Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

# 10993B

# Integrating On-Premises Identity Infrastructure with Microsoft Azure

*Companion Content*

Product Number: 10993B

Released: 12/2018

**MICROSOFT LICENSE TERMS**
**MICROSOFT INSTRUCTOR-LED COURSEWARE**

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to your use of the content accompanying this agreement which includes the media on which you received it, if any. These license terms also apply to Trainer Content and any updates and supplements for the Licensed Content unless other terms accompany those items. If so, those terms apply.

**BY ACCESSING, DOWNLOADING OR USING THE LICENSED CONTENT, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT ACCESS, DOWNLOAD OR USE THE LICENSED CONTENT.**

**If you comply with these license terms, you have the rights below for each license you acquire.**

## 1. DEFINITIONS.

a. "Authorized Learning Center" means a Microsoft IT Academy Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.

b. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.

c. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.

d. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of a MPN Member, or (iii) a Microsoft full-time employee.

e. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.

f. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.

g. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals and developers on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics or Microsoft Business Group courseware.

h. "Microsoft IT Academy Program Member" means an active member of the Microsoft IT Academy Program.

i. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.

j. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals and developers on Microsoft technologies.

k. "MPN Member" means an active Microsoft Partner Network program member in good standing.

l. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.

m. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.

n. "Trainer" means (i) an academically accredited educator engaged by a Microsoft IT Academy Program Member to teach an Authorized Training Session, and/or (ii) a MCT.

o. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.

**2. USE RIGHTS**. The Licensed Content is licensed not sold. The Licensed Content is licensed on a ***one copy per user basis***, such that you must acquire a license for each individual that accesses or uses the Licensed Content.

2.1 Below are five separate sets of use rights. Only one set of rights apply to you.

a. **If you are a Microsoft IT Academy Program Member:**
   i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
   ii. For each license you acquire on behalf of an End User or Trainer, you may either:
      1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
      2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
      3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

      **provided you comply with the following:**
   iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
   iv. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
   v. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
   vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,

vii. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,

viii. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and

ix. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

b. **If you are a Microsoft Learning Competency Member**:

i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

ii. For each license you acquire on behalf of an End User or Trainer, you may either:

1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
3. you will provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

**provided you comply with the following**:

iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,

iv. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,

v. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,

vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for your Authorized Training Sessions,

viii. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,

ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and

x. you will only provide access to the Trainer Content to Trainers.

c. **If you are a MPN Member**:

  i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

  ii. For each license you acquire on behalf of an End User or Trainer, you may either:

    1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
    2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
    3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content,

  **provided you comply with the following**:

  iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,

  iv. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,

  v. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

  vi. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,

  vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,

  viii. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,

  ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and

  x. you will only provide access to the Trainer Content to Trainers.

d. **If you are an End User:**

  For each license you acquire, you may use the Microsoft Instructor-Led Courseware solely for your personal training use. If the Microsoft Instructor-Led Courseware is in digital format, you may access the Microsoft Instructor-Led Courseware online using the unique redemption code provided to you by the training provider and install and use one (1) copy of the Microsoft Instructor-Led Courseware on up to three (3) Personal Devices. You may also print one (1) copy of the Microsoft Instructor-Led Courseware. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

e. **If you are a Trainer.**

  i. For each license you acquire, you may install and use one (1) copy of the Trainer Content in the form provided to you on one (1) Personal Device solely to prepare and deliver an Authorized Training Session or Private Training Session, and install one (1) additional copy on another Personal Device as a backup copy, which may be used only to reinstall the Trainer Content. You may not install or use a copy of the Trainer Content on a device you do not own or control. You may also print one (1) copy of the Trainer Content solely to prepare for and deliver an Authorized Training Session or Private Training Session.

ii. You may customize the written portions of the Trainer Content that are logically associated with instruction of a training session in accordance with the most recent version of the MCT agreement. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of "*customize*" refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

2.2 **Separation of Components.** The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.

2.3 **Redistribution of Licensed Content**. Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.

2.4 **Third Party Notices**. The Licensed Content may include third party code tent that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code ntent are included for your information only.

2.5 **Additional Terms**. Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

**3. LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY.** If the Licensed Content's subject matter is based on a pre-release version of Microsoft technology ("**Pre-release**"), then in addition to the other provisions in this agreement, these terms also apply:

a. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.

b. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.

c. **Pre-release Term**. If you are an Microsoft IT Academy Program Member, Microsoft Learning Competency Member, MPN Member or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest ("**Pre-release term**"). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

4. **SCOPE OF LICENSE**. The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:
   - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
   - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
   - modify or create a derivative work of any Licensed Content,
   - publicly display, or make the Licensed Content available for others to access or use,
   - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
   - work around any technical limitations in the Licensed Content, or
   - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.

5. **RESERVATION OF RIGHTS AND OWNERSHIP**. Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.

6. **EXPORT RESTRICTIONS**. The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

7. **SUPPORT SERVICES**. Because the Licensed Content is "as is", we may not provide support services for it.

8. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.

9. **LINKS TO THIRD PARTY SITES**. You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.

10. **ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.

11. **APPLICABLE LAW.**
    a. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.

12. **LEGAL EFFECT**. This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

13. **DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**

14. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

    This limitation applies to

    - anything related to the Licensed Content, services, content (including code) on third party Internet sites or third-party programs; and
    - claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

    It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

**Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.**

**Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.**

**EXONÉRATION DE GARANTIE.** Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

**LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES.** Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.
Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s’applique également, même si Microsoft connaissait ou devrait connaître l’éventualité d’un tel dommage. Si votre pays n’autorise pas l’exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l’exclusion ci-dessus ne s’appliquera pas à votre égard.

**EFFET JURIDIQUE.** Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d’autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Revised July 2013

# Module 1

## Introducing Azure AD

### Contents:

# Lesson 1
# Overview of Azure AD

## Contents:

## Question and Answers

**Question:** Which of the following are characteristics of Azure AD?

( ) Is multitenant by design

( ) Contains organizational units

( ) Uses LDAP for directory lookups

( ) Supports Group Policy

( ) Offers native support for multi-factor authentication

**Answer:**

(√) Is multitenant by design

( ) Contains organizational units

( ) Uses LDAP for directory lookups

( ) Supports Group Policy

(√) Offers native support for multi-factor authentication

**Feedback:**

Unlike AD DS, Azure AD is multitenant by design. It does not support organizational units (OUs). It relies on internet-friendly protocols for directory lookups (Graph API over HTTPS) rather than Lightweight Directory Access Protocol (LDAP). It does not support Group Policy for management of its domain-joined devices; you can use a mobile device management solution, such as Microsoft Intune, instead. It offers native support for multi-factor authentication.

