujitsu is conducting early evaluation of the latest Microsoft technologies with Fujitsu Server PRIMERGY and PRIMEQUEST to make sure our servers correctly work with Windows and to provide solution based on the latest Windows.

Reference URL

FUJITSU Server PRIMERGY	http://www.fujitsu.com/global/products/computing/servers/primergy/
FUJITSU Server PRIMEQUEST systems	http://www.fujitsu.com/global/products/computing/servers/mission-critical/
FUJITSU Notebook LIFEBOOK	http://www.fujitsu.com/global/products/computing/pc/notebooks/

Contact
FUJITSU Limited
Address: Shiodome City Center, 5-2, Higashi-shimbashi 1-chome, Minato-ku, Tokyo 105-7123, Japan
Website: www.fujitsu.com/global/