# Contents


0.0.1 Managing Modern Desktops . . . 5
0.1 title: Online Hosted Instructions permalink: index.html layout: home . . . 5

**1 Content Directory** **5**
1.1 Labs . . . 5
1.2 Demos . . . 5

**2 MD-101: Managing Modern Desktops** **5**
2.1 Lab Change Log . . . 5
2.1.1 05-14-21 . . . 6
2.1.2 04-05-21 . . . 6
2.1.3 02-21-21 . . . 6
2.1.4 07-17-20 . . . 6
2.1.5 05-15-20 . . . 6
2.1.6 04-17-20 . . . 6
2.1.7 02-24-19 . . . 6
2.1.8 12-02-19 . . . 7
2.1.9 11-08-19 . . . 7
2.1.10 11-04-19 . . . 7

**3 MD-101: Managing Modern Desktops** **7**
3.1 What are we doing? . . . 7
3.2 How should I use these files relative to the released MOC files? . . . 7
3.3 What about changes to the student handbook? . . . 7
3.4 How do I contribute? . . . 7
3.5 Notes . . . 7
3.5.1 Classroom Materials . . . 7

**4 Practice Lab: Managing Identities in Azure AD** **8**
4.1 Summary . . . 8
4.2 Exercise 1: Creating users in Azure AD . . . 8
4.2.1 Scenario . . . 8
4.2.2 Task 1: Create users by using the Azure Active Directory admin center . . . 8
4.2.3 Task 2: Create users by using PowerShell . . . 9
4.3 Exercise 2: Validating licenses and creating and managing groups . . . 9
4.3.1 Scenario . . . 9
4.3.2 Task 1: Review licenses and modify company branding . . . 9
4.3.3 Task 2: Create groups by using the Azure Active Directory admin center . . . 10
4.3.4 Task 3: Create groups by using PowerShell . . . 10

**5 Practice Lab: Using Azure AD Connect to connect AD DS to Azure AD** **11**
5.1 Summary . . . 11
5.1.1 Scenario . . . 11
5.1.1.1 Task 1: Configure directory synchronization with Azure AD Connect . . . 11
5.1.1.2 Task 2: Verify synchronization in Azure AD . . . 12

**6 Practice Lab: Configuring and managing Azure AD Join** **12**
6.1 Summary . . . 12
6.2 Exercise 1: Configuring Azure AD Join . . . 12
6.2.1 Scenario . . . 12
6.2.2 Task 1: Configure Azure AD join Device settings . . . 13
6.2.3 Task 2: Perform an Azure AD Join . . . 13
6.2.4 Task 3: Validate Azure AD Join . . . 13
6.2.5 Task 4: Sign in to Windows 10 as an Azure AD User . . . 14
6.2.6 Task 5: Remove a Windows 10 device from Azure AD . . . 14
6.3 Exercise 2: Configuring Hybrid Azure AD Join . . . 14
6.3.1 Scenario . . . 14
6.3.2 Task 1: Prepare the environment . . . 14
6.3.3 Task 2: Re-configure Azure AD Connect . . . 14
6.3.4 Task 3: Configure hybrid Azure AD join in Azure Active Directory Connect . . . 15

6.3.5 Task 4: Verify the Azure AD registration . . . 15

**7 Practice Lab: Manage Device Enrollment into Intune 16**
7.1 Summary . . . 16
7.1.1 Scenario . . . 16
7.1.2 Task 1: Review and assign licenses for device management . . . 16
7.1.3 Task 2: Enable Windows Automatic Enrollment into Microsoft Intune . . . 16
7.1.4 Task 3: Configure Enrollment Restrictions . . . 17

**8 Practice Lab: Enrolling devices into Microsoft Intune 17**
8.1 Summary . . . 17
8.1.1 Scenario . . . 17
8.1.2 Task 1: Automatically enroll a Windows 10 device to Microsoft Intune . . . 17
8.1.3 Task 2: Validate device enrollment into Azure AD And Intune . . . 18
8.1.4 Task 3: Sign in as an Azure AD user . . . 18
8.1.5 Task 4: Verifying device enrollment in the Intune console . . . 18

**9 Practice Lab: Creating and Deploying Configuration Profiles 19**
9.1 Summary . . . 19
9.2 Exercise 1: Create and apply a Configuration profile . . . 19
9.2.1 Scenario . . . 19
9.2.2 Task 1: Verify device settings before enrollment . . . 19
9.2.3 Task 2: Join SEA-WS2 to Azure AD and Enroll in Intune . . . 20
9.2.4 Task 3: Sign in to SEA-WS2 with an Azure AD account . . . 20
9.2.5 Task 4: Create device profile based on scenario . . . 20
9.2.6 Task 5: Create the Contoso Developer device group . . . 21
9.2.7 Task 6: Create a dynamic Azure AD device group . . . 21
9.2.8 Task 7: Assign a Configuration profile to Windows 10 devices . . . 21
9.2.9 Task 8: Verify that Configuration profile is applied . . . 22
9.3 Exercise 2: Modify an assigned Configuration profile policy . . . 22
9.3.1 Scenario . . . 22
9.3.2 Task 1: Change settings in assigned profile . . . 22
9.3.3 Task 2: Force device synchronization from Microsoft Endpoint Manager admin center . . . 22
9.3.4 Task 3: Verify profile changes on SEA-WS2 . . . 23

**10 Practice Lab: Monitor device and user activity in Intune 23**
10.1 Summary . . . 23
10.1.1 Scenario . . . 23
10.1.2 Task 1: Monitor user activity . . . 23
10.1.3 Task 2: Monitor device activity . . . 23

**11 Practice Lab: Configuring Enterprise State Roaming 24**
11.1 Summary . . . 24
11.1.1 Scenario . . . 24
11.1.2 Task 1: Enable Enterprise State Roaming . . . 24
11.1.3 Task 2: Verify sync is enabled on SEA-WS2 . . . 24
11.1.4 Task 3: Re-enroll SEA-WS2 (only perform if needed) . . . 25
11.1.5 Task 4: Test Enterprise State Roaming . . . 25

**12 Practice Lab: Deploying cloud apps using Intune 26**
12.1 Summary . . . 26
12.2 Exercise 1: Add a Microsoft Store App to Intune . . . 26
12.2.1 Scenario . . . 26
12.2.2 Task 1: Add Microsoft Remote Desktop to Intune . . . 26
12.2.3 Task 2: Assign a Group to the App . . . 26
12.2.4 Task 3: Install an app from the Company Portal Website . . . 27
12.3 Exercise 2: Configure and deploy Microsoft 365 Apps from Intune . . . 27
12.3.1 Scenario . . . 27
12.3.2 Task 1: Verify installed apps on SEA-WS2 . . . 27
12.3.3 Task 2: Add Microsoft 365 apps to Intune . . . 27
12.3.4 Task 3: Force policy synchronization from the Intune console . . . 28
12.3.5 Task 4: Verify Microsoft 365 apps are installed . . . 28

12.3.6 Task 5: Monitor app installation status in Intune . . . 28

**13 Practice Lab: Configure App Protection Policies for Mobile Devices 29**
13.1 Summary . . . 29
13.1.1 Scenario . . . 29
13.1.2 Task 1: Create an App protection policy in Intune . . . 29

**14 Practice Lab: Deploy Apps using Endpoint Configuration Manager 30**
14.1 Summary . . . 30
14.1.1 Scenario . . . 30
14.1.2 Task 1: Create a device collection . . . 30
14.1.3 Task 2: Assign a Device to an existing Collection . . . 30
14.1.4 Task 3: Configure a deployment type . . . 31
14.1.5 Task 4: Distribute content to distribution points . . . 31
14.1.6 Task 5: Create a deployment . . . 31
14.1.7 Task 6: Use Software center to install a deployed app . . . 32

**15 Practice Lab: Deploy Apps using Microsoft Store for Business 32**
15.1 Summary . . . 32
15.2 Exercise 1: Add a Microsoft Store App to Intune . . . 32
15.2.1 Scenario . . . 32
15.2.2 Task 1: Configure Microsoft Store for Business settings and integration with Intune . . . 32
15.2.3 Task 2: Purchasing and Adding apps to the Private Store . . . 33
15.2.4 Task 3: Review the apps in the Company store . . . 33
15.3 Exercise 2: Deploy Microsoft Store for Business Apps using Intune . . . 33
15.3.1 Scenario . . . 33
15.3.2 Task 1: Synchronize Intune with Microsoft Store for Business . . . 33
15.3.3 Task 2: Deploy Microsoft Store for Business apps . . . 33
15.3.4 Task 3: Force policy synchronization from the Intune console . . . 34
15.3.5 Task 4: Verify the app has installed . . . 34
15.3.6 Task 5: Monitor app installation status in Intune . . . 34

**16 Practice Lab: Configuring Multi-factor Authentication 35**
16.1 Summary . . . 35
16.2 Exercise 1: Configure per-user multi-factor authentication . . . 35
16.2.1 Scenario . . . 35
16.2.2 Task 1: Validate sign-in before enabling MFA . . . 35
16.2.3 Task 2: Enable MFA for a user . . . 35
16.2.4 Task 3: Register and Validate MFA . . . 35
16.2.5 Task 3: Remove per-user MFA . . . 36
16.3 Exercise 2: Configure multi-factor authentication using conditional access . . . 36
16.3.1 Scenario . . . 36
16.3.2 Task 1: Validate sign-in before enabling conditional access with MFA . . . 36
16.3.3 Task 2: Configure conditional access with MFA . . . 37
16.3.4 Task 3: Validate conditional access MFA . . . 37
16.3.5 Task 4: Remove conditional access MFA . . . 37

**17 Practice Lab: Configuring Self-service password reset for user accounts in Azure AD 38**
17.1 Summary . . . 38
17.1.1 Scenario . . . 38
17.1.2 Task 1: Configure password writeback . . . 38
17.1.3 Task 2: Enable self-service password reset . . . 38
17.1.4 Task 3: Validate self-service password reset . . . 39
17.1.5 Task 4: Optional - Run AD Sync . . . 39
17.1.6 Task 4: Verify password writeback . . . 39

**18 Practice Lab: Configuring and validating device compliance 39**
18.1 Summary . . . 39
18.2 Exercise 1: Configuring compliance policies . . . 39
18.2.1 Scenario . . . 39
18.2.2 Task 1: Create and assign a compliance policy . . . 40
18.3 Exercise 2: Creating a conditional access policy . . . 40

18.3.1 Scenario . . . 40
18.3.2 Task 1: Create a conditional access policy . . . 40
18.3.3 Task 2: Verify that the conditional access policy is working . . . 41
18.3.4 Task 3: Disable the conditional access policy . . . 41

**19 Practice Lab: Creating device inventory reports 41**
19.1 Summary . . . 41
19.2 Exercise 1: Reviewing device inventory with Intune . . . 42
19.2.1 Scenario . . . 42
19.2.2 Task 1: Examining device inventory . . . 42
19.3 Exercise 2: Exporting Intune data to Excel . . . 42
19.3.1 Scenario . . . 42
19.3.2 Task 1: Export Intune Data . . . 42
19.3.3 Task 2: Import Intune data into Microsoft Excel . . . 42
19.4 Exercise 3: Reviewing Intune Data using Power BI . . . 43
19.4.1 Scenario . . . 43
19.4.2 Task 1: Connect Power BI to the Intune Data Warehouse . . . 43
19.4.3 Task 2: Create a custom report using Power BI and Intune Data Warehouse . . . 43

**20 Practice Lab: Configure and Deploy Windows Information Protection Policies by using Intune 44**
20.1 Summary . . . 44
20.1.1 Task 1: Configure the MAM service . . . 44
20.1.2 Task 2: Configure an App protection policy for Windows Information Protection . . . 44
20.1.3 Task 3: Deploy the policy . . . 44
20.1.4 Task 4: Create a test file . . . 44
20.1.5 Task 5: Add a corporate account to Windows 10 . . . 45
20.1.6 Task 6: Verify the WIP policy . . . 45

**21 Practice Lab: Configuring Endpoint security using Intune 46**
21.1 Summary . . . 46
21.1.1 Scenario . . . 46
21.1.2 Task 1: Configure Windows Security Experience in Intune . . . 46
21.1.3 Task 2: Configure Microsoft Defender Antivirus policy in Intune . . . 46
21.1.4 Task 3: Sync the managed devices . . . 47
21.1.5 Task 4: Verify the configuration . . . 47

**22 Practice Lab: Configuring Disk Encryption Using Intune 47**
22.1 Summary . . . 47
22.1.1 Scenario . . . 47
22.1.2 Task 1: Configure device configuration policy in Intune . . . 47
22.1.3 Task 2: Verify and enable BitLocker settings . . . 48
22.1.4 Task 3: Verify BitLocker protection . . . 48

**23 Practice Lab: Deploying Windows 10 using Microsoft Deployment Toolkit 49**
23.1 Summary . . . 49
23.1.1 Scenario . . . 49
23.1.2 Task 1: Create a new Deployment Share . . . 49
23.1.3 Task 2: Add Operating System files to the Deployment Share . . . 49
23.1.4 Task 3: Add Applications to the Deployment Share . . . 49
23.1.5 Task 4: Create an MDT Task Sequence . . . 50
23.1.6 Task 5: Configure Deployment Share Properties and Windows PE settings . . . 50
23.1.7 Task 6: Deploy Windows 10 Using MDT . . . 51

**24 Practice Lab: Deploying Windows 10 using Endpoint Configuration Manager 52**
24.1 Summary . . . 52
24.1.1 Scenario . . . 52
24.1.2 Task 1: Create a device collection . . . 52
24.1.3 Task 2: Assign a Device to an existing Collection . . . 52
24.1.4 Task 3: Import an Operating System Image . . . 52
24.1.5 Task 4: Distribute content to distribution points . . . 53
24.1.6 Task 5: Configure Boot Images . . . 53

24.1.7 Task 6: Distribute Boot Images to distribution points . . . 53
24.1.8 Task 7: Create an Install image Task Sequence . . . 53
24.1.9 Task 8: Deploy the Windows 10 Task Sequence . . . 54
24.1.10 Task 9: Run the Windows 10 Task Sequence . . . 54

**25 Practice Lab: Deploying Windows 10 with Autopilot 55**
25.1 Summary . . . 55
25.1.1 Scenario . . . 55
25.1.2 Task 1: Create group in Azure AD . . . 55
25.1.3 Task 2: Generate a device-specific comma-separated value (CSV) file . . . 55
25.1.4 Task 3: Work with a Windows Autopilot deployment profile . . . 56
25.1.5 Task 4: Reset the PC . . . 57
25.1.6 Task 5: Verify Autopilot deployment . . . 57

**26 Practice Lab: Configuring Co-Management Using Configuration Manager 58**
26.1 Summary . . . 58
26.1.1 Scenario . . . 58
26.1.2 Task 1: Prepare the environment . . . 58
26.1.3 Task 2: Create a device collection . . . 58
26.1.4 Task 3: Assign a Device to an existing Collection . . . 59
26.1.5 Task 4: Tenant attach Endpoint Configuration Manager . . . 59
26.1.6 Task 5: Validate that SEA-CL1 is co-managed . . . 59

**27 Practice Lab: Managing Windows 10 security and feature updates 60**
27.1 Summary . . . 60
27.1.1 Scenario . . . 60
27.1.1.1 Task 1: Verify current update settings for a single device . . . 60
27.1.1.2 Task 2: Review applied settings . . . 60
27.1.1.3 Task 3: Configure update settings by using Intune . . . 60
27.1.1.4 Task 4: Verify that the device's update settings are managed centrally . . . 61

#### 0.0.1 Managing Modern Desktops

---

### 0.1 title: Online Hosted Instructions permalink: index.html layout: home

# 1 Content Directory

Hyperlinks to each of the lab exercises and demos are listed below.

## 1.1 Labs

{% assign labs = site.pages | where_exp:"page", "page.url contains '/Instructions/Labs'" %} | Module | Lab | | --- | --- | {% for activity in labs %}| {{ activity.lab.module }} | [{{ activity.lab.title }}{% if activity.lab.type %} - {{ activity.lab.type }}{% endif %}](/home/ll/Azure_clone/Azure_new/MD-101T00-ManagingModernDesktops/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

## 1.2 Demos

{% assign demos = site.pages | where_exp:"page", "page.url contains '/Instructions/Demos'" %} | Module | Demo | | --- | --- | {% for activity in demos %}| {{ activity.demo.module }} | [{{ activity.demo.title }}](/home/ll/Azure_clone/Azure_new/MD-101T00-ManagingModernDesktops/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

# 2 MD-101: Managing Modern Desktops

## 2.1 Lab Change Log

This log will be updated whenever updates are made to the lab steps in MD-101. Note that this log only contains changes to the labs. The change log for course content is still located in the Learning Download Center.