## Resources

## Azure AD as a directory service for cloud apps

**Additional Reading:** For more information, refer to How to configure your App Service application to use Azure Active Directory login: https://aka.ms/W0xp0l.

# Lesson 2
# Implementing and configuring Azure AD

## Contents:

## Question and Answers

**Question:** How will your organization use Azure AD?

**Answer:** Answers will vary, but might include:

- To secure access to Azure-based services.
- To delegate management of Azure-based services.
- To enhance authentication security by using multi-factor authentication.
- To provide SSO functionality for access to SaaS applications.

As an identity and access management solution, Azure AD provides a range of features that integrate with other cloud and on-premises services. It is easy to take advantage of Azure AD to authenticate Azure web apps, Azure PaaS cloud services, and web applications running in Azure virtual machines.

Similarly, you can delegate management of Azure AD resources that are accessible via the Azure Portal by using Role-Based Access Control (RBAC). You can also use Azure AD accounts when designating co-administrators of a subscription.

Azure AD offers additional authentication enhancements, including multi-factor authentication and SSO for access to SaaS applications or cloud-based Web applications, including both Azure portals. In addition, directory synchronization with AD DS makes it possible to sign in to cloud-based applications by using on-premises credentials.

For example, an organization that deploys a web app for sales personnel to Azure can use Azure AD to authenticate user requests to the app and can choose to implement multi-factor authentication when sales personnel access the app via a browser or a mobile device.

## Demonstration: Configuring an Azure AD tenant

### Demonstration Steps

1. On **LON-CL1**, open the Microsoft Edge browser.
2. In the Microsoft Edge window, go to https://portal.azure.com. If prompted, sign in with your Office 365 account that you created. If the **Stay signed in?** prompt appears, click **No**.

**Note:** This is the account that you created in Task 2 of the first exercise in the lab.

3. If the **Welcome to Microsoft Azure** window appears, click **Maybe later**.
4. On the **Microsoft Azure** page, click **Azure Active Directory** in the left navigation pane. This will open the adatum Azure Active Directory page.
5. In the middle navigation pane, click **Overview**, and then in the right pane, in the **Sign-ins** section, click **Start a free trial**.
6. On the **Activate** page, in the **ENTERPRISE MOBILITY + SECURITY E5** section, click **Free trial**, and then click **Activate**. Close the **Activate Enterprise Mobility + Security E5 trial** and **Activate** windows.
7. Click **Azure Active Directory** in the left navigation page.
8. Click **Licenses** in the middle navigation pane, and then click **All products** in the middle pane.
9. Ensure that you see licenses for Enterprise Mobility + Security E5 and Office 365 Enterprise E5. Close the **Licenses – All products** page.

10. In the Microsoft Edge browser window, in the Azure portal, click **Azure Active Directory**, and then click **Custom domain names**.

11. Click **Add custom domain**.

12. On the **Custom domain name** page, in the **Custom domain name** box, type ***yourdomain*.*hostdomain*.com**. Click **Add Domain**.

**Note: yourdomain** is the domain name assigned to you by the lab-hosting provider. If you are not sure about your domain name, ask your instructor.

13. On the ***yourdomain*.*hostdomain*.com** page, in the **RECORD TYPE** box, note the options for **RECORD TYPE**: **TXT** and **MX**.

# Lesson 3
# Managing Azure AD

## Contents:

## Question and Answers

**Question:** You can use a single account to manage multiple Azure AD tenants.

( ) True

( ) False

**Answer:**

(√) True

( ) False

**Feedback:**

You can manage all existing Azure AD directories, such as Azure, Office 365, and Intune, by using the same account—as long as the same account is a Global Administrator for all the directories.

## Resources

## User roles in Azure AD

**Additional Reading:** For more information, refer to Assigning administrator roles in Azure Active Directory: https://aka.ms/wxqeod.

## Demonstration: Creating and configuring users in Azure AD

### Demonstration Steps

1. On the **adatum – Custom domain names** page, click **Users** in the middle pane, click **All users**, and then click **New user**.
2. In the **User** dialog box, enter the following:
   a. Name: **Edmund Reeve**
   b. User Name: **ereeve@adatumyyxxxx.onmicrosoft.com**
3. Click **Show Password**, note and write down or copy the value for **Password**, and then click **Create**.
4. On the **adatum – Custom domain names** page, click **Users** in the middle pane, click **All users**, and then click **New user**.
5. In the **User** dialog box, enter the following:
   a. Name: **Miranda Snider**
   b. User Name: **msnider@adatumyyxxxx.onmicrosoft.com**
   c. Click **Directory role**, select **Global administrator**, and then click **Ok**.
6. Click **Show Password**, note and write down the value for **Password**, and then click **Create**.
7. In the **Users– All users** window, click **Edmund Reeve**.
8. In the **Edmund Reeve** window, click **Profile**. In the right pane, in the **Settings** section, click **Edit**, and then select your country/region in the **Usage location** drop-down box. If your country/region is not listed, select **United States**, and then click **Save**. Close the **Edmund Reeve – Profile** page.
9. Repeat steps 7 and 8 for user account **Miranda Snider**.
10. Close the **Users– All users** window, and then click **Licenses** in the middle pane.
11. Click **All products**, and then select **Enterprise Mobility + Security E5**. Click **Assign**.

12. Click **Users**, select all three users, and then click **Select**.
13. Click **Assign**.

# Module Review and Takeaways

## Review Question

**Question:** What are some benefits of hosting part or all of an organization's Active Directory infrastructure in Azure?

**Answer:** Benefits include:

- Centralized identity management.
- SSO across applications, including those that are hosted outside of the organization.
- Scalability and availability without additional infrastructure.
- Built-in disaster recovery.
- The integration of non-Microsoft identity providers, if required.
- Easily integrated with any existing Office 365, Intune, and Microsoft Dynamics CRM Online accounts.
- Hybrid scenarios also enable some resources to be secured on-premises, with others in the cloud.

# Lab Review Questions and Answers

## Lab: Creating and managing an Azure AD tenant

## Question and Answers

**Question:** What role should you assign to a user account in the Azure AD directory instance to enable the user to fully manage all of its objects?

> **Answer:** You should assign the Global Administrator role to the user account. The Global Administrator role grants full control of the Azure AD tenant where this role exists. Note that this role does not grant any access rights to Azure subscription resources.

**Question:** What account should you use to manage your Azure AD tenant?

> **Answer:** You should use your organizational account that you created during provisioning of the Azure AD tenant. Alternatively, you can use an account to which you delegate rights.

# Module 2

## Integrating on-premises Active Directory with Azure

### Contents:

# Lesson 1
# Extending an on-premises Active Directory domain to Azure

## Contents:

## Question and Answers

**Question:** When you deploy a domain controller from your local AD DS in the Azure, do you use Azure AD?

> **Answer:** In this scenario, Azure AD is not used. The local AD DS database is replicated to the domain controller deployed in Azure.

# Lesson 2
# Directory synchronization overview

## Contents:

## Question and Answers

**Question:** When you implement directory synchronization with password sync, what method is used to synchronize the user's password?

> **Answer:** Directory synchronization with password synchronization copies password hashes, instead of actual passwords, to Azure AD.

**Question:** When you implement directory synchronization, user accounts and groups are moved from your local AD DS to the Azure AD.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:**
>
> Directory synchronization does not move objects. It copies objects from local AD DS with a subset of their attributes, and it creates new objects in Azure AD.

## Resources

## What is pass-through authentication?

**Additional Reading:** To learn more about modern authentication in Office apps, refer to "How modern authentication works for Office 2013 and Office 2016 client apps" at https://aka.ms/AA21ej2.

**Additional Reading:** For more information, refer to "User sign-in with Azure Active Directory Pass-through Authentication" at https://aka.ms/lusqtt.

# Lesson 3
# Implementing and configuring directory synchronization

## Contents:

## Question and Answers

**Question:** If you want to have SSO for both cloud-based and on-premises services, what do you need to deploy?

( ) Azure monitoring tools

( ) AD FS

( ) Azure AD Connect

( ) Office 365

**Answer:**

( ) Azure monitoring tools

(√) AD FS

(√) Azure AD Connect

( ) Office 365

**Feedback:**

Deploy both AD FS and Azure AD Connect.

## Resources

## What is Azure AD Connect?

**Additional Reading:** For more information, refer to Azure AD Connect: Version release history at https://aka.ms/AA30hdg.

## Preparing on-premises Active Directory for directory synchronization

**Additional Reading:** For more information, refer to “Azure AD Connect sync: Attributes synchronized to Azure Active Directory“ at https://aka.ms/AA30p1z.

**Additional Reading:** To download the IdFix Directory Synchronization Error Remediation Tool, refer to http://aka.ms/xp2jdy.

**Additional Reading:** The CodePlex download link for Active DirectoryModify.NET is: http://aka.ms/j6168k.

## Installing and configuring directory synchronization by using Azure AD Connect

**Additional Reading:** For more information, refer to “Prerequisites for Azure AD Connect” at https://aka.ms/AA30p20.

## Demonstration: Implementing directory synchronization by using the Azure AD Connect custom wizard

### Demonstration Steps

1. On **LON-DS1**, download and run Azure AD Connect setup from **http://www.microsoft.com/en-us/download/details.aspx?id=47594**.
2. Choose to customize the setup process.
3. Select **Password Synchronization** as the setup mode.
4. Use **SYNC@*yourdomain*.onmicrosoft.com** to connect to Azure AD and use **Adatum\administrator** to connect to the local AD DS.
5. Ensure that your custom domain is listed as verified.
6. Choose to synchronize **Computers**, **IT**, **Managers**, **Marketing**, **Research**, and **Sales** to Azure AD.
7. Wait while Azure AD Connect performs the initial synchronization.
8. Sign in to the Microsoft Azure portal, and then verify that synchronization is complete by ensuring that the synchronized objects are present on the **USERS** tab.
9. On **LON-DS1**, open the Synchronization Service Manager, and then show the completed synchronization tasks.

# Lesson 4
# Managing synchronized directories

## Contents:

## Question and Answers

**Question:** What feature do you need to configure so that objects are synchronized from Azure AD to your local AD DS?

> **Answer:** You need to deploy writeback functionalities. Currently, you can use password writeback, groups writeback, and devices writeback.

## Resources

## Modifying directory synchronization scope

**Additional Reading:** For more information, refer to "Azure AD Connect sync: Configure Filtering” at https://aka.ms/AA30hdj.

## Demonstration: Modifying options for directory synchronization

### Demonstration Steps

1. On **LON-DS1**, configure the Active Directory Connector in Synchronization Service Manager for the **Research** OU.
2. On **LON-DS1**, use the Synchronization Rules Editor to configure a filter on the inbound synchronization rule with the following settings:
   - Name: **In from AD – User DoNotSyncFilter**
   - Connected System: **Adatum.com**
   - CS Object Type: **User**
   - Metaverse Object Type: **Person**
   - Link Type: **Join**
   - Precedence: **50**
   - Scoping filter:
     - Attribute: **MSDS-cloudExtensionAttribute15**
     - Operator: **EQUAL**
     - Value: **NoSync**
   - Transformation:
     - FlowType: **Constant**
     - Target Attribute: **cloudFiltered**
     - Source: **True**
3. Use Windows PowerShell to start the synchronization by executing the following command:

```
Start-ADSyncSyncCycle –PolicyType Initial
```

# Module Review and Takeaways

## Best Practices

- Always plan on how you want to extend your Active Directory functionality.
- Avoid using separate credentials for cloud resources.
- For simple deployments, use the Express installation option in Azure AD Connect.
- To establish two-way sync, use writeback functionalities.
- Keep credentials for the sync account in a secure place.

## Review Question

**Question:** What tools should you use to resolve potential attribute issues in AD DS before implementing directory synchronization?

> **Answer:** You can use the IdFix and ADModify.NET tools.

## Tools

- Azure AD Connect
- IdFix
- ADModify.NET
- Azure Management portal

# Lab Review Questions and Answers

## Lab: Implementing directory synchronization

## Question and Answers

**Question:** What was the purpose of adding new UPN to users locally?

> **Answer:** You added another UPN in your local AD DS so that you can use same UPN format when signing in locally and to cloud resources.