#### 2.1.1 05-14-21

- Minor updates to reflect UI changes
- Minor formatting corrections
- 0301 - Corrected rule syntax
- 0401 - Corrected step to reflect PIN change in earlier lab
- 0404 - Replace Translator app with Network Speed Test app
- 0502 - Made AD Sync separate optional task with explanation for it's purpose
- 0901 - Changed to use client WS2

#### 2.1.2 04-05-21

- Minor corrections
  - 0404 - Removed region in App store URL
  - 0303 - Removed legacy steps related to Notepad in ESR
  - 0702 - Removed steps to Mount the ISO on CFG1 in Task 1 - this is actually not necessary as the files are already in the sources folder. Updated Task 3 Step 4 to reflect this.
- Minor formatting errors

#### 2.1.3 02-21-21

- All labs have been refreshed
  - New Lab VM Set
  - New VM names (now SEA, instead of LON)
  - See Trainer Prep Guide for details and lab list.
- Clients now using Windows 10 20H2, Servers now on 2019

#### 2.1.4 07-17-20

- **Labs order has changed.** Labs have been updated to reflect the new module order and changes in the course updates published on 07-17-2020.
- New Lab: **Configure Hybrid Azure AD join** (Module 2)
- All labs have been updated to use Endpoint Manager admin center where applicable.
- **Protecting Data and Devices** and **Managing Updates** labs have been changed to use Endpoint Manager.
- All labs have been updated to reflect UI changes.

#### 2.1.5 05-15-20

- Several labs have been updated to address UI changes in the Intune console.
- Lab 0203 **Deploying Windows 10 with Autopilot** has been updated to use the Endpoint Manager admin center console. We will continue to update additional labs to this console in the near future.
- Lab 0502 **Configuring Windows Profiles** has been corrected to account for the possibility that both client devices may need to be re-enrolled for ESR to work correctly. Minor corrections and formatting issues.

#### 2.1.6 04-17-20

- Lab 0404 **Creating device inventory reports**, Scenario 3, updated steps to create reports using PowerBI instead of using pre-configured reports (that were causing a previous issue). Also updated to use the new Endpoint Manager URL.
- Minor adjustments related to formatting.

#### 2.1.7 02-24-19

- Lab **Configuring a WIP policy in Intune** was updated to address an issue where WIP was not blocking Internet Explorer. An additional domain boundary was added to account for sharepoint.com is not within the tenant AAD domain. Several steps were updated to reflect recent changes to the UI experience.
- Several labs were updated with corrected numerals in lists to address an issue that some lab hosts were having issues rendering the lists properly.

#### 2.1.8 12-02-19

- Lab **Connecting AD DS and Azure AD** - A new version of AD Connect was released in Nov 2019, which no longer supports using Domain Admin credentials. Updated lab to reflect new steps required to complete the lab.

#### 2.1.9 11-08-19

- An earlier draft version of several labs were committed. These were updated with the correct, final version of labs.

#### 2.1.10 11-04-19

- Initial Release

# 3 MD-101: Managing Modern Desktops

- **Download Latest Student Handbook and AllFiles Content**
- **Are you a MCT?** - Have a look at our GitHub User Guide for MCTs
- **Need to manually build the lab instructions?** - Instructions are available in the MicrosoftLearning/Docker-Build repository

## 3.1 What are we doing?

- To support this course, we will need to make frequent updates to the course content to keep it current with the services used in the course. We are publishing the lab instructions and lab files on GitHub to allow for open contributions between the course authors and MCTs to keep the content current with changes in the Azure platform.
- We hope that this brings a sense of collaboration to the labs like we've never had before - when Azure changes and you find it first during a live delivery, go ahead and make an enhancement right in the lab source. Help your fellow MCTs.

## 3.2 How should I use these files relative to the released MOC files?

- The instructor handbook and PowerPoints are still going to be your primary source for teaching the course content.
- These files on GitHub are designed to be used in conjunction with the student handbook, but are in GitHub as a central repository so MCTs and course authors can have a shared source for the latest lab files.
- It will be recommended that for every delivery, trainers check GitHub for any changes that may have been made to support the latest Azure services, and get the latest files for their delivery.

## 3.3 What about changes to the student handbook?

- We will review the student handbook on a quarterly basis and update through the normal MOC release channels as needed.

## 3.4 How do I contribute?

- Any MCT can submit a pull request to the code or content in the GitHub repro, Microsoft and the course author will triage and include content and lab code changes as needed.
- You can submit bugs, changes, improvement and ideas. Find a new Azure feature before we have? Submit a new demo!

## 3.5 Notes

### 3.5.1 Classroom Materials

It is strongly recommended that MCTs and Partners access these materials and in turn, provide them separately to students. Pointing students directly to GitHub to access Lab steps as part of an ongoing class will require

them to access yet another UI as part of the course, contributing to a confusing experience for the student. An explanation to the student regarding why they are receiving separate Lab instructions can highlight the nature of an always-changing cloud-based interface and platform. Microsoft Learning support for accessing files on GitHub and support for navigation of the GitHub site is limited to MCTs teaching this course only. Supporting files for both MD-100 and MD-101 are stored in the MD-100 GitHub repo.

https://github.com/MicrosoftLearning/MD-100T00-Windows10/tree/master/Allfiles/Labfiles/

# 4 Practice Lab: Managing Identities in Azure AD

## 4.1 Summary

In this lab, you will use the Azure Active Directory admin center to create and modify users, groups, and license assignments.

## 4.2 Exercise 1: Creating users in Azure AD

### 4.2.1 Scenario

You need to create user accounts in Azure AD for new employees that will start next week. New users are listed in the following table:

| Name | User Name | Password |
|---|---|---|
| Edmund Reeve | ereeve@yourtenant.onmicrosoft.com | Pa55w.rd |
| Miranda Snider | msnider@yourtenant.onmicrosoft.com | Pa55w.rd |
| Cody Godinez | cgodinez@yourtenant.onmicrosoft.com | Pa55w.rd |

*Note: For location use either your local region or United States.*

You've also been told that several more employees will be hired over the next couple of months. You've decided that scripting would be a far more efficient method of adding a large number of new users. You've decided to create a PowerShell script and test it out when you create Cody Godinez's account.

### 4.2.2 Task 1: Create users by using the Azure Active Directory admin center

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In the address bar, enter **http://portal.office.com**.
4. At the Sign-in prompt, enter **admin@yourtenant.onmicrosoft.com** and then select **Next**.
5. At the Enter password page, enter the password for the Admin account and then select **Sign in**. Note: Check with your instructor on the password to use for signing in with the Admin account.
6. At the Save password prompt, select **Save**.
7. At the Stay signed in prompt, select **No**. The Office 365 portal opens.
8. At the top corner, select the **App launcher** and then select **Admin**. The Microsoft 365 admin center opens.
9. Select the **Navigation menu** and then select **Show all**.
10. In the Navigation pane, under **Admin centers** select **Azure Active Directory**. The Azure Active Directory admin center opens.
11. In the Azure Active Directory admin center, in the navigation pane, select **Users**.
12. On the **Users | All users** page, select **New user**.
13. On the **New User** page, ensure that **Create user** is selected, enter the following:
    - User Name: **ereeve@yourtenant.onmicrosoft.com**
    - Name: **Edmund Reeve**
14. Select **Let me create the password.**

15. Next to **Initial password**, enter **Pa55w.rd**.
16. Under Settings, next to Usage location, select **United States**, and then select **Create**. If necessary, close the **Save password** prompt.
17. On the **Users | All users** page, select **New user**.
18. On the **New User** page, ensure that **Create user** is selected, enter the following:

```
- User Name: **msnider\@yourtenant.onmicrosoft.com**
- Name: **Miranda Snider**
```

19. Select **Let me create the password.**
20. Next to **Initial password**, enter **Pa55w.rd**.
21. Under Settings, next to Usage location, select **United States**, and then select **Create**. If necessary, close the **Save password** prompt.

#### 4.2.3 Task 2: Create users by using PowerShell

1. On SEA-CL1, on the taskbar, right-click **Start**, and then select **Windows PowerShell**.
2. In the **Windows PowerShell** window, type the following command, and then press **Enter**. If prompted, enter **Y** at the NuGet and repository messages:

```
Install-Module MSOnline
```

3. In the **Windows PowerShell** window, type the following command, and then press **Enter**:

```
Connect-MsolService
```

4. In the **Sign in to your account** dialog box, sign in as **admin@yourtenant.onmicrosoft.com** with the tenant password, and then select **Sign in**.
5. In the **Windows PowerShell** window, type the following code to create a new user, and then press **Enter**. Be sure to replace "yourtenant" with your assigned tenant name:

```
New-MsolUser -UserPrincipalName cgodinez@yourtenant.onmicrosoft.com -DisplayName "Cody Godinez" -FirstN
```

6. In the **Windows PowerShell** window, type the following command, and then press **Enter**:

```
Get-MsolUser
```

7. Verify that a list of users is displayed from your tenant.

**Results**: After completing this exercise, you will have successfully created new user accounts in Azure AD.

### 4.3 Exercise 2: Validating licenses and creating and managing groups

#### 4.3.1 Scenario

You need to review current license allocation for the tenant and modify the Company branding for the sign-in page.

You also need to add the three new users to a Security group and assign licenses as indicated in the table below.

| Name | Member of: | License to assign |
|---|---|---|
| Edmund Reeve | Contoso_Marketing | Office 365 E5, Enterprise Mobility + Security E5 |
| Miranda Snider | Contoso_Marketing | None |
| Cody Godinez | Contoso_Sales | None |

#### 4.3.2 Task 1: Review licenses and modify company branding

1. On SEA-CL1, switch to Microsoft Edge.
2. In the Azure Active Directory admin center, in the Navigation pane, select **Azure Active Directory**.
3. On the **Contoso|Overview** page, under **Manage**, select **Licenses**.

4. On the **Licenses|Overview** page, under **Manage**, select **All products**. Take note of the current licenses available and assigned for Enterprise Mobility + Security E5 and Office 365 E5.
5. In the Azure Active Directory admin center, in the Navigation pane, select **Azure Active Directory**.
6. On the **Contoso|Overview** page, under **Manage**, select **Company branding** and then select **Configure**.
7. On the Configure company branding page, configure the following settings and then select **Save**:
   - Sign-in page text: **Contoso Corp. Sign-in Page**
   - Show option to remain signed in: **Yes**
8. In the Azure Active Directory admin center, in the Navigation pane, select **Users**.
9. In the user list, select **Edmund Reeve**.
10. In the Edmund Reeve|Profile page, under Manage, select **Licenses**.
11. Select **Assignments**.
12. In the Update license assignments page, select the check box next to **Enterprise Mobility + Security E5** and **Office 365 E5**.
13. Select **Save**.

#### 4.3.3 Task 2: Create groups by using the Azure Active Directory admin center

1. On **SEA-CL1**, in the Azure Active Directory admin center, in the navigation pane, select **Azure Active Directory**.
2. On the **Contoso|Overview** page, under **Manage**, select **Groups**.
3. Select **New group**.
4. On the **New Group** page, enter the following:
   - Group type: Security
   - Group name: Contoso_Marketing
   - Membership type: Assigned
5. Under Members, select **No members selected**.
6. In the Add members page add **Edmund Reeve** and **Miranda Snider** and then click **Select**.
7. Select **Create**.

#### 4.3.4 Task 3: Create groups by using PowerShell

1. In the **Windows PowerShell** window, type the following code to create a new group, and then press **Enter**:

```
New-MsolGroup -DisplayName "Contoso_Sales" -Description "Contoso Sales team users"
```

2. In the **Windows PowerShell** window, type the following command, and then press **Enter**:

```
Get-MsolGroup
```

3. Verify that you get the list of groups in your tenant, including the Contoso_Sales group you just created.
4. In the **Windows PowerShell** window, type the following code to define a variable as the Contoso_Sales group, and then press **Enter**:

```
$group = Get-MsolGroup | Where-Object {$_.DisplayName -eq "Contoso_Sales"}
```

5. In the **Windows PowerShell** window, type the following code to define another variable as the user, and then press **Enter**:

```
$user = Get-MsolUser | Where-Object {$_.DisplayName -eq "Cody Godinez"}
```

6. In the **Windows PowerShell** window, type the following code to add Cody to Contoso_Sales using set variables, and then press **Enter**:

```
Add-MsolGroupMember -GroupObjectId $group.ObjectId -GroupMemberType "User" -GroupMemberObjectId $user.O
```

7. In the **Windows PowerShell** window, type the following code, and then press **Enter**:

```
Get-MsolGroupMember -GroupObjectId $group.ObjectId
```

8. Verify that you get **Cody Godinez** as a result. Minimize the **Windows PowerShell** window.
9. Close Windows PowerShell and Microsoft Edge.

**Results**: After completing this exercise, you should have successfully validated licenses, and created and managed groups.

**END OF LAB**

# 5 Practice Lab: Using Azure AD Connect to connect AD DS to Azure AD

## 5.1 Summary

In this lab, you will configure synchronization between Active Directory Domain Services and Azure Active Directory.

### 5.1.1 Scenario

Contoso Corporation is currently managing users in both AD DS and Azure AD as separate processes. This is time consuming and has led to inconsistent information. You have been tasked with addressing this issue by connecting the two directories by using the Azure AD Connect synchronization tool.

#### 5.1.1.1 Task 1: Configure directory synchronization with Azure AD Connect

1. On **SEA-SVR1**, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. On the taskbar, select **Internet Explorer**.
3. In the address bar, enter **http://www.microsoft.com/en-us/download/details.aspx?id=47594**.

   ***Important**: If you experience any problems with launching the download, add the https://download.microsoft.com website to your Trusted sites.*
4. On the Microsoft Azure Active Directory Connect page, select **Download** and then select **Save**. Azure AD Connect downloads.
5. Select **Open folder** and then in the Downloads window, double-click **AzureADConnect.msi**.
6. In the **Microsoft Azure Active Directory Connect** wizard, on the **Welcome to Azure AD Connect** page, select the **I agree to the license terms and privacy notice** check box, and then select **Continue**.
7. On the **Express Settings** page, select **Customize**.
8. On the **Install required components** page, select **Install**.
9. On the **User sign-in** page, ensure that **Password Hash Synchronization** is selected, and then select **Next**.
10. On the **Connect to Azure AD** page, in the **USERNAME** and **PASSWORD** boxes, enter **admin@yourtenant.onmicrosoft.com**, and your provided password, and then select **Next**.
11. On the **Connect your directories** page, ensure that **Contoso.com** is listed under **FOREST**, and then select **Add Directory**.
12. In the **AD forest account** window, select the **Create New AD Account** option, and in the **ENTERPRISE ADMIN USERNAME** field, type **Contoso\Administrator**, and then type **Pa55w.rd** in the **PASSWORD** field. Select **OK**, and then select **Next**.
13. On the **Azure AD sign-in configuration** page, ensure that in the **USER PRINCIPAL NAME** drop-down list, the **userPrincipalName** value is selected. Select **Continue without matching all UPN suffixes to verified domains** and then select **Next**.
14. On the **Domain and OU filtering** page, select **Sync selected domains and OUs**.

15. Expand **Contoso.com**, clear the checkbox next to **Contoso.com** and ensure that the only following check boxes are selected: **IT**, **Managers**, **Marketing**, **Research**, and **Sales**. Select **Next**.
16. On the **Uniquely identifying your users** page, select **Next**.
17. On the **Filter users and devices** page, select **Next**.
18. On the **Optional features** page, review available options, but do not make any changes. Ensure that **Password hash synchronization** is selected, and then select **Next**.
19. On the **Ready to configure** page, ensure that **Start the synchronization process when configuration completes** is selected, and then select **Install**.
20. When configuration is complete, select **Exit**.
*Note: At this time, synchronization of objects from your local Active Directory Domain Services (AD DS) and Azure AD begins. You should wait approximately 3-4 minutes for this process to complete.*
21. Close all open windows.

#### 5.1.1.2 Task 2: Verify synchronization in Azure AD

1. Switch to **SEA-CL1**.
2. On the taskbar, select **Microsoft Edge**.
3. In the address bar, enter **http://portal.office.com**.
4. At the Sign-in prompt, enter **admin@yourtenant.onmicrosoft.com** and then select **Next**.
5. At the Enter password page, enter the password for the Admin account and then select **Sign in**. Note: Check with your instructor on the password to use for signing in with the Admin account.
6. At the Save password prompt, select **Save**.
7. At the Stay signed in prompt, select **No**. The Office 365 portal opens.
8. At the top corner, select the **App launcher** and then select **Admin**. The Microsoft 365 admin center opens.
9. Select the **Navigation menu** and then select **Show all**.
10. In the Navigation pane, under **Admin centers** select **Azure Active Directory**. The Azure Active Directory admin center opens.
11. In the Azure Active Directory admin center, in the navigation pane, select **Users**.
12. Verify that you see users from your local AD DS. Ensure that these users have the value **Yes** in the **Directory synced** column.
13. In the Navigation pane, select **Azure Active Directory** and then select **Groups**. Verify that you see groups from your local AD DS.
14. Select the **Managers** group.
15. On the **Managers** group page, select **Members** and then ensure that you see users. Also, verify that you cannot add members or remove this group, as it is sourced from the local Active Directory.
16. Close Microsoft Edge.

**Results**: After completing this exercise, you should have successfully configured Azure AD Connect to synchronize between Active Directory Domain Services and Azure Active Directory.

**END OF LAB**

# 6 Practice Lab: Configuring and managing Azure AD Join

## 6.1 Summary

In this lab, you will configure Azure AD Join settings and perform both standard and hybrid Azure AD join scenarios for Windows 10 devices.

## 6.2 Exercise 1: Configuring Azure AD Join

### 6.2.1 Scenario

You need to configure Azure Active Directory device settings to ensure that all users are allowed to join devices to Azure AD. You also need to ensure that users can only join a maximum of 20 devices and that Megan Bowen is added as a local administrator on all Azure AD joined devices. Finally, you will verify that Azure AD join works as expected by joining SEA-WS1 to the tenant.