**Question:** What are some benefits of using filtering options in Azure AD Connect?

> **Answer:** Filtering makes synchronization more secure, with no forgotten accounts in online services, therefore providing a smaller attack surface. Filtering can also help you limit the number of objects, which in turn can help you minimize the size of your Azure AD Connect database.

# Module 3

## Using Azure AD as a directory service in hybrid environments

### Contents:

# Lesson 1
# Azure AD as a directory service for on-premises environments

## Contents:

## Question and Answers

**Question:** What service should you consider if you want to have the same features in Azure AD that you have in your on-premises AD DS?

**Answer:** You should consider Azure AD Domain Services.

**Question:** Which operating systems can join Azure AD?

( ) Windows 8

( ) Windows 8.1

( ) Windows 10

( ) Windows 7

( ) Windows 10 Mobile

**Answer:**

( ) Windows 8

( ) Windows 8.1

(√) Windows 10

( ) Windows 7

(√) Windows 10 Mobile

**Feedback:**

Windows 10 and Windows 10 Mobile.

## Resources

## What is Azure AD Domain Services?

**Additional Reading:** For more information, refer to "Azure Active Directory (AD) Domain Services" at https://aka.ms/AA31z7k.

## Demonstration: Joining Windows 10 clients to Azure AD

### Demonstration Steps

1. On **LON-CL2**, ensure that you are signed in as the local administrator.
2. Click the **Start** menu, click **Settings**, and then click **System**.
3. In the **System** window, in the navigation pane, click **About**, and then click **Connect to work or school**.
4. On the **Connect to work or school** page, click **Connect**.
5. On the **Set up a work or school account** page, click **Join this device to Azure Active Directory**.
6. On the **Let's get you signed in** page, type **Annie@*yourdomain*.hostdomain.com** for the username, and click **Next**. Type **Pa55w.rd** for the password, and then click **Sign in**.
7. At the **Make sure this is your organization** prompt, click **Join**, click **Done**, and then close the **Settings** window.
8. Restart **LON-CL2**.

9. When the computer restarts, click **Other user** on the sign-in screen.
10. Sign in as **Annie@*yourdomain*.hostdomain.com** with the password **Pa55w.rd**.
11. On the **Your organization requires Windows Hello** page, click **Set up PIN**.
12. Close the **Help us protect your account** page.
13. On the **Something went wrong** page, click **Skip for now.**
14. Ensure that you are signed in.

# Lesson 2
# Configuring SSO with Azure AD

## Contents:

## Question and Answers

**Question:** How can you verify if your local federation service on **fs.adatum.com** is working?

> **Answer:** You can browse to **https://fs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**.

## Resources

## What is claims-based authentication?

**Additional Reading:** For more information, refer to Claims-based identity term definitions: https://aka.ms/wimvc2.

## Deploying Azure AD Seamless SSO

**Additional Reading:** For more information on Azure AD Seamless SSO, refer to "Azure Active Directory Seamless Single Sign-On" at https://aka.ms/AA216ye.

## Integrating applications with Azure AD

**Reference Links:** You can access the Azure AD application gallery from: https://aka.ms/Wqkz4c.

## Demonstration: Enabling SSO for claims-aware applications in the Azure gallery

### Demonstration Steps

1. On **LON-CL2**, open Microsoft Edge, and then browse to **https://portal.azure.com**.
2. On the **Microsoft Azure** page, click **SIGN OUT**, and then click **SIGN IN**.
3. On the **Microsoft Azure** page, click **Use another account**, and then sign in with the account that is associated with your Azure trial tenant subscription.
4. On the Azure portal, click **Azure Active Directory**, and then click **Enterprise applications**.
5. Click **New application**.
6. In the **Add an application** window, type **Skype** in the search text box, and then press Enter.
7. Click **Skype**, and then in the right pane, click **Add**.
8. Close the **Add an application** window, and then close the **Categories** window.
9. Click **All applications**, and then click **Skype**.
10. In the **Skype** window, click **Users and groups**.
11. Click **Add user**, and then click **None Selected**.
12. In the **Users and groups** window, select **Abbi Skinner**, click **Select**, and then click **Assign**.
13. In the middle navigation pane, click **Single sign-on**, and then in the right pane, click **Password-based**. Click **Save**.
14. At the top right of the **Azure portal** page, click your Azure account name, and then click **Sign out**.

15. In the Microsoft Edge window, click the three dots icon in the top right corner, and then click **New InPrivate window**.
16. In the new browser window, type **https://myapps.microsoft.com** in the address bar, and then press Enter.
17. On the **Microsoft Azure** page, type **Abbi@*yourdomain.hostdomain*.com**, and then click **Next**. Type **Pa55w.rd** as password and click *Sign in*.
18. On the **Microsoft Azure** page, ensure that you see Skype in the list of apps.
19. Close Microsoft Edge.

# Lesson 3
# Implementing Azure AD PIM

## Contents:

## Question and Answers

**Question:** You can use Azure AD PIM to manage privileges for both local and cloud-based resources.

( ) True

( ) False

**Answer:**

( ) True

(√) False

**Feedback:**

Currently, Azure AD PIM can manage privileges for cloud-based resources only. You can use PAM to manage privileges for local resources.

## Demonstration: Enabling and configuring Azure AD PIM

### Demonstration Steps

1. On your local computer, open the Microsoft Edge browser, and then browse to **https://portal.azure.com**.
2. Sign in as **msnider@*adatumyyxxxx*.onmicrosoft.com** with *your password*.
3. On the Azure portal, click **All services**, navigate through the list, and then in the **IDENTITY** section, click the star icon next to the **Azure AD Privileged Identity Management**. Then in the left navigation pane click **Azure AD Privileged Identity Management.**
4. In the **Privileged Identity Management** window, click **Consent to PIM**.
5. In the right pane, click **Verify my identity**.
6. On the **More information required** page, click **Next**.
7. On the **Additional security verification** page, ensure that **Authentication phone** is selected in first drop-down list, select your country or region, and then type your mobile phone number. Select the **Send me a code by text message** option, and then click **Contact me**.
8. On the **Additional security verification** page, type the code that you received in SMS, and then click **Verify**.
9. When you receive the "Verification successful!" message, click **Done**. You will redirect back to the Azure portal.
10. On the Azure portal, click **Azure AD Privileged Identity Management**, and then click **Consent to PIM**. In the right pane, click **Consent** and then click **Yes**.
11. In the Azure portal, on the **Privileged Identity Management – Quick start** page, click **Azure AD directory roles**, click **Sign up**, and then click **Yes**.
12. In the left navigation pane, click **Azure AD Privileged Identity Management** to refresh the view.
13. Click **Azure AD directory roles**.
14. On the **Azure AD directory roles** page, click **Members**.
15. Click the **User Administrator** item under **Edmund Reeve**, and then click **Make eligible**.
16. Close the **Edmund Reeve** page and verify that his **ACTIVATION** status changed from **Permanent** to **Eligible**.
17. In the middle pane, click **Settings**.

18. On the **Settings** page, click **Roles**, and then click **User Administrator**.
19. In the User Administrator pane, click **Enable** in the **Notifications** section, and then click **Enable** in the **Incident/Request Ticket** section.
20. Change the **Maximum Activation duration (hours)** value to **2**.
21. In the **Require approval** section, click **Enable**, and then click **No approver selected**.
22. In the **Search** box, type **Miranda Snider**. Click the account, and then click **Select**.
23. Click **Save**. Close the **User Administrator** page and the **Roles** page.
24. In the Settings pane, click **Alerts**.
25. In the Alerts pane, click **Roles are being activated too frequently**.
26. In the Security alert settings pane, in the **Number of renewals** section, change the value to **7**, and then click **Save**.
27. In the Alerts pane, click **Administrators aren't using their privileged roles**.
28. On the **Security alert settings** page, change the value to **21 days**, and then click **Save**. Close the **Security alert settings** page and the **Alerts** page.
29. Click the **msnider** account in the top-right corner, and then click **Sign out**.

# Module Review and Takeaways

## Best Practices

- Join Azure AD computers that are frequently out of your local network and that access most resources in the cloud.
- If you configure SSO with AD FS, always provide a high-availability infrastructure for AD FS.
- Be aware that in an SSO with AD FS scenario, your local internet link becomes even more critical.
- Avoid configuring too many permanent administrators in Azure AD PIM.

## Common Issues and Troubleshooting Tips

| Common Issue | Troubleshooting Tip |
|---|---|
| You cannot join a computer to Azure AD. | • Check if Azure AD is configured to allow devices to join.<br>• Check if you have permissions to join a computer to Azure AD. |
| Users cannot access your local AD FS sign-in page in an SSO scenario. | • Check if you have configured certificates properly.<br>• Check if you configured your firewall to accept authentication requests from Azure AD.<br>• Check if you configured Web Application Proxy properly. |

# Lab Review Questions and Answers

## Lab: Using Azure AD in hybrid environments

## Question and Answers

**Question:** What was the purpose of the **Convert-MsolDomainToFederated** cmdlet that you executed in the lab?

> **Answer:** This cmdlet converts the domain that was configured in Azure AD to a federated domain. By doing this, you configure Azure AD to redirect authentication requests to your local AD FS and AD DS.

**Question:** What is the purpose of the Web Application Proxy component when configuring SSO?

> **Answer:** Authentication requests from Azure AD that come to your local AD DS proxy through Web Application Proxy to AD FS.

# Module 4

## Configuring and protecting authentication in hybrid environments

### Contents:

# Lesson 1
# Authenticating users in hybrid environments

## Contents:

## Question and Answers

**Question:** If you implement directory synchronization with password synchronization between AD DS and Azure AD, which system authenticates users when they access services such as Office 365?

> **Answer:** In this case, Azure AD authenticates the users because this scenario does not support SSO.

**Question:** When you join a computer to the AD DS domain, you establish a trust relationship.

( ) True

( ) False

> **Answer:**
>
> (√) True
>
> ( ) False
>
> **Feedback:**
>
> When you join a computer to the AD DS domain, your computer starts to trust tokens that Kerberos, the authentication service in AD DS, issues. Because of this, you can access local resources on your laptop or desktop computer, when you sign in with the domain account from AD DS.

## Demonstration: Configuring self-service password reset

### Demonstration Steps

1. On **LON-DS1**, run Azure AD Connect.
2. Choose to customize the synchronization options.
3. Use the **SYNC@adatumyyxxxx.onmicrosoft.com** account to connect to Azure AD.
4. Enable the option for password writeback.
5. Sign in to the Azure portal.
6. Enable users for password reset.
7. Configure the mobile phone number, alternate email address, and security questions as alternative authentication methods.

**Note:** You require at least three security questions for password reset.

8. Ensure that password writeback is configured in the Azure portal.

# Lesson 2
# Implementing multi-factor authentication

## Contents:

## Question and Answers

**Question:** Adatum Corporation requires that their applications use multi-factor authentication. The organization has implemented this technology in its on-premises infrastructure and wants to extend it for apps and resources that reside in Azure. Adatum wants to use authentication methods that are similar to what they are currently using in the on-premises infrastructure. Can they use Multi-Factor Authentication for this, and if so, why?

> **Answer:** Yes, they can use Multi-Factor Authentication. Azure Multi-Factor Authentication Server supports the following authentication methods to complement user names and passwords:
>
> - A phone call
> - A two-way SMS
> - A two-way SMS with PIN
> - A one-way SMS
> - A one-way SMS with PIN
> - An OAuth token
> - Mobile app

**Question:** Do you have any resources in your organization that you need to protect with multi-factor authentication?

> **Answer:** Answers might vary.

## Demonstration: Configuring and enabling Multi-Factor Authentication

### Demonstration Steps

1. Sign in to the Azure portal.
2. Open the configuration pane for the **Adatum** directory item.
3. Click the **Users** option, and then select to configure multi-factor authentication.
4. Enable multi-factor authentication for **Abbi Skinner**.
5. Review the options in the multi-factor authentication administration portal.

## Demonstration: Configuring on-premises Multi-Factor Authentication Server

### Demonstration Steps

1. Sign in to **LON-SVR2**, and then open the **Routing and Remote Access from Server Manager** console.
2. On **LON-SVR2**, open the Routing and Remote Access configuration wizard.
3. Select the remote access (dial-up or VPN) scenario, and then configure just the **VPN** option.
4. Configure authentication to work over RADIUS.
5. Configure **lon-svr1.adatum.com** as the RADIUS server for the VPN connections, configure the shared secret as **Pa55w.rd**, and then complete the wizard.
6. Open the **Properties** dialog box for **LON-SVR2**, and then configure time-out for the RADIUS server as **60 seconds**.
7. Switch to **LON-SVR1**, and then open the **Azure Multi-Factor Authentication Server Setup Wizard**.