### 6.2.2 Task 1: Configure Azure AD join Device settings

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. On the taskbar select **Microsoft Edge**, in the address bar type **https://aad.portal.azure.com**, and then press **Enter**.
3. Sign in as user Admin@yourtenant.onmicrosoft.com, and use the tenant Admin password. If the **Stay signed in?** prompt appears, select **No**. The Azure Active Directory admin center opens.
4. In the Azure Active Directory admin center, in the navigation pane, select **Azure Active Directory**.
5. In the **Contoso|Overview** page, under **Manage**, select **Devices**. Notice that there are no devices found, as we have not joined any devices yet.
6. On the **Devices** pane, select **Device settings**.
7. In the details pane, under **Users may join devices to Azure AD**, verify that **All** is selected. This means that all Azure AD users are allowed to join their devices to Azure Active Directory.
8. In the **Devices to be Azure AD joined or Azure AD registered require Multi-factor Authentication** section, verify that the setting is set to **No**.
9. In the **Maximum number of devices per user** section, select **20**.
10. In the **Additional local administrators on all Azure AD joined devices** section, select **Manage Additional local administrators on all Azure AD joined devices**. The Device Administrators page opens.
11. In the Device Administrators page, select **Add assignments**.
12. In the Search box, enter **Megan Bowen**, select the **Megan Bowen** user object, and then select **Add**. Megan Bowen will now be added as a Device Administrator on all Azure AD joined devices.
13. Scroll back to or select the **Devices** navigation link at the top of the page.
14. On the Device settings page, select **Save**.
15. In the Azure Active Directory admin center, select **Dashboard**.

### 6.2.3 Task 2: Perform an Azure AD Join

1. Switch to **SEA-WS1** and sign in as **Admin** with the password of **Pa55w.rd**.
2. On the taskbar, select **Start** and then select **Settings**.
3. In the **Settings** window, select **Accounts**.
4. In the Accounts navigation pane, select **Access work or school**.
5. In the **Access work or school** page, select **Connect**.
6. In the **Microsoft account** window, select **Join this device to Azure Active Directory**.
7. On the **Sign in** page, type **JoniS@yourtenant.onmicrosoft.com** and then select **Next**.
8. On the **Enter password** page, enter the tenant password provided by your instructor.
9. On the **Make sure this is your organization** dialog box, select **Join**.
10. On the **You're all set!** page, select **Done**.
11. On the **Access work or school** page, verify that **Connected to Contoso's Azure AD** is displayed.
12. Close the **Settings** page.

### 6.2.4 Task 3: Validate Azure AD Join

1. On SEA-WS1, right-click **Start**, and then select **Windows PowerShell (Admin)**. At the User Account Control, select **Yes**.
2. In the PowerShell console, type the following and press **Enter**:

```
dsregcmd /status
```

3. In the output under **Device State**, verify that **AzureAdJoined : YES** is displayed. This indicates that the device is Azure AD joined.
4. Close PowerShell and sign out of SEA-WS1.
5. Switch to SEA-CL1.
6. In Microsoft Edge, in the Azure Active Directory admin center, select **Azure Active Directory**.
7. In the **Contoso** page, under **Manage**, select **Devices**. In the Devices pane, notice that SEA-WS1 is listed.
8. Verify that the **Join Type** is listed as **Azure AD joined** and that the owner is **Joni Sherman**. Also note that the MDM column shows None. This indicates that this device is not managed by Microsoft Intune.
9. In the Azure Active Directory admin center, select Azure Active Directory.

### 6.2.5 Task 4: Sign in to Windows 10 as an Azure AD User

1. Switch to SEA-WS1 and then sign in as **JoniS@yourtenant.onmicrosoft.com** with the Tenant password as provided by your instructor. Wait for the profile to be created.
2. At the **Use Windows Hello with your account** page, select **OK**.
3. On the **More information required** page, select **Next**.
4. On the **Keep your account secure** page, select **I want to set up a different method**.
5. In the **Choose a different method** dialog box, select **Phone** and then select **Confirm**.
6. On the **Phone** page, in the **Enter phone number** field, enter your mobile phone number which is able to receive text messages. Select **Next**.
7. When you receive the verification code, enter the code on the Phone page and then select **Next**.
8. On the verification page, select **Next** and then select **Done**.
9. On the **Set up a PIN** page, in the **New PIN** and **Confirm PIN** boxes, type **102938** and then select **OK**.
10. On the **All set!** page, select **OK**.

### 6.2.6 Task 5: Remove a Windows 10 device from Azure AD

1. On SEA-WS1, signed in as **JoniS@yourtenant.onmicrosoft.com**, select **Start** and then select **Settings**.
2. In the **Settings** window, select **Accounts**.
3. In the Accounts navigation pane, select **Access work or school**.
4. In the **Access work or school** page, select **Connected to Contoso's Azure AD**.
5. Select **Disconnect** and then select **Yes**.
6. On the **Disconnect from the organization** page, select **Disconnect**.
7. On the **Windows Security** dialog box, in the **Email address** box, enter **Admin** and in the **Password** box, type **Pa55w.rd**. Select **OK**.
8. In the **Restart your PC** dialog box, select **Restart now**.
9. After SEA-WS1 restarts, sign in as **Admin** with the password of **Pa55w.rd**.

**Results**: After completing this exercise, you will have configured Azure Active Directory device settings and joined a device to Azure AD.

## 6.3 Exercise 2: Configuring Hybrid Azure AD Join

### 6.3.1 Scenario

Some Contoso Windows devices are currently joined to the local Active Directory Domain Services. To enable those devices to seamlessly access cloud services you plan to enable hybrid Azure AD join. You will test hybrid Azure AD join by re-configuring Azure AD Connect and testing out the process on SEA-CL2.

### 6.3.2 Task 1: Prepare the environment

1. Switch to **SEA-SVR1** and sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. Select **Start**, expand **Windows Administrative Tools**, and then select **Active Directory Users and Computers**.
3. In **Active Directory Users and Computers**, right-click **Contoso.com**, point to **New**, and then select **Organizational Unit**.
4. In the **New-Object - Organizational Unit** dialog box, type **Azure AD clients** and then select **OK**.
5. In the navigation pane, select **Seattle Clients**.
6. Right-click **SEA-CL2** and then select **Move**.
7. In the **Move** dialog box, select **Azure AD clients** and then select **OK**.
8. Close **Active Directory Users and Computers**.

### 6.3.3 Task 2: Re-configure Azure AD Connect

1. On **SEA-SVR1**, on the **Desktop**, double-click **Azure AD Connect**.
2. In the **Microsoft Azure Active Directory Connect** window select **Configure**.
3. On the **Additional tasks** page, select **Customize synchronization options** and select **Next**.
4. On the **Connect to Azure AD** page enter the Admin Tenant password into the **PASSWORD** box, then select **Next**.
5. On the **Connect your directories** page, select **Next**.

6. On the **Domain and OU filtering** page, ensure that **Sync selected domains and OUs** is selected and then expand **Contoso.com**.
7. Select the check box next to **Azure AD clients**. Do not make any other changes and then select **Next**.
8. In the **Optional features** page, do not make any changes and then select **Next**.
9. In the **Ready to configure** window, select **Configure** to run the configuration and start synchronization.
10. When the configuration is complete, select **Exit**.
11. On the taskbar, right-click **Start** and select **Windows Powershell (Admin)**.
12. In the **Windows PowerShell** window, type the following command, and then press **Enter**:

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

13. Close the PowerShell window.

#### 6.3.4 Task 3: Configure hybrid Azure AD join in Azure Active Directory Connect

1. On **SEA-SVR1**, on the **Desktop**, double-click **Azure AD Connect**.
2. In the **Microsoft Azure Active Directory Connect** window select **Configure**.
3. On the **Additional tasks** page, select **Configure device options** and select **Next**.
4. On the **Overview** page, select **Next**.
5. On the **Connect to Azure AD** page, enter the Admin Tenant password into the **PASSWORD** box, then select **Next**.
6. On the **Device options** page, select **Configure Hybrid Azure AD join**, and then select **Next**.
7. On the **Device operating systems** page, select **Windows 10 or later domain-joined devices**, and then select **Next**.
8. On the **SCP configuration** page, select the check box next to **Contoso.com**. Select **Azure Active Directory** from the **Authentication Service** dropdown and select **Add**.
9. In the **Enterprise Admin Credentials** window enter **Contoso\Administrator** as **User name** and **Pa55w.rd** as **Password**. Select **OK** and select **Next**.
10. In the **Ready to configure** page, select **Configure** to run the configuration.
11. When the configuration is complete, select **Exit**.

#### 6.3.5 Task 4: Verify the Azure AD registration

1. Switch to **SEA-CL2**.
2. On the taskbar, right-click **Start**, select **Shut down or sign out** and then select **Restart**.

   *Note: The reboot will trigger the hybrid Azure AD join on SEA-CL2.*

3. After **SEA-CL2** has restarted, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
4. On the taskbar, right-click **Start** and select **Windows PowerShell (Admin)**.
5. In the **Windows PowerShell** window, type the following command, and then press **Enter**:

```
dsregcmd /status
```

6. In the output under **Device State**, verify that **AzureAdJoined : YES** and **DomainJoined : YES** are displayed.

   *Note: If the device is not yet joined to Azure AD wait for the Azure AD Connect sync to complete and reboot SEA-CL2 again.*

7. Close all windows on SEA-CL2 and sign out.
8. Switch to SEA-CL1 and ensure that you have the Azure Active Directory admin center open.
9. Select **Azure Active Directory**, and then select **Devices**.
10. Verify that **SEA-CL2** has **Hybrid Azure AD joined** as value for the row **Join Type** and that **Registered** contains a time stamp.
11. Close all windows and sign out of SEA-CL1.

**Results**: After completing this exercise, you will have successfully configured and validated hybrid Azure AD join.

**END OF LAB**

# 7 Practice Lab: Manage Device Enrollment into Intune

## 7.1 Summary

In this lab, you will prepare for device management using Microsoft Intune by reviewing and assigning licenses, configuring Windows automatic enrollment, and configuring enrollment restrictions.

### 7.1.1 Scenario

You need to prepare for device management using Microsoft Intune. First of all, you need to ensure that users are assigned appropriate licenses for device management. As a verification test, you will assign Aaron Nicholls the required licenses. You also need to ensure that any Windows 10 device that is joined or registered to Azure AD will automatically be enrolled into Intune. Finally you have been asked to ensure that members of the Sales group are restricted from enrolling personal Android and iOS devices into Intune.

### 7.1.2 Task 1: Review and assign licenses for device management

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. On the taskbar select **Microsoft Edge**, in the address bar type **https://aad.portal.azure.com**, and then press **Enter**.
3. Sign in as user Admin@yourtenant.onmicrosoft.com, and use the tenant Admin password. If the **Stay signed in?** prompt appears, select **No**. The Azure Active Directory admin center opens.
4. In the Azure Active Directory admin center, in the navigation pane, select **Azure Active Directory**.
5. On the **Contoso** page, under **Manage**, select **Licenses**.
6. On the **Licenses** page, under **Manage**, select **All products**. Take note of the licenses that are available in the tenant.
7. Select **Enterprise Mobility + Security E5**. Notice all the users that have been assigned this license. You can assign and remove licenses from this location.
8. Under **General**, select **Service plan detail**. Take note of the services included in the Enterprise Mobility + Security E5 license. Microsoft Intune is one of the supported services for this license.
9. In the Azure Active Directory admin center navigation pane, select **Users**.
10. Select **Aaron Nicholls**.
11. In the Aaron Nicholls pane, select **Edit**.
12. Under Settings, in the **Usage location** field, select **United States** and then select **Save**.

    *Note: Before you can assign a license to a user, the user must have a usage location set.*
13. In the Aaron Nicholls navigation pane, select **Licenses**.
14. In the Aaron Nicholls|Licenses pane, select **Assignments**.
15. In the **Update license assignments** page, select both **Enterprise Mobility + Security E5** and **Office 365 E5**, and then select **Save**.
16. In the Azure Active Directory admin center navigation pane, select **Dashboard**.

### 7.1.3 Task 2: Enable Windows Automatic Enrollment into Microsoft Intune

1. In **SEA-CL1**, open a new tab in **Microsoft Edge**, and then in the address bar type **https://endpoint.microsoft.com** and then press **Enter**. The Microsoft Endpoint Manager admin center opens.
2. In the Microsoft Endpoint Manager admin center, select **Devices**.
3. On the Devices pane, select **Enroll devices**.
4. In the Enroll devices pane, select **Windows enrollment**.
5. In the General section, select **Automatic Enrollment**.

6. On the **MDM user scope** row, select **All** and then select **Save**.

   ***Note**: By performing this step, you enabled automatic enrollment into Intune for any Windows device that performs an Azure AD join.*

#### 7.1.4 Task 3: Configure Enrollment Restrictions

1. In the Microsoft Endpoint Manager admin center, select **Devices**.
2. On the **Devices** pane, select **Enrollment restrictions**. Notice that you can specify Device type restrictions and Device limit restrictions.
3. In the details pane, select **Create restriction** and then select **Device type restriction**.
4. On the Create restriction page, in the Name box enter **Android and iOS Personal Device Restriction**. Select **Next**.
5. On the Platform settings page, under **Personally owned**, select **Block** for the following device types:
   - Android Enterprise (work profile)
   - Android device administrator
   - iOS/iPadOS
6. On the Platform settings page, select **Next**.
7. On the Scope tags page, select **Next**.
8. On the Assignments page, select **Select groups to include**.
9. Select **Sales** and then click **Select** and then click **Next**.
10. On the Review + create page, select **Create**.
11. In the Microsoft Endpoint Manager admin center, in the navigation pane, select **Home**.

**Results**: After completing this exercise, you will have successfully reviewed and assigned licenses, configured Windows automatic enrollment, and enabled and assigned enrollment restrictions.

**END OF LAB**

# 8 Practice Lab: Enrolling devices into Microsoft Intune

## 8.1 Summary

In this lab, you will join a Windows 10 client to Azure AD and verify that the device has automatically enrolled in to Microsoft Intune.

#### 8.1.1 Scenario

You have assigned Aaron Nicholls appropriate licenses and will now test the process of joining a Windows 10 device to Azure AD and have it automatically enroll in Microsoft Intune.

#### 8.1.2 Task 1: Automatically enroll a Windows 10 device to Microsoft Intune

1. Sign in to SEA-WS3 as **Admin** with the password of **Pa55w.rd**.
2. Select **Start** and then select **Settings**.
3. In **Settings**, select **Accounts**.
4. In the Accounts navigation pane, select **Access work or school**.
5. In the **Access work or school** page, select **Connect**.
6. In the **Microsoft account** window, select **Join this device to Azure Active Directory**.
7. On the **Sign in** page, type **Aaron@yourtenant.onmicrosoft.com** and then select **Next**.
8. On the **Enter password** page, enter **Pa55w.rd** and then select **Sign in**.
9. On the **Make sure this is your organization** dialog box, select **Join**.
10. On the **You're all set!** page, read the information and then select **Done**.
11. In the **Access work or school** section, verify that **Connected to Contoso's Azure AD** displays.
12. Select **Connected to Contoso's Azure AD** and then select **Info**.
13. Take note of the information regarding the areas managed by Contoso, scroll down, and then select **Sync**. This will force a Device sync with Intune.

14. Close the **Settings** window.

### 8.1.3 Task 2: Validate device enrollment into Azure AD And Intune

1. On the **SEA-WS3** taskbar, select **Start**, type **certlm.msc**, press **Enter** and when prompted select **Yes**.
2. In the **Certificates** console, in the navigation pane, expand **Personal** and select the **Certificate** node. Verify that the following certificates are listed in the details pane:
   - Microsoft Intune MDM Device CA
   - MS-Organization-Access
   - MS-Organization-P2P-Access [2021]

   This indicates that the device is enrolled in Azure AD and Intune.
3. Close the Certificates window.
4. Right-click **Start**, and then select **Windows PowerShell (Admin)**. When prompted select **Yes**.
5. In the PowerShell console, type the following and press **Enter**:

```
dsregcmd /status
```

6. In the output under **Device State**, verify that **AzureAdJoined : YES** is displayed. This indicates that the device is Azure AD joined.
7. In the output under **Tenant Details**, verify that the following three entries exist:

- mdmUrl : **https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc**
- mdmTouUrl : **https://portal.manage.microsoft.com/TermsofUse.aspx**
- mdmComplianceUrl : **https://portal.manage.microsoft.com/?portalAction=Compliance**

*Note: These entries indicate that the device is enrolled in Intune.*

### 8.1.4 Task 3: Sign in as an Azure AD user

1. Sign out of **SEA-WS3**.
2. Select **Other user**, and sign in as **Aaron@yourtenant.onmicrosoft.com** with the password **Pa55w.rd**. Wait for the profile to be created.
3. At the **Use Windows Hello with your account** page, select **OK**.
4. On the **More information required** page, select **Next**.
5. On the **Keep your account secure** page, select **I want to set up a different method**.
6. In the **Choose a different method** dialog box, select **Phone** and then select **Confirm**.
7. On the **Phone** page, in the **Enter phone number** field, enter your mobile phone number which is able to receive text messages. Select **Next**.
8. When you receive the verification code, enter the code on the Phone page and then select **Next**.
9. On the verification page, select **Next** and then select **Done**.
10. On the **Set up a PIN** page, in the **New PIN** and **Confirm PIN** boxes, type **102938** and then select **OK**.
11. On the **All set!** page, select **OK**.