8. Configure **lon-svr2.adatum.com** as a RADIUS client, and then provide the same shared secret as in step 5.

9. Complete the wizard and reboot the server, if needed.

10. After **LON-SVR1** reboots, open the **Multi-factor Authentication Server** console.

11. Import users from the local AD DS to the **Multi-factor Authentication Server** console.

12. Configure **Administrator** as the user portal administrator.

13. Enable user **Abbi Skinner** for local multi-factor authentication by using a standard phone call. Provide your mobile phone number and configure the phone call language as your local language.

14. In the **Multi-Factor Authentication Server** window, click **RADIUS Authentication** in the left pane, and then enable multi-factor authentication user match for **LON-SVR2**.

# Module Review and Takeaways

## Best Practices

- Implement the password writeback functionality to keep passwords consistent between Azure AD and AD DS.
- Suggest that users use the mobile app as a multi-factor authentication method.
- Use Multi-Factor Authentication Server to protect VPN connections.
- Protect privileged role activation with Multi-Factor Authentication.
- Configure multi-factor authentication messages in the local language to make this service easier for your users to use.

## Review Question

**Question:** If you don’t want to use self-service password reset from Azure AD, what is the alternative to provide this functionality for AD DS?

**Answer:** You can deploy Microsoft Identity Manager on premises.

## Common Issues and Troubleshooting Tips

| Common Issue | Troubleshooting Tip |
|---|---|
| Multi-factor authentication does not work for VPN connections | Ensure that you configured your VPN server or VPN appliance as the RADIUS client for Multi-Factor Authentication Server |

# Lab Review Questions and Answers

## Lab: Configuring authentication in hybrid environments

## Question and Answers

**Question:** When a user resets the password by using the Azure AD profile page, what should you enable to maintain password consistency in Azure AD and AD DS?

**Answer:** You should implement the password writeback functionality.

**Question:** You want to enforce multi-factor authentication for your business-critical website. What should you use?

**Answer:** You should use Multi-Factor Authentication Server.

# Module 5

## Deploying Azure Information Protection with on-premises services

### Contents:

# Lesson 1
# Overview of data protection technologies based on rights management

## Contents:

## Question and Answers

**Question:** How does Azure Information Protection fit into a company-wide data protection initiative?

**Answer:** Answers will vary, but might include:

- Azure Information Protection protects specific files that users have opted to protect. However, you should still protect data that users have not specifically protected with the help of Azure Information Protection. You can use BitLocker Drive Encryption to protect entire volumes while still using Azure RMS to further protect documents, especially those that will be shared.
- Azure Information Protection protects email messages, but only when users opt to do so. However, to automate protection, you can use server-based Exchange transport rules to protect email messages after a user sends them, but before they leave the organization.
- Beyond just protecting data with Azure Information Protection, you need the ability to audit data access. You can track documents protected with Azure Information Protection. You also can use the advanced auditing features of Group Policy to audit access to files and folders.

**Question:** You can protect picture files with Azure Information Protection.

( ) True

( ) False

**Answer:**

(√) True

( ) False

**Feedback:**

Azure Information Protection with the RMS sharing application or the Azure Information Protection client allows you to protect picture files.

**Question:** What are some of the key differences between Azure Information Protection and AD RMS?

**Answer:** Azure Information Protection integrates with on-premises servers, and with Microsoft Office 365, Exchange Online, and SharePoint Online. AD RMS only integrates with on-premises servers. In addition, Azure Information Protection lets you share protected content seamlessly with users outside of your organization. While AD RMS offers this functionality, it requires a large amount of setup time and federation with each outside organization with which you will share protected content. Finally, Azure Information Protection supports Azure Multi-Factor Authentication, but AD RMS does not.

## Resources

## What is Azure Information Protection?

**Additional Reading:** For more information on Azure Information Protection, refer to "What is Azure Information Protection?" at https://aka.ms/Ty1miv.

## What is Azure RMS?

**Additional Reading:** For more information, refer to "Protecting and Tracking Sensitive Data with RMS: Today and What's Next" at http://aka.ms/w4bald.

## Comparing Azure Information Protection, Azure Information Protection for Office 365, and AD RMS

**Additional Reading:** For more information, refer to “Comparing Azure Information Protection and AD RMS” at http://aka.ms/sndlw0.

# Lesson 2
# Implementing Azure Information Protection

## Contents:

## Question and Answers

**Question:** What is the disadvantage of configuring a protected document to be immediately revocable?

> **Answer:** When you configure a protected document to be immediately revocable, the recipient of the document must authenticate to Azure Information Protection every time they open the document.

## Resources

## Activating Azure Information Protection

**Additional Reading:** For more information, see "Azure Information Protection" at http://aka.ms/wqy43u.

## Azure Information Protection document tracking

**Additional Reading:** For more information on how to configure and use document tracking, refer to "Admin Guide: Configuring and using document tracking for Azure Information Protection" at https://aka.ms/AA31z7l.

## Demonstration: Configuring Azure Information Protection labels and protection

### Demonstration Steps

1. In the Azure portal, click **Azure Information Protection** in the left navigation pane.
2. Click **Policies** and verify that **Global policy** is present.
3. Click **Labels**.
4. In the right pane, click **Add a new label**.
5. In the **Label** pane, in the **Label name** text box, type **Adatum Documents Protection**.
6. In the **Description** field, type any text.
7. In the **Color** drop-down box, select the color of your choice.
8. In the **Set permissions for documents and emails containing this label** section, click **Protect**.
9. Click **Protection Azure (cloud key)**.
10. In the Protection pane, select **Set permissions**, and then click **Add permissions**.
11. On the **Add permissions** page, select **Add Adatum Corp – All members**.
12. In the **Choose permissions from preset or set custom** section, click **Viewer**, and then click **OK**.
13. On the **Protection** page, set **Content expiration** to **By days** and type **7**, and then click **OK**.
14. In the **Set visual marking (such as header or footer)** section, click **On** for **Documents with this label have header**.
15. In the **Header** text box, type **This document is protected to use only in Adatum Corp**.
16. In the **Configure conditions for automatically applying this label** section, click **Add a new condition**.