### 8.1.5 Task 4: Verifying device enrollment in the Intune console

1. Switch to **SEA-CL1**.
2. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**. In the navigation pane, select **Devices**.
3. On the **Devices | Overview** blade under **Intune enrolled devices**, verify that 1 is displayed next to **Windows**. It may take a while to display.
4. On the **Devices | Overview** blade, select **All devices** and verify that **SEA-WS3** is listed.
5. Note that for SEA-WS3, the **Managed by** column displays **Intune** and the **Ownership** column displays **Corporate**.

*Note: This view lists devices that are joined to Azure AD. Remember that you configured automatic enrollment between Azure AD and Intune, and because of that, any device that is joined to Azure AD is automatically enrolled to Intune. Any devices joined prior to setting up enrollment are only joined to Azure AD, but not enrolled in Intune.*

6. Open a new tab in **Microsoft Edge**, in the address bar type **https://aad.portal.azure.com**, and then press **Enter**.
7. In the Azure Active Directory admin center, select **Azure Active Directory**.
8. In the Contoso page, select **Devices**. Take note of SEA-WS3. Notice that the Join Type column displays **Azure AD joined** and the MDM column displays **Microsoft Intune**.
9. Close all open Windows.

**Results**: After completing this exercise, you will have successfully joined a Windows 10 client to Azure AD and verified that the device has automatically enrolled in to Microsoft Intune.

**END OF LAB**

# 9 Practice Lab: Creating and Deploying Configuration Profiles

## 9.1 Summary

In this lab, you will use Microsoft Intune to create and apply a Configuration profile for a Windows 10 device.

## 9.2 Exercise 1: Create and apply a Configuration profile

### 9.2.1 Scenario

You need to use Azure Active Directory (Azure AD) and Intune to manage members of the Developers department at Contoso . You have been asked to evaluate the solutions that would enable the users to work effectively and securely on Windows 10 devices. Diego Siciliani has volunteered to help you test and evaluate the solution and provide feedback. He has also given you some initial requirements that must be included and applied to the developer's Windows 10 devices:

- The Gaming section in Settings should not be visible.
- The Privacy section in Settings should be restricted as much as possible.
- The C:\DevProjects folder must be excluded from Windows Defender.
- The process devbuild.exe must be excluded from Windows Defender.
- Most used apps and Recently added apps should not be displayed on the Start menu.

### 9.2.2 Task 1: Verify device settings before enrollment

1. Sign in to **SEA-WS2** as **Admin** with the password of **Pa55w.rd**.
2. On **SEA-WS2**, on the taskbar, select **Start** and then select **Settings**.
3. In **Settings**, verify that you can see the **Gaming** tile.
4. Select **Privacy** and verify that you can see several customization options.
5. Select the left arrow in the upper left corner to go back to the main Windows Settings page.
6. Select the **Personalization** tile and then in the navigation pane, select **Start**. Verify that **Show recently added apps** and **Show most used apps** are both set to **On**.
7. Select the left arrow in the upper left corner to go back to the main Windows Settings page.
8. In the **Settings** app, select **Update and Security**.
9. On the **Update & Security** page, select **Windows Security** and then **Open Windows Security**.
10. On the **Windows Security** page, select the **Open Navigation** button and then select **Virus & threat protection**.
11. On the **Virus & threat protection** page, under **Virus & threat protection settings**, select **Manage settings** . Scroll down to **Exclusions** and select **Add or remove exclusions**.
12. On the **Exclusions** page, verify that no exclusions have been configured.
13. Close the **Windows Security** window.
14. On the Settings page, select the left arrow in the upper left corner to go back to the main Windows Settings page.

### 9.2.3 Task 2: Join SEA-WS2 to Azure AD and Enroll in Intune

1. On **SEA-WS2**, with the **Settings** app still open, navigate to the **Accounts** page.
2. Select **Access work or school**. In the **Access work or school** section, select **Connect**.
3. In the **Microsoft account** window, on the **Set up a work or school account** page, select **Join this device to Azure Active Directory**.
4. On the **Sign in** page, type **DiegoS@yourtenant.onmicrosoft.com** and select **Next**.
5. On the **Enter password** page, enter the default Tenant password and then select **Sign in**.
6. On the **Make sure this is your organization** dialog box, select **Join**.
7. On the **You're all set!** page, select **Done**.
8. In the **Access work or school** section, verify that Connected to Contoso's Azure AD is displayed.
9. Close the Settings window.

### 9.2.4 Task 3: Sign in to SEA-WS2 with an Azure AD account

1. Sign out of **SEA-WS2**.
2. Select **Other user**, and in the **Email address** field type **DiegoS@yourtenant.onmicrosoft.com**.
3. In the Password field, enter the default tenant password and then press **Enter**.
4. At the **Use Windows Hello with your account** page, select **OK**.
5. On the **More information required** page, select **Next**.
6. On the **Keep your account secure** page, select **I want to set up a different method**.
7. In the **Choose a different method** dialog box, select **Phone** and then select **Confirm**.
8. On the **Phone** page, in the **Enter phone number** field, enter your mobile phone number which is able to receive text messages. Select **Next**.
9. When you receive the verification code, enter the code on the Phone page and then select **Next**.
10. On the verification page, select **Next** and then select **Done**.
11. On the **Set up a PIN** page, in the **New PIN** and **Confirm PIN** boxes, type **102938** and then select **OK**.
12. On the **All set!** page, select **OK**.

### 9.2.5 Task 4: Create device profile based on scenario

1. Switch to **SEA-CL1**.
2. On **SEA-CL1**, on the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. Sign in as **admin@yourtenant.onmicrosoft.com** with the tenant Admin password.
5. In the Microsoft Endpoint Manager admin center, select **Devices** from the navigation bar.
6. On the **Devices | Overview** page, select **Configuration Profiles**.
7. On the **Devices | Configuration profiles** blade, in the details pane, select **Create profile**.
8. In the **Create a profile** blade, select the following options, and then select **Create**:
   - Platform: **Windows 10 and later**
   - Profile: **Device restrictions**
9. In the **Basics** blade, enter the following information, and then select **Next**:
   - Name: **Contoso Developer - standard**
   - Description: **Basic restrictions and configuration for Contoso Developers.**
10. On the **Configurations settings** blade, expand **Control Panel and Settings**.
11. Select **Block** next to the **Gaming** and **Privacy** options.
12. On the **Device restrictions** blade, expand **Start**. Scroll down and select **Block** next to **Most used apps**, **Recently added apps** and **Recently opened items in Jump Lists**.
13. On the **Device restrictions** blade, scroll down and expand **Microsoft Defender Antivirus**.
14. Under **Microsoft Defender Antivirus,** scroll down and expand **Microsoft Defender Antivirus Exclusions**.

15. Under **Microsoft Defender Antivirus Exclusions** in the **Files and folders** box, type the following: **C:\DevProjects**.
16. In the **Processes** box, type the following: **DevBuild.exe**.
17. Then select **Next** three times until you reach the **Review + create** blade. Select **Create**.

#### 9.2.6 Task 5: Create the Contoso Developer device group

1. In the Microsoft Endpoint Manager admin center, in the navigation pane, select **Groups**.
2. On the **Groups | All groups** blade, select **New group**.
3. On the **New Group** blade, enter the following information:
   - Group type: **Security**
   - Group name: **Contoso Developer devices**
   - Group description: **All Windows 10 devices in Contoso Developer department**
   - Membership type: **Assigned**
4. Under **Members**, select **No members selected**.
5. On the **Add members** blade, in the **Search** box type **Sea**. Select **SEA-WS2** and then choose **Select**.
6. On the **New Group** blade, select **Create**.
7. On the **Groups | All groups** blade, verify that the **Contoso developer devices** group is displayed.

#### 9.2.7 Task 6: Create a dynamic Azure AD device group

1. On the **Groups | All Groups** blade, on the details pane, select **New group**.
2. On the **Group** blade, provide the following values:
   - Group type: **Security**
   - Group name: **Windows Devices**
   - Membership type: **Dynamic Device**
3. Under the **Dynamic Device Members** section, select **Add dynamic query**.
4. On the **Dynamic membership rules** blade, in the **Rule syntax** section, select **Edit**.
5. In the **Edit rule syntax** text box, add the following simple membership rule and select **OK**.

```
(device.deviceOSType -contains "Windows")
```

6. On the **Dynamic membership rules** blade, select **Save**.
7. On the **New Group** page, select **Create**.

#### 9.2.8 Task 7: Assign a Configuration profile to Windows 10 devices

1. In the Microsoft Endpoint Manager admin center, select **Home** in the breadcrumb navigation menu and then select **Devices**.
2. On the **Devices | Overview** blade, select **Configuration profiles**.
3. On the **Devices | Configuration profiles** blade, in the details pane, select the **Contoso Developer – standard** profile.
4. On the **Contoso Developer – standard** blade, select **Properties**. Scroll down to the **Assignments** section, and select **Edit**.
5. In the **Assignments** section, select **Select groups to include**.
6. On the **Select groups to include** blade, in the **Search** box, select **Contoso Developer devices** and then select **Select**.
7. Back on the **Device restrictions** blade, select **Review + save**, then select **Save**.
8. In the Microsoft Endpoint Manager admin center, select **Devices** in the breadcrumb navigation menu.

### 9.2.9 Task 8: Verify that Configuration profile is applied

1. Switch to **SEA-WS2**.
2. On **SEA-WS2**, on the taskbar, select **Start** and then select **Settings**.
3. In **Settings**, select the **Accounts** tile and then select **Access work or school**.
4. In the **Access work or school** section, select the **Connected to Contoso's Azure AD** link and then select **Info**.
5. In the **Managed by Contoso** page, select **Info**. Scroll down and then under Device sync status, select **Sync**. Wait for the synchronization to complete.

   *Note: The sync progress should only take a few seconds, however it may take up to 15 minutes before the profile is applied to Windows 10 device. Signing out or rebooting can accelerate this process.*
6. Close the **Settings** app, and open it again. Verify that the **Gaming** tile has been removed.
7. Select **Privacy** and notice that most of the privacy settings are now hidden. Select the left arrow in the upper left corner.
8. Select the **Personalization** tile and then select **Start**. Verify that **Show recently added apps** and **Show most used apps** are set to **Off**. Select the left arrow in the upper left corner.
9. In the **Settings** app, select **Update and Security**.
10. On the **Update & Security** page, select **Windows Security** and then **Open Windows Security**.
11. On the **Windows Security** page, select **Virus & threat protection**.
12. On the **Virus & threat protection** page, select **Manage settings** under **Virus & threat protection settings**. Scroll down to **Exclusions** and select **Add or remove exclusions**.
13. On the **Exclusion** page, verify that **C:\DevProjects** and **DevBuild.exe** are displayed.
14. Close the **Windows Security** page and then close the **Settings** app.

**Results**: After completing this exercise, you will have successfully created and assigned a Configuration profile for Windows 10 devices.

## 9.3 Exercise 2: Modify an assigned Configuration profile policy

### 9.3.1 Scenario

There was an exception to Contoso's policy that specifies that members of the Developer department should not have the Privacy options blocked in Settings on their devices. This change should be implemented and tested.

### 9.3.2 Task 1: Change settings in assigned profile

1. On **SEA-CL1**, in the Microsoft Endpoint Manager admin center, select **Devices | Configuration profiles** in the breadcrumb navigation pane.
2. On the **Devices | Configuration profiles** blade, in the details pane select **Contoso Developer - standard**.
3. On the **Contoso Developer - standard** blade, select **Properties**.
4. On the **Contoso Developer - standard|Properties** blade, on the **Configuration settings** line, select **Edit**.
5. On the **Configuration settings** page, expand **Control Panel and Settings**.
6. Next to **Privacy**, select **Not configured**.
7. Select **Review + save**, and then select **Save**.

### 9.3.3 Task 2: Force device synchronization from Microsoft Endpoint Manager admin center

1. On **SEA-CL1**, in the Microsoft Endpoint Manager admin center, select **Devices** in the navigation pane and then select **All devices**.
2. In the details pane, select **SEA-WS2**.
3. On the **SEA-WS2** blade, select **Sync** and when prompted select **Yes**.

   *Note: Intune will contact the device and tell it to synchronize all policies. This may take up to 5 minutes.*

### 9.3.4 Task 3: Verify profile changes on SEA-WS2

1. Switch to **SEA-WS2**.
2. On **SEA-WS2** and on the taskbar, select **Start** and then select the **Settings** app.
3. In the **Settings** app, select **Privacy** and verify that all of the customization options are back.
4. Close all open windows.

**Results**: After completing this exercise, you will have successfully modified an assigned Configuration profile and verified the changes.

**END OF LAB**

# 10 Practice Lab: Monitor device and user activity in Intune

## 10.1 Summary

In this lab, you will monitor user Sign-in activity, Audit logs, and device activity.

### 10.1.1 Scenario

You need to review Diego Siciliani's sign-in activity and general information provided by the Audit logs. You also need to verify the hardware on SEA-WS2 and confirm the configuration profile assigned to this device is successfully applied.

### 10.1.2 Task 1: Monitor user activity

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. Sign in as **admin@yourtenant.onmicrosoft.com** with the tenant Admin password.
5. On the **Microsoft Endpoint Manager admin center** page, select **Users**.
6. In the Users navigation pane, in the Activity section, select **Sign-ins**.
7. In the Details pane, user sign-ins are listed. Select on the first entry where the **User** column displays **Diego Siciliani**.
8. In the **Details** pane, Diego Siciliani´s sign-in details are displayed.
9. Select each of the main pages, including **Basic info**, **Location**, **Device info**, **Authentication Details**, and **Conditional Access**. Scroll to examine information on each page.
10. In the Users navigation pane, in the Activity section, select **Audit logs**.
11. In the details pane, audit information is displayed about administrative changes to users. Examine the information by selecting the various entries.

### 10.1.3 Task 2: Monitor device activity

1. In the Microsoft Endpoint Manager admin center, from the navigation pane, select **Devices**.
2. In the Devices navigation pane, select **Overview**.
3. In the details pane, take note of the device information for enrolled devices. Select the ellipse icon (if shown) to view all of the overview tabs. Available tabs include **Enrollment status**, **Enrollment alerts**, **Compliance status**, **Configuration status**, and **Software update status**. Select each tab to view information.
4. Select **All devices**, and in the details pane, select **SEA-WS2**. Information about the device such as name, Primary user, and operating system is displayed.
5. In the SEA-WS2 navigation pane, select **Hardware** and examine the hardware inventory.
6. In the SEA-WS2 navigation pane, select **Discovered apps** and examine the app inventory.
7. In the SEA-WS2 navigation pane, select **Device configuration** and in the details pane, take note of the Device configuration profiles assigned to the device. The **State** column should display **Succeeded**, which means that the profiles were applied successfully to the device.
8. In the details pane, select **Contoso Developer – standard**. On the **Contoso Developer – standard** blade, take note of each setting you configured in the profile. The **State** should display **Succeeded** next to all of them.
9. In the Microsoft Endpoint Manager admin center, from the navigation pane, select **Home**.

**Results**: After completing this exercise, you will have successfully monitored user Sign-in activity, Audit logs, and device activity.

**END OF LAB**

# 11 Practice Lab: Configuring Enterprise State Roaming

## 11.1 Summary

In this lab, you will enable Enterprise State Roaming in Azure AD.

### 11.1.1 Scenario

Enterprise State Roaming in Azure AD provides the ability for user settings and application settings to be synchronized to the cloud. Diego Siciliani works with multiple Windows devices and would like to have all user settings to be the same on each device. You need to enable and test Enterprise State Roaming to address Diego's requirements.

### 11.1.2 Task 1: Enable Enterprise State Roaming

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://aad.portal.azure.com** in the address bar, and then press **Enter**.
4. Sign in as **admin@yourtenant.onmicrosoft.com** with the tenant Admin password.
5. In the Azure Active Directory admin center, in the navigation pane, select **Azure Active Directory**.
6. On the **Contoso** blade, in the navigation pane, select **Devices**.
7. On the **Devices** blade, make a note of devices that are listed in the details pane. In the Devices navigation pane, select **Enterprise State Roaming**.
8. On the **Devices|Enterprise State Roaming** blade, in the details pane, next to **Users may sync settings and app data across devices** section, select **Selected**.
9. Select **Selected No member selected**, select **Add** and type **Diego Sicilian** in the text box.
10. Select **Diego Siciliani** and then select **Select**.
11. Select **OK**, and then select **Save**. Close the **Devices | Enterprise State Roaming** blade.

    *Note: By performing this task, you enabled Enterprise State Roaming for Diego Siciliani.*

### 11.1.3 Task 2: Verify sync is enabled on SEA-WS2

1. Switch to **SEA-WS2** and sign in as **DiegoS@yourtenant.onmicrosoft.com** with the default tenant password if you are not already signed in.
2. On the taskbar, select **Start** and then select the **Settings** icon.
3. Select **Accounts** and then select Access work or school.
4. In the **Access work or school** page, select **Connected to Contoso's Azure AD** and then select **Info**.
5. On the **Managed by Contoso** page, scroll down and then select **Sync**.
6. Select the Back button to return to the Accounts page.
7. In the **Accounts** navigation pane, select **Sync your settings**.
8. On the **Sync your settings** page, verify that **Sync settings** is set to **On**.

   ***Important**: If Sync settings is set to off and it is greyed out, restart the device and sign back in. If the settings remain greyed out then you must rejoin to Azure AD. This is due to an issue with ESR being enabled after devices have been enrolled. If this occurs, continue with Task 3, otherwise skip Task 3 and continue with Task 4.*

### 11.1.4 Task 3: Re-enroll SEA-WS2 (only perform if needed)

1. In Accounts, select **Access work or school**. Select **Connected to Contoso's Azure AD** and select **Disconnect**. Select **Yes** and then select **Disconnect** to confirm.
2. In the **Windows Security** dialog enter **Admin** as **Email Address** and **Pa55w.rd** as **Password**. Select **OK**.
3. On the **Restart your PC** dialog box, select **Restart now**.
4. After SEA-WS2 has restarted, sign in as **Admin**, with the password **Pa55w.rd**.
5. Select **Start**, type **View advanced system settings** and press **Enter**.
6. In the **Advanced** tab under **User Profiles** select **Settings**.
7. In the **User Profiles** window select **Account Unknown** and then select **Delete**. Confirm with **Yes** and then select **OK** twice.
8. Select **Start**, select **Settings**, and then select **Accounts**.
9. Select **Access work or school** and select **Connect**.
10. In the **Microsoft account** window, select **Join this device to Azure Active Directory**.
11. On the **Sign in** page, type **diegos@yourtenant.onmicrosoft.com** and then select **Next**.
12. On the **Enter password** page, enter the tenant password and select **Sign in**.
13. On the **Make sure this is your organization** dialog, select **Join**.
14. On the **You're all set!** page, select **Done**.
15. Sign out of SEA-WS2.
16. Sign in to **SEA-WS2** as **DiegoS@yourtenant.onmicrosoft.com** with the default tenant password.
17. At the **Use Windows Hello with your account** page, select **OK**.
18. At the **Enter code** page, enter the code that has been texted to your mobile device and then select **Verify**.
19. At the **Set up a PIN** dialog box, in the **New PIN** and **Confirm PIN** boxes, type **102938** and then select **OK**.
20. On the **All set!** page, select **OK**.

### 11.1.5 Task 4: Test Enterprise State Roaming

1. On SEA-WS2, on the taskbar, select **Start** and then select the **Settings** icon.
2. Select **Accounts** then select **Sync your settings**.
3. On the **Sync your settings** page, verify that **Sync settings** is set to **On**.
4. Close the Settings window.
5. On SEA-WS2 perform the following customizations:
   - Pin Feedback Hub, Calculator, and Calendar to the Start screen.
   - Pin Maps to the taskbar
   - Unlock the taskbar and move it to the right side of the screen.
6. On **SEA-WS2**, on the taskbar, select **Microsoft Edge** and in the address bar, type **www.microsoft.com/learn**, and then press **Enter**.
7. When the page loads, select the star and the end of the address bar (or press CTRL+D). In the **Favorite added** pop-up, select **Done**.
8. Close Microsoft Edge.
9. Sign out of **SEA-WS2**.
10. Switch to **SEA-WS3**.
11. Sign in to **SEA-WS3** as **DiegoS@yourtenant.onmicrosoft.com** with the default tenant password.
12. At the **Use Windows Hello with your account** page, select **OK**.
13. At the **Enter code** page, enter the code that has been texted to your mobile device and then select **Verify**.
14. At the **Set up a PIN** dialog box, in the **New PIN** and **Confirm PIN** boxes, type **102938** and then select **OK**.
15. On the **All set!** page, select **OK**.
16. On the taskbar, select **Microsoft Edge**.

17. In **Microsoft Edge**, press CTRL+I to view favorites. Verify if the Microsoft Learn favorites page is already synced from **SEA-WS2**.

    *Note: It can take several minutes for settings to sync. If the favorites option doesn't show, try rebooting and signing back in as DiegoS@yourtenant.onmicrosoft.com.*

18. Sign out of **SEA-WS3**.

**Results**: After completing this exercise, you will have successfully enable Enterprise State Roaming in Azure AD.

**END OF LAB**

# 12 Practice Lab: Deploying cloud apps using Intune

## 12.1 Summary

In this lab, you will create and deploy cloud-based apps using Intune and the Company Portal Website.

## 12.2 Exercise 1: Add a Microsoft Store App to Intune

### 12.2.1 Scenario

You use Microsoft Intune to manage desktops and apps for Contoso Corporation. The Research department often connects to various servers to perform tasks and has asked for the Windows 10 Microsoft Remote Desktop app to be available for Research members to install as needed. The Microsoft Remote Desktop is available from the Microsoft Store, but you decide to add the app to Intune so that users can access it from the Company Portal website. A Research member named Aaron Nicholls has agreed to test the installation process after you have published the app to the portal.

### 12.2.2 Task 1: Add Microsoft Remote Desktop to Intune

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. Sign in as **admin@yourtenant.onmicrosoft.com** with the tenant Admin password.
5. On the **Microsoft Endpoint Manager admin center** page, select **Apps**.
6. On the **Apps** page, in the navigation pane, select **All apps**.
7. In the details pane, select **Add**.
8. On the **Select app type** page, click the drop-down menu and then select **Microsoft Store app**.
9. Read the information about Microsoft store app and then click **Select**. The Add App page opens.
10. On the App information page, enter the following information and then select **Next**:
    - Name: Microsoft Remote Desktop
    - Description: Microsoft Remote Desktop for Research Department
    - Publisher: Microsoft
    - Appstore URL: https://www.microsoft.com/p/microsoft-remote-desktop/9wzdncrfj3ps
    - Category: Business
    - Show this as a featured app in the Company Portal: Yes
11. Select **Next** and then select **Create**.
12. The Microsoft Remote Desktop page opens. Take note of the Properties, Device install status, and User install status nodes.

### 12.2.3 Task 2: Assign a Group to the App

1. In the Microsoft Remote Desktop page, select **Properties**.
2. In the details pane, scroll down to the **Assignments** section and then select **Edit**.
3. On the **Assignments** page, select **Add group**.
4. On the **Select groups** page, select the **Research** group and then click **Select**.
5. Select **Review + save** and then select **Save**.

### 12.2.4 Task 3: Install an app from the Company Portal Website

1. Switch to **SEA-WS3**.
2. Select **Other user**, and sign in as **Aaron@yourtenant.onmicrosoft.com** with the password **Pa55w.rd**.
3. On the taskbar, select **Microsoft Edge**.
4. In the address bar browse to https://portal.manage.microsoft.com.
5. Sign in as **Aaron@yourtenant.onmicrosoft.com** with the PIN **102938**.
6. On the Contoso web portal, select **Devices**.
7. On the Devices page, select **Tap here to tell us which device you're using or add a new device**.
8. On the **Which device are you using** dialog box select the option next to **SEA-WS3**, and then select **Select**. Notice that the message now changes to Apps will be installed onto: SEA-WS3.
9. At the top-left corner, select the navigation button and then select **Apps**. Take note of the Microsoft Remote Desktop app listed on the Apps page.
10. Select **Microsoft Remote Desktop**.
11. On the Microsoft Remote Desktop page, select **View in Store**.
12. On the **This site is trying to open Microsoft Store**, select **Open**.
13. On the **Microsoft Remote Desktop** page, select **Get**.
14. At the Use across your devices message, select **No, thanks**. The app starts to download and installs on SEA-WS3.
15. After the app is installed close all open windows.
16. Select Start and verify that **Remote Desktop** is displayed on the Start menu.

**Results**: After completing this exercise, you will have successfully added and installed a Microsoft Store App from Intune.

## 12.3 Exercise 2: Configure and deploy Microsoft 365 Apps from Intune

### 12.3.1 Scenario

All the developers at Contoso require Microsoft 365 Apps. You've been asked to deploy the 64-bit versions of Microsoft Excel, Outlook, PowerPoint and Word to their Windows 10 devices. You also need to ensure they are configured for the Current Channel for updates.

### 12.3.2 Task 1: Verify installed apps on SEA-WS2

1. On **SEA-WS2**, sign in as **DiegoS@yourtenant.onmicrosoft.com** with the default tenant password.
2. On the taskbar, select **Start** and then select the **Settings** app.
3. In the **Settings** app, select the **Apps** tile and on the **Apps & features** page, select **Programs and Features** under **Related Settings**.
4. In the **Program and Features** window, verify that **Microsoft 365 Apps for enterprise - en-us** is not listed.
5. Close all open windows.

### 12.3.3 Task 2: Add Microsoft 365 apps to Intune

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. Sign in as **admin@yourtenant.onmicrosoft.com** with the tenant Admin password.
5. On the **Microsoft Endpoint Manager admin center** page, select **Apps**.
6. In the **Apps | Overview** blade, select **All Apps**. In the details pane, select **Add**.
7. In the **Select app type** blade, select **Windows 10** under **Microsoft 365 Apps**, and then select **Select**.
8. On the **Microsoft 365 Apps** blade, configure the following options and select **Next**:
   - Suite Name: **Microsoft 365 Apps (Contoso developers)**
   - Suite Description: **Microsoft 365 Apps for developers at Contoso**
9. On the **Configure app suite** blade, expand the **Select Office apps** dropdown, select the following Office 365 apps and select **Next**:

- Excel
- Outlook
- PowerPoint
- Word

10. On the **Configure app suite** tab, configure the following options and select **Next**:
    - Architecture: **64-bit**
    - Update channel: **Current Channel**
    - Accept the Microsoft Software License Terms on behalf of users: **Yes**
11. On the **Assignments** tab, in the **Required** section, select **Add group.**
12. On the **Select groups** blade, select **Contoso Developer devices**, and then choose **Select**.
13. Select **Next**. On the **Review + Create** tab, select **Create**.
14. On the **Microsoft 365 Apps (Contoso developers)** page, select **Properties**.
15. In the details pane verify that **Contoso Developer devices** is listed under **Required** in the Assignments section.

#### 12.3.4 Task 3: Force policy synchronization from the Intune console

1. In the **Microsoft Endpoint Manager admin center**, select **Devices** and then select **All devices**.
2. In the details pane, select **SEA-WS2**.
3. On the **SEA-WS2** blade, select **Sync** and when prompted select **Yes**. Intune will contact the device and tell it to synchronize all policies. This may take up to 5 minutes.

#### 12.3.5 Task 4: Verify Microsoft 365 apps are installed

1. Switch to **SEA-WS2** and wait approximately 10-15 minutes for the Office 365 Suite to install on the device.
2. On **SEA-WS2**, on the taskbar, select **Start** and then select the **Settings** app.
3. In the **Settings** app, select the **Apps** tile and on the **Apps & features** page, scroll down and verify that **Microsoft 365 Apps for enterprise - en-us** is listed.
4. Close the **Settings** app and select the **Start** button.
5. In the app list, scroll down to **W** and select **Word** and verify that the app opens.
6. Close all open windows.

#### 12.3.6 Task 5: Monitor app installation status in Intune

1. Switch to **SEA-CL1**.
2. In the **Microsoft Endpoint Manager admin center**, select **Apps**.
3. On the **Apps | Overview** blade, select **Monitor** and then select **App install status**. In the details pane, select **Microsoft 365 Apps (Contoso developers)**.
4. In the details pane, under **Device status** and under **User status**, verify that **1** is displayed under Installed.

   *Note: This indicates that the app is installed on one device and for one user. Note that it may take some time for the information to display.*
5. Select **Device install status**. In the details pane, you can see the devices that the app is installed on, and also the name of the user. The **Device Name** column should list **SEA-WS2** and the **Status** column should say **Installed**. This means that the app is installed on SEA-WS2.
6. In the **Microsoft Endpoint Manager admin center**, select **Devices**.
7. On the **Devices | Overview** blade, select **All devices** and then in the details pane, select **SEA-WS2**.
8. On the **SEA-WS2** blade, select **Managed Apps**.

9. On the **SEA-WS2 | Managed Apps** blade, in the details pane, select **Microsoft 365 Apps (Contoso developers)**.
10. On the **Microsoft 365 Apps (Contoso developers) - Installation details** blade, you can see the entire lifecycle of the application, that is - when it was created, assigned, installation time and status and the last time the device checked in (synced with Intune).
11. Close all open windows.

**Results**: After completing this exercise, you will have successfully configured and deployed Microsoft 365 Apps from Intune.

**END OF LAB**

# 13 Practice Lab: Configure App Protection Policies for Mobile Devices

## 13.1 Summary

In this lab, you will configure an App protection policy for a mobile device.

### 13.1.1 Scenario

All of the developers at Contoso have iPhones running the latest version of iOS. The security department in is concerned with data leaks and wants to prevent data from the corporate e-mail to be copied out to other apps on the mobile devices. You must provide a solution that addresses the concerns from the security department. You need to ensure the following:

- Outlook data must be restricted from backing up to iTunes or iCloud.
- Only policy managed apps can send and receive data from Outlook.
- Only policy managed apps can cut, copy, or paste with Outlook.
- Users must provide their Work or school account credentials for access to Outlook.

### 13.1.2 Task 1: Create an App protection policy in Intune

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. Sign in as **admin@yourtenant.onmicrosoft.com** with the tenant Admin password.
5. On the **Microsoft Endpoint Manager admin center** page, select **Apps**.
6. On the **Apps | Overview** blade, under **Policy**, select **App protection policies**.
7. In the details pane, select **Create policy** and then select **iOS/iPadOS**.
8. On the **Basics** tab, configure the following options and select **Next**:
   - Name: **Outlook – Developers**
   - Description: **Policy to prevent cut/copy and paste from Outlook**
9. On the **Apps** tab, select **Select public apps**.
10. On the **Select apps to target** blade, in the text box, type **Outlook**. Select **Microsoft Outlook** and then select **Select**, and then select **Next**.
11. On the **Data protection** tab, configure the following options and select **Next**:
    - Backup Org data to ITunes and iCloud backups: **Block**
    - Send Org data to other apps: **Policy managed apps**
    - Receive data from other apps: **Policy managed apps**
    - Restrict cut, copy, and paste with other apps: **Policy managed apps**
    - Leave all other settings at default

12. On the **Access requirements** tab, configure the following options and select **Next**:
    - PIN for access: **Not required**
    - Work or school account credentials for access: **Require**
13. On the **Conditional launch** tab, review the settings. Select **Next**.

    *Note: Here you can set the sign-in security requirements for your access protection policy. You can select a setting and enter the value that users must meet to sign in to your company app. Make note of the various settings but do not change anything.*
14. On the Assignments tab, under **Included groups** select **Add groups**.
15. Select the **Contoso Developer devices** group, then choose **Select**.
16. Select **Next**. On the **Review + create** tab, review the settings and select **Create**.
17. On the **Apps | App protection policies** blade, in the details pane, verify that **Outlook - Developers** is listed.
18. Close Microsoft Edge.

**Results**: After completing this exercise, you will have successfully configured an App protection policy for a mobile device.

**END OF LAB**

# 14 Practice Lab: Deploy Apps using Endpoint Configuration Manager

## 14.1 Summary

In this lab, you will use Microsoft Endpoint Configuration Manager to deploy applications to desktop client workstations.

### 14.1.1 Scenario

Contoso uses Microsoft Endpoint Configuration Manager to manage desktop workstations within the environment. You need to deploy a new application named Microsoft PowerBI desktop to the Windows 10 Configuration Manager clients. The Endpoint Configuration Manager administrator has already created the application object for you. Your tasks include creating a collection for the target devices, distributing the application content to distribution points, and then creating the deployment assigned to the target collection. You will verify the process by ensuring that the application is displayed in the Software Center on SEA-CL1.

### 14.1.2 Task 1: Create a device collection

1. On **SEA-CFG1**, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Configuration Manager Console**. The Microsoft Endpoint Configuration Manager console opens.
3. In the **Assets and Compliance** workspace, select **Device Collections**.
4. Right-click **Device Collections** and then select **Create Device Collection**. The Create Device Collection Wizard opens.
5. On the **General** page, configure the following and then select **Next**:
    - Name: **PowerBI App Deployment**
    - Comment: **Devices targeted to install PowerBI Desktop**
    - Limiting collection: **All Windows 10 Workstations**
6. On the **Membership Rules** page, select **Next**. At the Configuration Manager warning, select **OK**. You will add a direct member at a later step.
7. On the **Summary** page, select **Next** and then at the **Completion** page, select **Close**. The **PowerBI App Deployment** collection is displayed in the Device Collections list.

### 14.1.3 Task 2: Assign a Device to an existing Collection

1. In the **Assets and Compliance** workspace, select **Devices**. Take note of the devices listed. Any device that has a green circle with a white checkmark are currently active.
2. In the details pane, select **SEA-CL1**.

3. Right-click **SEA-CL1**, point to **Add Selected Items**, and then select **Add Selected Items to Existing Device Collection**.
4. On the **Select Collection** dialog box, select **PowerBI App Deployment**, and then select **OK**.
5. To verify, in the **Assets and Compliance** workspace, select **Device Collections** and then double-click **PowerBI App Deployment**. SEA-CL1 should be listed as a member of this collection.