17. In the **Condition** window, click **Custom**. Type **Internal doc** for the name, and then in the **Match exact phrase or pattern** text box, type **Adatum-Internal**.
18. Click **Save** and then click **OK**.
19. In the **Label** window, below the **Conditions** section, click **Automatic**.
20. In the **Label** window, click **Save**, and then click **OK**.
21. Click **Policies**.
22. Click **Global policy**.
23. Click **Add or remove labels**.
24. Select **Adatum Documents Protection**, click **OK**, click **Save**, and then click **OK**.
25. In the **Policy: Global** window, click **On** for **All documents and emails must have label**.
26. Click **Save** and then click **OK**.

## Demonstration: Installing and using the Azure Information Protection client application

### Demonstration Steps

1. On the **LON-CL2** computer, open Microsoft Edge.
2. In the Microsoft Edge address bar, type **https://aka.ms/AA31rhh**, and then press Enter.
3. On the **Download Center** page, click **Download**.
4. On the **Choose the download you want** page, select **AzInfoProtection.exe**, and then click **Next**.
5. On the **Thank you for downloading** page, at the prompt that appears on the bottom of the page, click **Save as**.
6. In the left menu, click the **Downloads** folder, and then click **Save**.
7. On the taskbar, click the **File Explorer** icon.
8. In File Explorer, navigate to the **Downloads** folder.
9. Double-click the **AzInfoProtection** file.
10. In the **Install the Azure Information Protection client** window, click **I agree**. If a **User Account Control** dialog box appears, click **Yes**.
11. Ensure that you have the **Completed Successfully** status at the end of the installation.
12. Click **Close**.
13. Restart the computer and then sign in again as **Adam@***yourdomain.hostdomain***.com**, with password **Pa55w.rd**. On the **Set up a PIN** page, click **Set up PIN**. Close the **Help us protect your account** window, and then click **Skip for now**.
14. On **LON-CL2**, open Microsoft Word 2016, and create a blank document.
15. Type **Adatum-Internal** in the first line of the document, and then type any text in the rest of the document.
16. Save the document in any folder on **LON-CL2**.
17. Ensure that the document is automatically protected with the **Adatum Documents protection** label. You will notice this is in the title bar. Close Word.
18. Close and reopen Word 2016.

19. Create a blank document and type any text. Note: Do not write the **Adatum-Internal** text.

20. Try to save the document. Notice the prompt to select the label.

21. Click **Public** in the **Microsoft Azure Information Protection** window and then click **OK**. Save the document.

22. Ensure that the label **Public** is applied. You can view this in the title bar.

23. Close Word.

24. On **LON-CL2**, open File Explorer, create the **C:\temp** folder, right-click the empty space, click **New**, and then click **Text Document**.

25. Name the new document **Doc1**.

26. Open **Doc1**, and type some text. Save the document, and then close it.

27. Right-click the document and click **Classify and protect**.

28. In the **Classify and protect - Azure Information Protection** window, click **Adatum Documents Protection**, and then click **Apply**. Click **Close**.

29. After the protecting window closes, ensure that the file has changed the extension to **.ptxt**.

30. Double-click **Doc1**. Ensure that it now opens in the Azure Information Protection Viewer and not in Notepad.

31. Close the file.

# Lesson 3
# Integrating Azure Information Protection with on-premises services

## Contents:

## Question and Answers

**Question:** What kind of Azure RMS protection would you implement in your organization?

> **Answer:** Answers might vary, but students will most probably mention that Azure RMS integration with Windows Server FCI or with SharePoint library would be the appropriate option.

## Resources

## What is the RMS connector?

**Additional Reading:** For more information on deploying the RMS connector, refer to http://aka.ms/ylfrax.

## Demonstration: Installing and configuring an RMS connector

### Demonstration Steps

1. If needed, sign in to **LON-SVR2** as **ADATUM\Administrator** with the password **Pa55w.rd**.
2. Open Internet Explorer from the taskbar and navigate to **https://aka.ms/AA31z7m**.
3. On the **Microsoft Rights Management connector** page, click **Download**.
4. On the **Choose the download you want** page, select all items, and then click **Next**.
5. Click **Allow once** to allow the popup window for the download.
6. Save all three files to the **Downloads** folder.
7. Open File Explorer, navigate to **Downloads**, and then double-click **RMSConnectorSetup.exe**.
8. In the **Open File – Security Warning** window, click **Run**.
9. In the **Microsoft Rights Management connector setup** window, on the **Welcome to Microsoft Rights Management connector setup** page, click **Next**.
10. On the **End-User License Agreement** page, select the **I accept the terms in the License Agreement** check box, and then click **Next**.
11. On the **Microsoft RMS administrator credentials** page, type **msnider@adatumyyxxxx.onmicrosoft.com** *for* the *user name*, type **Pa55w.rd!** for the password, and then click **Next**.
12. On the **Ready to install Microsoft Rights Management connector** page, click **Install**.
13. On the **Installation of Microsoft Rights Management connector completed** page, clear the **Launch connector administration console to authorize servers** check box, and then click **Finish**.
14. In the **File Explorer** window, in the **Downloads** folder, right-click **GenConnectorConfig.ps1**, and then select **Copy**.
15. In the address bar of File Explorer, type **\\LON-SVR1\C$**, and then press Enter.
16. Right-click the empty space in the window and select **Paste**.
17. Close the Internet Explorer window on **LON-SVR2**.

## Demonstration: Configuring Azure Information Protection with FCI

### Demonstration Steps

1. On **LON-SVR2**, on the desktop, double-click the **Microsoft RMS connector administration tool** shortcut.

2. In the **Microsoft Rights Management connector administration tool** window, in the **Username** text box, type **msnider@*adatumyyxxxx*.onmicrosoft.com**. In the **Password** text box, type your password, and then click **Sign In**.

3. On the **Servers allowed to utilize the connector** page, click **Add**.

4. In the **Allow a server to utilize the connector** window, click the **Role** drop-down list box, and then click **FCI Server**.

5. Next to the **Account or group** designation, click **Browse**.

6. In the **Select User, Computer, Service Account, or Group** window, type **LON-SVR1**, and then click **Check Names**.

7. After the server name resolves (it will be underlined), click **OK**.

8. In the **Allow a server to utilize the connector** window, click **OK**.

9. In the **Microsoft Rights Management connector administration tool** window, click **Close**.

10. If needed, sign in to **LON-SVR1** as **ADATUM\Administrator** with the password **Pa55w.rd**.

11. Click **Start**, and then click the **Windows PowerShell** icon.

12. At the Windows PowerShell command-line prompt, navigate to **C:\**. Run the **.\GenConnectorConfig.ps1 –ConnectorUri http://lon-svr2.adatum.com -SetFCI2012** command.