#### 14.1.4 Task 3: Configure a deployment type

1. In the Microsoft Endpoint Configuration Manager console select the **Software Library** workspace.
2. In the **Software Library** workspace, expand **Application Management** and then select **Applications**. Notice the applications that have been created by the Endpoint Configuration Manager administrator.
3. In the details pane, select **Microsoft Power BI Desktop (x64)**.
4. In the results pane, select the **Deployment Types** tab. Notice that there is one deployment type that is based upon Windows Installer.
5. Right-click the **Microsoft PowerBI Desktop (x64) - Windows installer** deployment type and then select **Properties**.
6. In the **Properties** dialog box, select the **Programs** tab. Take note of how the application is installed. It will use msiexec with the /q switch which performs a quiet installation.
7. In the **Properties** dialog box, select the **Requirements** tab and then select **Add**.
8. In the **Create Requirement** dialog box, configure the following and then select **OK**:
   - Category: Device
   - Condition: Operating System
   - Rule type: Value
   - Operator: One of Windows 10 (Select the check box next to Windows 10)
9. In the **Properties** dialog box, select **OK**. This requirement will prevent the app from installing on any operating system except Windows 10.

#### 14.1.5 Task 4: Distribute content to distribution points

1. In the **Software Library** workspace, select **Microsoft Power BI Desktop (x64)**.
2. Right-click **Microsoft Power BI Desktop (x64)** and then select **Distribute Content**.
3. On the **General** page, select **Next**.
4. On the **Content** page, select **Next**.
5. On the **Content Destination** page, select **Add** and then select **Distribution Point**.
6. On the **Add Distribution Points** dialog box, select the check box next to **SEA-CFG1.CONTOSO.COM**, and then select **OK**.
7. On the **Content Destination** page, select **Next**.
8. On the **Summary** page, select **Next** and then select **Close**.
9. In the results pane, select **Content Status**. The Content Status page opens for Microsoft Power BI Desktop. In the results pane, verify that a green circle is displayed and that Success:1 displays next to the circle. This indicates that the content is now distributed to the distribution points and can now be deployed to devices.
10. In the top left corner select the **Back to Applications** arrow to return to the Software Library Applications node.

#### 14.1.6 Task 5: Create a deployment

1. In the **Software Library** workspace, select **Microsoft Power BI Desktop (x64)**.
2. Right-click **Microsoft Power BI Desktop (x64)** and then select **Deploy**. The **Deploy Software Wizard** opens.
3. On the **General** page, next to **Collection**, select **Browse**.
4. On the **Select Collection** page, select **User Collections** and then select **Device Collections**.
5. In the **Device Collections** list, select **PowerBI App Deployment** and then select **OK**.
6. On the **General** page, select **Next**.
7. On the **Content** page, select **Next**.
8. On the **Deployment Settings** page, verify that the **Action** is set to **Install** and the **Purpose** is set to **Available**. Select **Next**.
9. On the **Scheduling** page, select **Next**. The application will be available as soon as possible by default.
10. On the **User Experience** page, next to **User notifications**, select **Display in Software Center and show all notifications**. Select **Next**.
11. On the **Alerts** page, select **Next**.
12. On the **Summary** page, select **Next** and then select **Close**.

13. In the results pane, on the **Deployments** tab, verify that the deployment displays.

#### 14.1.7 Task 6: Use Software center to install a deployed app

1. Switch to SEA-CL1, and if necessary sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. Click **Start** and then enter **Control Panel**.
3. In the results, select **Control Panel**.
4. In the **Control panel**, select **System and Security**.
5. In **System and Security**, select **Configuration Manager**. Configuration Manager Properties is displayed.
6. In the **Configuration Manager Properties** dialog box, select the **Actions** tab.
7. On the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle**, and then select **Run Now**. At the message prompt, select **OK**.
8. Select **OK** to close the **Configuration Manager Properties**, and then close **Control Panel**.
9. In the notification area, select **New Software is Available** and then select **Open Software Center**. You might need to expand the notification area arrow to display the icon.
10. In the **Software Center**, on the **Applications** page, notice the new application available named **Microsoft Power BI Desktop (x64)**. This application is now available to any device that is a member of the **PowerBI App Deployment** collection created previously.
11. Select **Microsoft Power BI Desktop (x64)** and then select **Install**. The application downloads and installs without user input. You will know that the install was successful when the **Power BI Desktop** shortcut displays on the desktop.
12. Close Software Center.

**Results**: After completing this exercise, you will have successfully used Microsoft Endpoint Configuration Manager to deploy applications to desktop client workstations.

**END OF LAB**

# 15 Practice Lab: Deploy Apps using Microsoft Store for Business

## 15.1 Summary

In this lab, you will configure and deploy cloud-based apps using Microsoft Store for Business integrated with Microsoft Intune.

## 15.2 Exercise 1: Add a Microsoft Store App to Intune

### 15.2.1 Scenario

You have decided to integrate Microsoft Store for Business with Intune. You need to configure the Microsoft Store for Business integration settings and the test out the purchase and adding of the apps to the private Contoso app store. You also need to ensure that only people that you assign a purchasing role to are able to buy Microsoft Store for Business apps.

### 15.2.2 Task 1: Configure Microsoft Store for Business settings and integration with Intune

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://www.microsoft.com/en-us/business-store** in the address bar, and then press **Enter**.
4. In the top right-hand corner, select **Sign in** to sign in as **admin@yourtenant.onmicrosoft.com** with the tenant Admin password.
5. In the menu bar, select **Manage**. The **Overview** page displays.
6. On the **Overview** page, select **Settings**.
7. On the **Shop** page, under **Shopping behavior**, configure the **Make everyone a Basic Purchaser** setting to **Off**.
8. At the **Stop people from buying** message, select **Don't let people buy**. This restricts Microsoft Store for business purchases to only users that you have specifically assigned a purchasing role to.
9. Select the **Distribute** page.
10. On the Distribute page, take note of the current name for the private store. The current name is the name associated with the tenant.

11. Under Management tools, verify that **Microsoft Intune** Status is set to **Active**. If it is not, under Action select **Activate**.
12. In Microsoft Edge, open a new tab and browse to https://endpoint.microsoft.com. The Microsoft Endpoint Manager admin center opens.
13. In the Microsoft Endpoint admin center, in the navigation pane, select **Tenant administration**.
14. In the **Tenant admin** navigation pane, select **Connectors and tokens**.
15. On the **Connectors and tokens** page, select **Microsoft Store for Business**.
16. If necessary, on the **Microsoft Store for Business** page, select **Enable** and then select **Save**. The status should display as **Active**.
17. At the bottom of the Microsoft Store for Business page, select **Sync**.

#### 15.2.3 Task 2: Purchasing and Adding apps to the Private Store

1. In Microsoft Edge, switch to the **Microsoft Store for Business** tab (if there's no tab click on the url link **Open business store**).
2. In the menu bar, select **Shop for my group**.
3. Scroll down to the **Made by Microsoft** section.
4. In the **Made by Microsoft** section, select **Network Speed Test**.
5. On the **Network Speed Test** page, select **Get the app**.
6. Click on the box next to the **I accept this agreement** and select **Accept**
7. On the **Thanks for your order** page, select **Close**.
8. On the Network Speed Test page, select the ellipse button and then select **Manage**.
9. On the Network Speed Test manage page, select the **Private store availability** tab.
10. On the **Private store availability** tab, under **Choose groups of people who can see this app**, select **Everyone**.
11. Repeat steps 2-10 and select the app named **Fresh Paint**.
12. In the menu bar, select **Contoso**. This is a view of the private store which displays the apps that you have purchased and made available to users.

#### 15.2.4 Task 3: Review the apps in the Company store

1. Switch to **SEA-WS3**.
2. Sign in as as Aaron Nicholls with the PIN **102938**.
3. On the taskbar, select **Microsoft Store**.
4. In the **Microsoft Store**, in the menu bar select **Contoso**. (You may have to select More to display the Contoso menu item.)
5. In the **Contoso** store, review the apps that are available. You should see Fresh Paint and Network Speed Test as available options.
6. Close the Microsoft Store.

**Results**: After completing this exercise, you will have successfully integrated Microsoft Store for Business with Intune.

### 15.3 Exercise 2: Deploy Microsoft Store for Business Apps using Intune

#### 15.3.1 Scenario

Now that you have integrated Microsoft Store for Business with Intune, you need to verify that you can successfully deploy the apps to devices. You decide to deploy the Network Speed Test app to all devices. Aaron Nicholls has agreed to test out the app to make sure it is deployed successfully.

#### 15.3.2 Task 1: Synchronize Intune with Microsoft Store for Business

1. Switch to **SEA-CL1**.
2. In Microsoft Edge, switch to the tab that contains Microsoft Endpoint Manager admin center.
3. In the Microsoft Endpoint admin center, in the navigation pane, select **Tenant administration**.
4. In the **Tenant admin** navigation pane, select **Connectors and tokens**.
5. On the **Connectors and tokens** page, select **Microsoft Store for Business**.
6. At the bottom of the Microsoft Store for Business page, select **Sync**.

#### 15.3.3 Task 2: Deploy Microsoft Store for Business apps

1. On the **Microsoft Endpoint Manager admin center** pane, select **Apps**.

2. In the **Apps | Overview** blade, select **All Apps**. Notice the Apps that have synced from Microsoft Store for Business.
3. In the app list, select **Network Speed Test (Online)**.
4. On the **Network Speed Test (Online)** pane, select **Properties**.
5. Scroll down to the **Assignments** section and then select **Edit**.
6. On the **Edit application** page, under **Required**, select **Add all devices**.
7. Select **Review + save** and then select **Save**.

#### 15.3.4 Task 3: Force policy synchronization from the Intune console

1. In the **Microsoft Endpoint Manager admin center**, select **Devices** and then select **All devices**.
2. In the details pane, select **SEA-WS3**.
3. On the **SEA-WS3** blade, select **Sync** and when prompted select **Yes**. Intune will contact the device and tell it to synchronize all policies. This may take up to 5 minutes.

#### 15.3.5 Task 4: Verify the app has installed

1. Switch to **SEA-WS3** and if necessary sign in as Aaron Nicholls with the PIN **102938**. Wait approximately 5 minutes for the app to install on the device.
2. On **SEA-WS3**, on the taskbar, select **Start** and then select the **Settings** app.
3. In the **Settings** app, select the **Apps** tile and on the **Apps & features** page, scroll down and verify that **Network Speed Test** is listed.
4. Close the **Settings** app and select the **Start** button.
5. In the app list, scroll down to **T** and select **Network Speed Test** and verify that the app opens.
6. Close all open windows.

#### 15.3.6 Task 5: Monitor app installation status in Intune

1. Switch to **SEA-CL1**.
2. In the **Microsoft Endpoint Manager admin center**, select **Apps** in the navigation menu.
3. On the **Apps | Overview** blade, select **Monitor** and then select **App install status**. In the details pane, select **Network Speed Test (Online)**.
4. In the details pane, under **Device status** and under **User status**, verify that **1** is displayed under Installed.

   *Note: This indicates that the app is installed on one device and for one user. Note that it may take some time for the information to display.*
5. Select **Device install status**. In the details pane, you can see the devices that the app is installed on, and also the name of the user.
6. In the **Microsoft Endpoint Manager admin center**, select **Devices**.
7. On the **Devices | Overview** blade, select **All devices** and then in the details pane, select **SEA-WS3**.
8. On the **SEA-WS3** blade, select **Managed Apps**.
9. On the **SEA-WS3 | Managed Apps** blade, in the details pane, select **Network Speed Test**.
10. On the **Network Speed Test - Installation details** blade, you can see the entire lifecycle of the application, that is - when it was created, assigned, installation time and status and the last time the device checked in (synced with Intune).
11. Close all open windows.

**Results**: After completing this exercise, you will have successfully deployed a Microsoft Store for Business app to a Windows 10 device using Intune.

**END OF LAB**

# 16 Practice Lab: Configuring Multi-factor Authentication

## 16.1 Summary

In this lab, you will configure and test per-user multi-factor authentication (MFA) and MFA using conditional access.

## 16.2 Exercise 1: Configure per-user multi-factor authentication

### 16.2.1 Scenario

To provide additional security for user sign on events, you need to configure and test multi-factor authentication (MFA). You decide to first test out per-user MFA. Alex Wilber has agreed to validate the settings for you.

### 16.2.2 Task 1: Validate sign-in before enabling MFA

1. Sign in to **SEA-WS1** as **Admin** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In the address bar, enter **outlook.office.com** and press Enter.
4. At the **Sign in** page, enter **AlexW@yourtenant.onmicrosoft.com** and then select **Next**.
5. On the **Enter password** page, enter the tenant password. At the Edge Save password prompt, select **Save**.
6. In Outlook, close the **Welcome** page. Take note that only the password was required to sign in to Outlook on the Web.
7. At the top-right corner, select the **Account manager for Alex Wilber** and then select **Sign out**.
8. Close Microsoft Edge.

### 16.2.3 Task 2: Enable MFA for a user

1. Switch to **SEA-CL1**.
2. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
3. On the taskbar select **Microsoft Edge**, in the address bar type **https://aad.portal.azure.com**, and then press **Enter**.
4. Sign in as user **Admin@yourtenant.onmicrosoft.com**, and use the tenant Admin password. If the **Stay signed in?** prompt appears, select **No**. The Azure Active Directory admin center opens.
5. In the Azure Active Directory admin center, in the navigation pane, select **Users**.
6. Select **All users** and then at the top of the results pane select **Multi-Factor Authentication**. You may need to select the ellipse first to view the Multi-Factor Authentication option.
7. On the multi-factor authentication page, select **service settings**.
8. Scroll down to the **verification options** section. Take note of the various methods that can be configured for user verification. Do not make any changes.
9. In the **remember multi-factor authentication on trusted device** section, select the check box next to **Allow users to remember multi-factor authentication on devices they trust**.
10. Next to **Number of days users can trust devices for**, enter **30** and then select **save**. Select **close** when prompted.
11. At the top of the page, under **multi-factor authentication**, select **users**.
12. In the user list, select the check box next to **Alex Wilber**.
13. In the Alex Wilber page, select **Enable**.
14. On the **About enabling multi-factor auth** message, select **enable multi-factor auth**.
15. On the **Updates successful** message, select **close**. Take note that the **Multi-Factor Auth Status** for Alex Wilber is now **Enabled**.
16. Close Microsoft Edge.

### 16.2.4 Task 3: Register and Validate MFA

1. Switch to **SEA-WS1**.
2. On the taskbar, select **Microsoft Edge**.
3. In the address bar, enter **outlook.office.com** and press Enter.
4. On the **Pick an account** page, select **AlexW@yourtenant.onmicrosoft.com**.
5. On the **Enter password** page, enter the tenant password and select **Sign in**.
6. At the **More information required** page, select **Next**.
7. On the **Keep your account secure** page, select **I want to set up a different method**.
8. In the **Choose a different method** dialog box, select **Phone**, and then select **Confirm**.

9. On the **Phone** page, enter your mobile phone number which you can receive text messages, and then select **Next**.
10. After you receive the verification code as a text message, enter the code where indicated on the **Phone** page and then select **Next**.
11. At the SMS verified message, select **Next** and then select **Done**.
12. At the Stay signed in message, select **No**. Outlook on the Web opens to Alex Wilber's inbox.
13. At the top-right corner, select the **Account manager for Alex Wilber** and then select **Sign out**.
14. Close Microsoft Edge.

*Note: Users only have to register the first time they use MFA. Subsequent sign-ins only require providing the validation code which it texted to the phone number that you entered during registration.*

15. On the taskbar, select **Microsoft Edge**.
16. In the address bar, enter **outlook.office.com** and press Enter.
17. On the **Pick an account** page, select **AlexW@yourtenant.onmicrosoft.com**.
18. On the **Enter password** page, enter the tenant password and select **Sign in**. The Enter code dialog box opens. Notice that you can select a check box to specify Don't ask again for 30 days.
19. At the **Enter code** page, enter the code sent to your mobile phone, and then select **Verify**.
20. At the Stay signed in message, select **No**. Outlook on the Web opens to Alex Wilber's inbox.
21. At the top-right corner, select the **Account manager for Alex Wilber** and then select **Sign out**.
22. Close Microsoft Edge.

#### 16.2.5 Task 3: Remove per-user MFA

1. Switch to **SEA-CL1**.
2. On **SEA-CL1**, if necessary, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
3. On the taskbar select **Microsoft Edge**, in the address bar type **https://aad.portal.azure.com**, and then press **Enter**.
4. Sign in as user **Admin@yourtenant.onmicrosoft.com**, and use the tenant Admin password. If the **Stay signed in?** prompt appears, select **No**. The Azure Active Directory admin center opens.
5. In the Azure Active Directory admin center, in the navigation pane, select **Users**.
6. Select **All users** and then at the top of the results pane select **Multi-Factor Authentication**. You may need to select the ellipse first to view the Multi-Factor Authentication option.
7. At the top of the page, under **multi-factor authentication**, select **users**.
8. In the user list, select the check box next to **Alex Wilber**. Take note that the **Multi-Factor Auth Status** for Alex Wilber is now set to **Enforced** (was previously set to Enabled). This is because Alex has registered and is using MFA.
9. In the Alex Wilber page, select **Disable**.
10. On the **Disable multi-factor authentication** message, select **yes**.
11. On the **Updates successful** message, select **close**. Take note that the **Multi-Factor Auth Status** for Alex Wilber is now **Disabled**.
12. Close Microsoft Edge.

**Results**: After completing this exercise, you will have successfully configured per-user multi-factor authentication.

### 16.3 Exercise 2: Configure multi-factor authentication using conditional access

#### 16.3.1 Scenario

To provide additional security for user sign on events, you need to configure and test multi-factor authentication (MFA). You decide that using conditional access will provide greater flexibility for your MFA requirements. Alex Wilber has agreed to validate the settings for you.

#### 16.3.2 Task 1: Validate sign-in before enabling conditional access with MFA

1. Sign in to **SEA-WS1** as **Admin** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In the address bar, enter **outlook.office.com** and press Enter.
4. On the **Pick an account** page, select **AlexW@yourtenant.onmicrosoft.com**.
5. On the **Enter password** page, enter the tenant password and select **Sign in**.
6. On the **Stay signed in** page, select **No**. Outlook opens to Alex's inbox. Take note that only the password was required to sign in to Outlook on the Web.

7. At the top-right corner, select the **Account manager for Alex Wilber** and then select **Sign out**.
8. Close Microsoft Edge.

### 16.3.3 Task 2: Configure conditional access with MFA

1. Switch to **SEA-CL1**.
2. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
3. On the taskbar select **Microsoft Edge**, in the address bar type **https://aad.portal.azure.com**, and then press **Enter**.
4. Sign in as user **Admin@yourtenant.onmicrosoft.com**, and use the tenant Admin password. If the **Stay signed in?** prompt appears, select **No**. The Azure Active Directory admin center opens.
5. In the Azure Active Directory admin center, in the navigation pane, select **Azure Active Directory**.
6. On the **Contoso** navigation pane, select **Security**.
7. On the **Security** page, select **Conditional Access**.
8. On the **Conditional Access** page, select **Policies** and then select **New policy**.
9. On the **New Conditional access policy** page, in the **Name** box, enter **Contoso MFA Policy**.
10. Under **Assignments**, select **Users and groups**.
11. In the Users and groups pane, select the option next to **Select users and groups** and then select the check box next to **Users and groups**.
12. On the **Select** page, select **Alex Wilber** and then click **Select**. Note that typically you would specify a group, however for this exercise we will just test the setting on Alex Wilber.
13. Select **Cloud apps or actions** and then click **Select apps**.
14. On the **Select** page, select the check box next to **Office 365** and then click **Select**.
15. Under **Access controls**, select **Grant**.
16. On the **Grant** page, select **Grant access**, select the check box next to **Require multi-factor authentication**, and then click **Select**.
17. Under **Enable policy**, select **On**.
18. Select **Create** to create the Contoso MFA Policy. Notice that the policy is listed with a State of **On**.
19. In the Azure Active Directory admin center, select **Users**.
20. In the User list, select **Alex Wilber**.
21. On the Alex Wilber page, select **Authentication methods**. Notice that a phone number has already been configured for Alex. This was because he registered MFA during the previous lab. We will leave this setting so that Alex does not have to re-register the phone number.

### 16.3.4 Task 3: Validate conditional access MFA

1. Switch to **SEA-WS1**.
2. On the taskbar, select **Microsoft Edge**.
3. In the address bar, enter **outlook.office.com** and press Enter.
4. On the **Pick an account** page, select **AlexW@yourtenant.onmicrosoft.com**.
5. On the **Enter password** page, enter the tenant password and select **Sign in**. The Enter code dialog box opens. Notice that you can select a check box to specify Don't ask again for 30 days.
6. At the **Enter code** page, enter the code sent to your mobile phone, and then select **Verify**.
7. At the Stay signed in message, select **No**. Outlook on the Web opens to Alex Wilber's inbox.
8. At the top-right corner, select the **Account manager for Alex Wilber** and then select **Sign out**.
9. Close Microsoft Edge.

### 16.3.5 Task 4: Remove conditional access MFA

1. Switch to **SEA-CL1**.
2. On **SEA-CL1**, if necessary, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
3. On the taskbar select **Microsoft Edge**, in the address bar type **https://aad.portal.azure.com**, and then press **Enter**.
4. Sign in as user **Admin@yourtenant.onmicrosoft.com**, and use the tenant Admin password. If the **Stay signed in?** prompt appears, select **No**. The Azure Active Directory admin center opens.
5. In the Azure Active Directory admin center, in the navigation pane, select **Azure Active Directory**.
6. On the **Contoso** navigation pane, select **Security**.
7. On the **Security** page, select **Conditional Access**.

8. On the **Conditional Access** page, select **Policies** and then select **Contoso MFA Policy**.
9. On the **Contoso MFA Policy** page, select **Delete** and then select **Yes**.
10. Close Microsoft Edge.

**Results**: After completing this exercise, you will have successfully configured conditional access with multi-factor authentication.

**END OF LAB**

# 17 Practice Lab: Configuring Self-service password reset for user accounts in Azure AD

## 17.1 Summary

In this lab, you will configure and validate self-service password reset (SSPR) for user accounts in Azure Active Directory.

### 17.1.1 Scenario

The Help Desk has indicated that a large number of support tickets are related to password resets. You have been asked to propose a solution for users to reset their own password. For accounts that are synchronized from AD DS, the process should reset both their Azure AD and AD DS password.

### 17.1.2 Task 1: Configure password writeback

1. Sign in to **SEA-SVR1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the desktop, double-click **Azure AD Connect**.
3. On the **Welcome to Azure AD Connect** page, select **Configure**.
4. On the **Additional tasks** page, select **Customize synchronization options**, and then select **Next**.
5. On the **Connect to Azure AD** page, if needed type **admin@yourtenant.onmicrosoft.com** in the **USERNAME** text box, type your Admin tenant password in the **PASSWORD** text box, and then select **Next**.
6. On the **Connect to your directories** page, select **Next**.
7. On the **Domain and OU filtering** page, select **Next**.
8. On the **Optional features** page, select **Password writeback**, and then select **Next**.
9. On the **Ready to configure** page, select **Configure**.
10. On the **Configuration complete** page, select **Exit**.

### 17.1.3 Task 2: Enable self-service password reset

1. Switch to **SEA-CL1** and sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar select **Microsoft Edge**, in the address bar type **https://aad.portal.azure.com**, and then press **Enter**.
3. Sign in as user **Admin@yourtenant.onmicrosoft.com**, and use the tenant Admin password. If the **Stay signed in?** prompt appears, select **No**. The Azure Active Directory admin center opens.
4. In the Azure Active Directory admin center, in the navigation pane, select **Users**.
5. In the **Users** navigation pane, select **Password reset**.
6. In the **Password reset | Properties** window, select **All** to enable self-service password reset to all users. Select **Save**.
7. On the **Password reset | Properties** blade, select **Authentication methods**.
8. For the methods available to users, ensure that **Mobile Phone** and **Email** are selected, and then select **Security Questions**.
9. For the **Number of questions required to register**, select **3**.
10. For the **Number of questions required to reset**, select **3**.
11. In the **Select security questions** section, select **No security questions configured**, then select **Predefined**. Select three questions of your choice, and then select **OK** twice.
12. Select **Save**.

13. Select **Registration** Select **No** for **Require users to register when signing in**, and the select **Save**.
14. In the navigation pane, select **On-premises integration**.
15. Verify that your on-premises writeback client is running and select **Yes** for the **Write back passwords to your on-premises directory** option. If needed, select **Save**.
16. Close Microsoft Edge.

#### 17.1.4 Task 3: Validate self-service password reset

1. Switch to SEA-WS1.
2. If necessary, sign in as **Admin** with the password of **Pa55w.rd**.
3. On the taskbar, select **Microsoft Edge**.
4. Browse to **https://myaccount.microsoft.com**.
5. On the **Pick an account** page, select **Use another account**.
6. On the **Sign in** page, enter **Aaron@yourtenant.onmicrosoft.com**.
7. On the **Enter password** page, enter **Pa55w.rd** and then select **Sign in**. If the Microsoft Edge prompts to save the password, select **Save**.
8. On the **My Account** page, in the navigation pane, select **Password**.
9. On the change password page, enter the following information and then select submit: - Old password: **Pa55w.rd** - Create new password: **Pa55w.rd1234** - Confirm new password: **Pa55w.rd1234**
10. On the Microsoft Save password prompt, select **Save**.
11. Close Microsoft Edge and sign out of SEA-WS1.

#### 17.1.5 Task 4: Optional - Run AD Sync

Note that this step is normally not necessary for password writeback, but is recommended to address issues inherent in lab environments and ensure AD is synchronized.

1. Switch to **SEA-SVR1**.
2. Right-click **Start** and then select **Windows PowerShell (Admin)**.
3. At the **Windows PowerShell** command prompt, type the following command, and then press **Enter**:

```
Start-ADSyncSyncCycle -PolicyType Delta
```

4. Close Windows PowerShell, and then wait for approximately 3-4 minutes.

#### 17.1.6 Task 4: Verify password writeback

1. Switch to **SEA-CL2** and sign out if necessary.
2. On **SEA-CL2**, select **Other user**, and then attempt to sign in as **Contoso\Aaron** with the password of **Pa55w.rd**.
3. Attempt to sign in as **Contoso\Aaron** with the password **Pa55w.rd**.
4. Ensure that you get the message that the user name or password is incorrect.
5. Sign in to **SEA-CL2** as **Contoso\Aaron** with the password **Pa55w.rd1234**. You should be able to sign in. This confirms that the password you changed in the Azure portal is written back to the local Active Directory Domain Services (AD DS) account.
6. Sign out of **SEA-CL2**.

**Results**: After completing this exercise, you will have successfully configured and validated self-service password reset.

**END OF LAB**

# 18 Practice Lab: Configuring and validating device compliance

## 18.1 Summary

In this lab, you validate device compliance by configuring a compliance policy and associated conditional access rule used to determine the status of a managed device.

## 18.2 Exercise 1: Configuring compliance policies

### 18.2.1 Scenario

Contoso would like to ensure that Windows devices that are enrolled in Intune meet a minimum configuration specification. The following are specifications are required:

- Minimum Windows 10 operating system version: 10.0.19041.329
- Microsoft Defender Antimalware required

If a device meets these requirements, it will be marked as compliant. If the device does not meet these requirements, the device should be marked as non-compliant.

### 18.2.2 Task 1: Create and assign a compliance policy

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. Sign in as as **admin@yourtenant.onmicrosoft.com** with the default tenant password.
5. From the navigation pane select **Devices**, then select **Compliance policies**.
6. On the **Compliance policies | Policies** blade, in the details pane select **Create Policy**.
7. On the **Create a policy** blade, provide the following value and select **Create**:
   - Platform: **Windows 10 and later**
8. On the **Basics** tab, provide the following value and select **Next**:
   - Name: **Compliance1**
9. On the **Compliance settings** tab, expand **Device Health** and review the available settings.
10. On the **Compliance settings** tab, expand **Device Properties**. In the **Minimum OS version** field, type **10.0.19041.329**.
11. On the **Compliance settings** tab, expand **System Security**. Set the **Microsoft Defender Antimalware** setting to **Require**.
12. Select **Next**. On the **Actions for noncompliance** tab, note the action to Mark device noncompliant default setting is immediately. Review how you can configure the number of days after which the device is marked as noncompliant, and configuration additional actions.
13. Select **Next**. On the **Assignments** tab, under **Included groups** select **Add groups**. Select **Windows Devices**, choose **Select**, and then select **Next**.

    *Note: The **Windows Devices** group was created in the Module 3 lab.*
14. Select **Create**.
15. In the navigation menu, select **Devices** and then in the Devices navigation pane, select **Compliance policies**.
16. On the **Compliance policies** page, select **Compliance policy settings**.
17. On the **Compliance policy settings** page, next to **Mark devices with no compliance policy assigned as**, select **Not Compliant** and then select **Save**. This setting will ensure that any device that does not have a compliance policy assigned will be set to Not compliant.

**Results**: After completing this exercise, you will have successfully configured a compliance policy.

## 18.3 Exercise 2: Creating a conditional access policy

### 18.3.1 Scenario

When a user uses a device that is marked as non-compliant, they should not be able to access their e-mail. You've been asked to configure a conditional access policy that enforces this rule, and verify it functions as expected.

### 18.3.2 Task 1: Create a conditional access policy

1. On **SEA-CL1**, in the **Microsoft Endpoint Manager admin center** select **Devices**, then select **Conditional access**.
2. In the **Details** pane, select **New policy**.
3. On the **New** blade, in the **Name** text box, type **Conditional1** and then select **Users and groups**.

4. On the **Users and groups** blade, select the **All users** radio button.
5. On the **New** blade, select **Cloud apps or actions**, select the **Select apps** radio button, select **Office 365 Exchange Online**, and then click **Select**.
6. On the **New** blade, select **Conditions**, select **Device platforms**, in the **Configure** section select **Yes**, select the **Select device platforms** radio button, select the **Windows** check box, and then select **Done**.
7. On the **New** blade under **Access controls**, select **Grant**, select the **Require device to be marked as compliant** check box, and then select **Select**.
8. On the **New** blade, select **On** for the **Enable policy** option and then select **Create**.
9. From the top right corner select the Account manager and then select **Sign out**.
10. Close Microsoft Edge.

#### 18.3.3 Task 2: Verify that the conditional access policy is working

1. On **SEA-CL1**, on the taskbar, select **Microsoft Edge**.
2. In Microsoft Edge, type **Outlook.office.com** and then press Enter.
3. On the pick an account dialog box, select use another account.
4. On the Sign in page, enter **Aaron@yourtenant.onmicrosoft.com**.
5. On the **Enter password** page, enter **Pa55w.rd1234** and select **Sign in**. If the Microsoft Edge Save password prompt appears, select **Never**.
6. Verify that you receive the message **"You can't get there from here"**.
7. Select **More details**. You should see more information about why you are blocked.

   *Note: This is because SEA-CL1 is not joined to Azure AD and not managed by Intune, so not marked as compliant.*
8. **Close** the browser window.
9. Switch to **SEA-WS3**, and sign in as as **Aaron@yourtenant.onmicrosoft.com** with the password **Pa55w.rd1234** (or enter PIN **102938**). Note: SEA-WS3 is a managed Windows 10 device that is enrolled in Intune.
10. On the taskbar, select **Microsoft Edge**.
11. In Microsoft Edge, type **Outlook.office.com** and then press Enter. Close the Welcome page.
12. Verify that you can access Aaron's mailbox.

    *Note: This is because SEA-WS3 is a managed device and marked as compliant.*
13. Close Microsoft Edge and sign out of SEA-WS3.

#### 18.3.4 Task 3: Disable the conditional access policy

1. Switch to **SEA-CL1**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. Sign in as as **admin@yourtenant.onmicrosoft.com** with the default tenant password.
5. From the navigation pane select **Devices**, then select **Conditional access**.
6. On the **Conditional Access** page, select **Conditional1**.
7. On the **Conditional1** page, at the bottom of the page, select **Off** and then select **Save**.
8. Close Microsoft Edge.

**Results**: After completing this exercise, you will have successfully configured a conditional access policy to determine device compliance.

**END OF LAB**

# 19 Practice Lab: Creating device inventory reports

## 19.1 Summary

In this lab, you will view device inventory within Intune, Excel, and using Power BI.

## 19.2 Exercise 1: Reviewing device inventory with Intune

### 19.2.1 Scenario

You've been asked to review the inventory for SEA-WS3. Use Intune to review the devices hardware and app inventory.

### 19.2.2 Task 1: Examining device inventory

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. Sign in as **admin@yourtenant.onmicrosoft.com** with the tenant Admin password.
5. In the Microsoft Endpoint Manager admin center, select **Devices** from the navigation bar.
6. In the Devices navigation pane, select **All devices** and in the details pane, select the **SEA-WS3** entry. Examine the various information displayed about the device.
7. Select **Properties** and note that you can change the **Management name**, **Device category** and **Device ownership**.
8. In the **Management name** field, replace the existing text with **SEA-WS3** and select **Save**.
9. Under **Monitor**, select **Hardware** and examine the hardware from **SEA-WS3**. You need to scroll down to see it all.
10. Under **Monitor**, select **Discovered apps** and examine the app inventory from **SEA-WS3**. You may need to scroll down to see it all.

**Results**: After completing this exercise, you will have successfully reviewed device hardware and app inventory.

## 19.3 Exercise 2: Exporting Intune data to Excel

### 19.3.1 Scenario

Management is requesting a report of all devices. They do not have access to the Intune dashboards, and have requested the information be sent in an Excel file.

### 19.3.2 Task 1: Export Intune Data

1. On **SEA-CL1**, in the Microsoft Endpoint Manager admin center, select **Devices** and then select **All devices**.
2. On the **Devices | All devices** blade, in the details pane, select **Export**.
3. At the Export all managed devices message, select **Yes**, and wait for the export to be prepared and a message that indicates that the export is complete.
4. At the bottom of the Microsoft Edge window, next to the zip file, select the ellipse and then select **Show in folder**.
5. In the Downloads folder, right-click the downloaded zip file and select **Extract all**. Browse to the **Downloads** folder and select **Extract**.