13. Type **R** if prompted, and then press Enter.

# Module Review and Takeaways

## Best Practices

- When protecting content, configure documents to have immediate revocation if the files are sensitive or if your organization has a high-security environment.
- Run at least two RMS connector servers to provide for high availability and to ensure that users can always gain access to protected content.
- If you have Exchange, SharePoint, and Windows Server FCI, you should integrate all three with Azure RMS to expand the availability of data protection.
- Use Group Policy to configure servers for Azure RMS. You can use a GPO to populate the registry with your Azure RMS information automatically.
- Use an application delivery solution, such as Microsoft System Center Configuration Manager, to distribute the RMS sharing application to all employees. This helps to maximize the use of data protection.

## Review Question

**Question:** What changes must you make on an Exchange Server, a SharePoint Server, or an FCI server to integrate it with Azure RMS?

**Answer:** You must update the registry to point to Azure RMS.

## Common Issues and Troubleshooting Tips

| Common Issue | Troubleshooting Tip |
|---|---|
| You cannot view a protected document that you used to be able to view. | The sender might have revoked your access. Contact the sender to inquire. |
| You cannot import the Active Directory Rights Management (AADRM) module for Windows PowerShell. | By default, the AADRM module is not available for import. You need to download and install the Azure Rights Management Administration Tool, and then you can import the AADRM module. You can download the tool from http://aka.ms/h45lwq. |
| You cannot activate Azure Information Protection. | A standard Azure subscription does not include use rights for Azure Information Protection, and thus you will not be able to activate Azure Information Protection. To activate Azure Information Protection, you must have either an Office 365 subscription, an Azure Information Protection P1 or P2 subscription, an Enterprise Mobility + Security subscription, or an RMS for individual subscription. |

# Lab Review Questions and Answers

## Lab: Implementing Azure Information Protection

## Question and Answers

**Question:** When configuring Azure RMS integration for Windows Server FCI, Exchange, or SharePoint, why do you need to use Windows PowerShell as part of the process?

> **Answer:** You need to obtain your RMS connector Uniform Resource Indicator (URI), which you use to configure the registry on integrated servers.

**Question:** What application should you use to protect JPEG files with RMS?

> **Answer:** You should use the Azure Information Protection client application for Windows.

# Module 6

## Monitoring Azure AD

### Contents:

# Lesson 1
# Azure AD reporting

## Contents:

## Question and Answers

**Question:** What should you use to provide alert and notification capabilities for locally deployed AD DS?

> **Answer:** Because AD DS does not have built-in capabilities for alerts or notifications, you should use additional software solutions such as Operations Manager.

## Demonstration: Using Azure AD reports and configuring notifications

### Demonstration Steps

1. Sign in to the Azure portal on your host machine with administrative credentials for your Azure AD tenant.
2. Browse to **Audit logs**.
3. Review the available reports.
4. Filter reports for the user object type.
5. Review the **Sign-ins** report.
6. Review the **Notification** settings.
7. On the Azure portal, on the **adatum directory** page, open the **Password reset** pane.
8. Configure notifications for password reset so that users and admins receive password reset notifications.
9. Save the changes and close the Azure portal.

# Lesson 2
# Monitoring Azure AD

## Contents:

## Question and Answers

**Question:** Do you need to deploy agent software to monitor Azure AD with Azure Monitor?

**Answer:** No. You need agent software only for AD DS monitoring.

**Question:** Which of the following resources can you monitor and manage by using Azure Monitor?

( ) An infrastructure as a service (IaaS) VM that is running Linux

( ) A platform as a service (PaaS) Cloud Service worker role

( ) A PaaS web app

( ) An Azure Storage account

( ) An on-premises computer that is running the 32-bit Enterprise edition of Windows 8

**Answer:**

(√) An infrastructure as a service (IaaS) VM that is running Linux

(√) A platform as a service (PaaS) Cloud Service worker role

( ) A PaaS web app

( ) An Azure Storage account

(√) An on-premises computer that is running the 32-bit Enterprise edition of Windows 8

**Feedback:**

By using Azure Monitor, you can monitor Windows and Linux operating systems, both in Azure and on-premises, but not Azure platform as a service (PaaS) services.

## Demonstration: Configuring Azure AD Connect Health

### Demonstration Steps

1. On **LON-DC1**, open the new Azure portal, and then sign in with your administrative account.
2. Open the services list, and then go to Azure AD Connect Health.
3. Pin Azure AD Connect Health to the dashboard.
4. In the **Azure AD Connect Health** pane, click your tenant, and then review the report.
5. Download the Microsoft Azure AD Connect Health Agent for AD DS, and then install the agent software on **LON-DC1**.
6. Start the agent configuration after it installs.
7. Restore the Azure portal, and then browse to the Azure AD Connect Health dashboard.
8. Ensure that you see the **Active Directory Domain Services** section.
9. Click **Adatum.com**, and then review the available reports.

# Module Review and Takeaways

## Best Practices

- If you cannot use cloud services for AD DS monitoring, we recommend that you use Operations Manager with the AD DS management pack.
- Review Azure AD reports frequently.
- Ensure that at least one Azure AD administrator reviews the notifications that Azure AD provides.
- Use Azure AD Connect Health for directory synchronization monitoring.

## Review Question

**Question:** If you want to check the status of antivirus and antimalware scans on multiple servers, which tool or service should you use?

> **Answer:** You should use Azure Monitor with the Malware Assessment solution that is available in the Management solutions gallery.

## Common Issues and Troubleshooting Tips

| Common Issue | Troubleshooting Tip |
|---|---|
| The agent that is installed on a locally deployed server cannot communicate with Azure Monitor. | Check the firewall on the local computer. |

# Lab Review Questions and Answers

## Lab: Configuring reporting and monitoring

## Question and Answers

**Question:** What report should you use to discover sign-in activities in your Azure AD tenant?

> **Answer:** You should use the **Sign-ins** report available in the Azure Active Directory administration pane.

**Question:** What can you monitor with Azure AD Connect Health?

> **Answer:** The primary function of Azure AD Connect Health is to monitor syncing between AD DS and Azure AD. However, you can also use it to monitor Active Directory Federation Services (AD FS) and AD DS.