### 19.3.3 Task 2: Import Intune data into Microsoft Excel

1. On **SEA-CL1**, select **Start** and then select **Excel**.
2. In Excel, select **Open Other Workbooks**, then **Browse**, select the **Downloads** folder and in the **All Excel Files** drop-down box, select **All Files**.
3. In the **Open** dialog box, select the file you just extracted. Then select **Open**.
4. In the **Text Import Wizard – Step 1 of 3** dialog box, select **Delimited** and then select **Next**.
5. In the **Text Import Wizard – Step 2 of 3** dialog box, remove the check mark next to **Tab** and select the check box next to **Comma**. Then select **Next**.
6. In the **Text Import Wizard – Step 3 of 3** dialog box, select **Finish**.
7. Review the report content. When finished, close Excel and select **Don't Save** when asked about saving the report.
8. Close all open Windows.

**Results**: After completing this exercise, you will have successfully exported Intune data to Excel for review.

## 19.4 Exercise 3: Reviewing Intune Data using Power BI

### 19.4.1 Scenario

Your organization uses Power BI for reporting. You need to set up Power BI on SEA-CL1 and connect to the Intune Data Warehouse. You need to see a report that shows the primary user of each device.

*Note: Power BI Desktop was deployed and installed using Configuration Manager in Module 4.*

### 19.4.2 Task 1: Connect Power BI to the Intune Data Warehouse

1. On SEA-CL1, on the desktop, double-click **Power BI Desktop**.
2. After Power BI loads, with the **Home** tab selected in the ribbon, select **Get Data**.
3. In the **Get Data** dialog box, select **Other** on the left side, and then select **OData Feed** and then select **Connect**.
4. On the taskbar, select **Microsoft Edge**.
5. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
6. Sign in as **admin@yourtenant.onmicrosoft.com** with the tenant Admin password.
7. In the Microsoft Endpoint Manager admin center, select **Reports** and then select **Data warehouse**.
8. In the **OData feed for reporting service** field, copy the Odata URL into the clipboard.
9. Switch back to **Power BI Desktop** and in the OData feed dialog box, paste the **OData URL** into the **URL** box and select **OK**.
10. In the **OData feed** dialog box, select the **Organizational account** tab and then select **Sign in**.
11. On the **Sign in** page, select **admin@yourtenant.onmicrosoft.com**.
12. On the **Enter password** page, enter the tenant Admin password, and select **Sign in**.
13. Back on the **OData feed** dialog box, select **Connect**. Wait for the connection and load of data. The **Navigator** window opens.
14. In the **Navigator** window, select all tables. You can select the first table, and then shift-select the last table to select all tables. With all tables selected, select **Load**. It will take a few minutes for the process to complete.

### 19.4.3 Task 2: Create a custom report using Power BI and Intune Data Warehouse

1. In the **Visualizations** pane, select the **Treemap** option (the icon appears to have several rectangles of various sizes). The Treemap chart will be added to the report canvas.
2. In the menu bar, select **View**, and then in the ribbon select **Page view** and then select **Actual size**.
3. In the **Fields** pane, find the **devices** table and expand it.
4. Select the **deviceName** data field and drag it onto the Treemap chart in the report canvas.
5. Drag the **deviceKey** data field from the devices table to the **Visualizations** pane and drop it on under the **Values** section in the box labeled **Add data fields here**.
6. In the Fields pane, scroll down and find the **users** table and expand it.
7. Drag the **displayName** data field from the users table to the **Visualizations** pane and drop it on under the **Details** section.

   *Note: You should now see device names in each report object, with a user name listed under each device.*
8. Select the **Treemap** you added to the report canvas. In the **Visualizations** pane, select the **Table** report option (the icon appears as a spreadsheet) to switch the report canvas to a table view.
9. Select **File**, select **Export**, then select **Export to PDF**. The browser should launch and display the report in a PDF format.
10. Close all open windows.

**Results**: After completing this exercise, you will have successfully connected Power BI desktop to the Intune Data Warehouse and created a report using Power BI.

**END OF LAB**

# 20 Practice Lab: Configure and Deploy Windows Information Protection Policies by using Intune

## 20.1 Summary

In this lab, you will configure and apply a Windows Information Protection policy to provide application protection for non-managed Windows 10 devices.

### 20.1.1 Task 1: Configure the MAM service

1. On **SEA-CL1**, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. On the taskbar select **Microsoft Edge**, in the address bar type **https://endpoint.microsoft.com**, and then press **Enter**.
3. Sign in as user **Admin@yourtenant.onmicrosoft.com**, and use the tenant Admin password. If the **Stay signed in?** prompt appears, select **No**.
4. In the navigation pane, select **Devices**.
5. In the **Devices** navigation pane, select **Enroll devices**.
6. On the **Enroll devices** page, select **Automatic Enrollment**.
7. On the **Configure** page, next to **MAM user scope**, select **All**, and then select **Save**.

### 20.1.2 Task 2: Configure an App protection policy for Windows Information Protection

1. In the Microsoft Endpoint Manager admin center, in the navigation pane, select **Apps**.
2. Select **App protection policies**, select **Create policy** and select **Windows 10**.
3. In the **Name** text box, type **Windows 10 WIP policy**.
4. In the **Enrollment state** list, select **Without enrollment** and select **Next**.
5. On the **Targeted apps** tab, under **Protected apps**, select **Add**.
6. Select **Notepad** and **MsEdge - WIPMode-Allow-Enterprise AppLocker Policy File.xml**. Select **OK** and select **Next**.
7. On the **Required settings** tab, next to the **Windows Information Protection mode** option, select **Block** and then select **Next**. Note: Do not change the Corporate identity setting.
8. On the **Advanced settings** tab, in the **Network perimeter** section, select **Add**.
9. On the **Add network boundary** pane, configure the following, replacing ***<yourtenant>*** with the tenant name provided to you, and then select **OK**:
   - Boundary type: **Cloud resources**
   - Name: **SharePoint online**
   - Value: ***<yourtenant>*.sharepoint.com**
10. On the **Advanced settings** tab, next to **Show the enterprise data protection icon**, select **On** and then select **Next**.
11. On the **Assignments** tab, select **Next** and then select **Create**.

### 20.1.3 Task 3: Deploy the policy

1. On the **Apps|App protection policies** page, in the details pane, select **Windows 10 WIP policy**.
2. On the **Windows 10 WIP policy** page, select **Properties**.
3. Scroll down and click **Edit** next to **Assignments**.
4. Under **Included groups** select **Add groups**, select **Contoso_Marketing**, and then click **Select**.
5. Select **Review + save** and then select **Save**.
6. Close Microsoft Edge.

### 20.1.4 Task 4: Create a test file

1. Sign in to **SEA-WS1** as **Admin** with the password of **Pa55w.rd**. Note that SEA-WS1 is not managed by Intune.
2. Right-click on the desktop and select **New**, and then select **Text Document**.
3. Rename the file to **Sample Document.txt**.
4. Open **Sample Document.txt**.
5. In the Notepad window, enter **This is a sample corporate file**.
6. Save and close the file.
7. On the taskbar select Microsoft Edge and then navigate to **https://yourtenant.sharepoint.com**.
8. Sign in as **ereeve@yourtenant.onmicrosoft.com** with the password of **Pa55w.rd**.
9. If **Update your password** displays enter the following and then select **Sign in**:

- Current password: **Pa55w.rd**
- New password: **Pa55w.rd1234**
- Confirm password: **Pa55w.rd1234**

10. If the Microsoft Edge Update password prompt displays, select **No thanks**.
11. On the top, click **Documents**.
12. From the desktop, drag and drop the **Sample Document.txt** file into the Documents library to upload the file.
13. Once uploaded, delete the **Sample Document.txt** file from the Desktop.
14. Close all open windows.

#### 20.1.5 Task 5: Add a corporate account to Windows 10

1. On SEA-WS1, on the **Start** menu, select **Settings**.
2. Select **Accounts** and then select **Access work or school**.
3. Under **Access work or school**, select **Connect**.
4. In the **Set up a work or school account** pane, enter **ereeve@yourtenant.onmicrosoft.com** and then select **Next**.
5. Enter the password **Pa55w.rd1234**, and then select **Sign in**.
6. On the **More information required** page, select **Next**.
7. On the **Keep your account secure** page, enter your mobile phone number that is able to receive text messages and then select **Next**.
8. When you receive a text message, enter the provided code in the **Enter code** field and then select **Next**.
9. On the SMS verified message page, select **Next** and then select **Done**.
10. On the **Use Windows Hello with your account** page, select **OK**.
11. In the Windows Security prompt, in the **New PIN** and **Confirm PIN** fields, enter **102938**, and then select **OK**.
12. On the **Almost done** page, select **Next**.
13. On the **Windows Security** page, enter **Pa55w.rd** and then select **OK**.
14. On the Access work or school page, select **Work or school account** and then select **Info**. Scroll down and notice that the Connection info specifies that a wip.mam management server is being used.
15. Select the **Sync** button and then close the **Settings** window.

#### 20.1.6 Task 6: Verify the WIP policy

1. On the taskbar, select **Microsoft Edge**.
2. In **Microsoft Edge**, navigate to **https://yourtenant.sharepoint.com**.
3. If necessary, sign in as **ereeve@yourtenant.onmicrosoft.com** with the password of **Pa55w.rd1234**.
4. Take note of the briefcase icon at the right side of the address bar. Select the icon and verify that this website is managed by the tenant.
5. On the top, select **Documents**.
6. Select **Sample Document.txt** and select **Download**.
7. At the bottom of the Edge browser, select **Save as**.
8. In the **Save As** dialog box, select the **Documents** folder.
9. Next to the File name, notice the drop down arrow that shows a briefcase. Select the **Work** briefcase icon and then select **Save**.
10. On the taskbar, open **File Explorer** and browse to the **Documents** folder.

*Note: The briefcase icon in the file icon and the File ownership column indicates that the file is protected.*

11. Open the **Sample Document.txt** file using **Notepad**. The file should open because Notepad is a managed app indicated in the policy.
12. Close **Notepad**.
13. Attempt to open the **Sample Document.txt** file using **WordPad**. The file will not open and a dialog box will display to indicate that access to the file is denied. WordPad is not a managed app and is not be able to open protected files.
14. Open the **Sample Document.txt** file using Notepad.
15. Open **WordPad** and attempt to copy and paste text from Notepad into WordPad. Notice that you are prevented from pasting content into WordPad.
16. Close all open windows and sign out of SEA-WS1.

**Results**: After completing this exercise, you will have successfully configured a Windows Information Protection policy to provide data protection.

**END OF LAB**

# 21 Practice Lab: Configuring Endpoint security using Intune

## 21.1 Summary

In this lab, you will create a policy to configure Microsoft Defender for managed devices in Intune.

### 21.1.1 Scenario

You've been asked to ensure that the Contoso Developers Group have Microsoft Defender correctly configured. It's been requested that:

- Tamper protection be prevented
- Hide the Account protection, App and browser control, Device security, Device performance and health, and Family options areas in the Windows Security app
- Contact name and phone number must be added.
- Real-time protection, Remediation, and scan settings are also to be configured.

Settings will be verified by testing on an enrolled device, SEA-WS2 and a non-enrolled device, SEA-CL1.

### 21.1.2 Task 1: Configure Windows Security Experience in Intune

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. Sign in as as **admin@yourtenant.onmicrosoft.com** with the default tenant password.
5. From the navigation pane select **Endpoint security**, then select **Antivirus**.
6. On the **Endpoint security |Antivirus** pane, select **Create Policy**.
7. In the **Create a profile** pane, select **Windows 10 and later** for Platform. In the Profile list, select **Windows Security experience**. Then select **Create**.
8. On the Basics tab, in the **Name** field, enter **Windows Security Settings**. Select **Next**.
9. On the **Configuration settings** tab, expand the **Windows Security** section.
10. Under Windows security, configure the following settings:
    - Enable tamper protection to prevent Microsoft Defender from being disabled: Enable
    - Hide the Account protection area in the Windows Security app: Yes
    - Hide App and browser control are in the Windows Security app: Yes
    - Hide the Device security area in the Windows Security app: Yes
    - Hide the Device performance and health area in the Windows Security app: Yes
    - Hide the Family options area in the Windows Security app: Yes
11. Next to **Organization's support contact information** select **Display in app and in notifications**.
12. In the **Contact name** field, enter **Contoso IT**.
13. For **Phone number**, enter **555-1234** and then select **Next**.
14. On the **Scope tags** page, select **Next**.
15. On the **Assignments** tab, under **Included groups** select **Add groups**. Choose the **Contoso Developers Devices** group and then choose **Select**.
16. Select **Next** and then on the **Review + Create** tab, review the information and select **Create**.

### 21.1.3 Task 2: Configure Microsoft Defender Antivirus policy in Intune

1. On the **Endpoint security |Antivirus** pane, select **Create Policy**.
2. In the **Create a profile** pane, select **Windows 10 and later** for Platform. In the Profile list, select **Microsoft Defender Antivirus**. Then select **Create**.
3. On the Basics tab, in the **Name** field, enter **Microsoft Defender Antivirus Settings**. Select **Next**.
4. On the **Configuration settings** tab, expand the **Real-time protection** section.
5. Under **Real-time protection**, configure the following settings:
    - Turn on real-time protection: Yes
    - Monitor for incoming and outgoing files: Only monitor incoming files
    - Scan all downloaded files and attachments: Yes
6. On the **Configuration settings** tab, expand the **Remediation** section.
7. Under **Remediation**, configure the following settings:
    - Number of days to keep quarantined malware: 60

- Submit samples consent: Always prompt

8. On the **Configuration settings** tab, expand the **Scan** section.
9. Under **Scan**, configure the following settings:
   - Run daily quick scan at: 12 PM
   - Check for signature updates before running scan: Yes
10. On the **Configuration settings** tab, select **Next**.
11. On the **Scope tags** page, select **Next**.
12. On the **Assignments** tab, under **Included groups** select **Add groups**. Choose the **Contoso Developers Devices** group and then choose **Select**.
13. Select **Next** and then on the **Review + Create** tab, review the information and select **Create**.

#### 21.1.4 Task 3: Sync the managed devices

1. In the Microsoft Endpoint Manager admin center, select **Devices** and then select **All devices**.
2. On the **Devices | All devices** pane, select **SEA-WS2** and then on the **SEA-WS2** blade, select **Sync** on the toolbar, and then select **Yes**. Wait for 3-4 minutes for the sync to complete.
3. Close Microsoft Edge.

#### 21.1.5 Task 4: Verify the configuration

1. On **SEA-CL1**, in the notification area, right-click the **Windows Security** icon and select **View security dashboard** to open Windows Security. Notice that all security options are displayed. This is because SEA-CL1 is not enrolled to Intune.
2. Close **Windows Security**.
3. Switch to **SEA-WS2**, and sign in as **Diego Siciliani** with the PIN **102938**.
4. In the notification area, right-click the **Windows Security** icon and select **View security dashboard** to open Windows Security. Notice that all of the restricted areas as configured in the Intune policy are not displayed. SEA-WS2 is enrolled in Intune and has been applied the security settings.
5. Close **Windows Security** and sign out of **SEA-WS2**.

**Results**: After completing this exercise, you will have successfully created and applied a policy to configure Microsoft Defender for managed devices in Intune.

**END OF LAB**

# 22 Practice Lab: Configuring Disk Encryption Using Intune

## 22.1 Summary

In this lab, you will configure BitLocker disk encryption using Intune.

#### 22.1.1 Scenario

It's been determined that all the information on SEA-WS2 should be encrypted. You've been asked to configure full disk encryption on SEA-WS2 and require additional authentication at startup.

#### 22.1.2 Task 1: Configure device configuration policy in Intune

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. Sign in as as **admin@yourtenant.onmicrosoft.com** with the default tenant password.
5. In the Microsoft Endpoint Manager admin center, select **Devices** from the navigation bar.
6. On the **Devices | Overview** page, select **Configuration Profiles**.
7. On the **Devices | Configuration profiles** blade, in the details pane, select **Create profile**.
8. In the **Create a profile** page, select the following options, and then select **Create**:
   - Platform: **Windows 10 and later**
   - Profile type: **Templates**

- Profile: **Endpoint protection**

9. On the **Basics** page, enter the following information, and then select **Next**:
   - Name: **Contoso BitLocker**
   - Description: **Enable BitLocker for all devices**
10. On the **Configurations settings** page, expand **Windows Encryption** and then configure the following options:
    - Encrypt devices: **Require**
    - Additional authentication at startup: **Require**
11. On the **Configurations settings** page, select **Next**.
12. On the **Assignments** tab, under **Included groups** select **Add groups**. Select **Contoso Developer devices**, choose **Select**, and then select **Next** twice.
13. On the **Review + create** page, select **Create**.
14. Close all open windows on **SEA-CL1**.

#### 22.1.3 Task 2: Verify and enable BitLocker settings

1. On **SEA-WS2**, sign in as **Diego Siciliani** with the PIN **102938**.
2. On the taskbar, select **Start** and then select the **Settings** app.
3. In the **Settings** app, select the **Accounts** tile and then select **Access work or school**.
4. In the **Access work or school** section, select the **Connected to Contoso's Azure AD** link and then select **Info**. Select **Sync**.
5. Select the **Encryption needed** notification.

   *Note: It may take some time until the notification shows up.*
6. On the **Are you ready to start encryption?** dialog select the first checkbox and select **Yes**.
7. On the **Choose how to unlock your drive at startup?** page, select **Enter a password**
8. Enter **Pa55w.rd** in the **Enter your password** and **Reenter your password** boxes, and then select **Next**.
9. On the **How do you want to back up your recovery key?** page, select **Save to your Azure AD account**. Then select **Next**.
10. On the **Choose how much of your drive to encrypt** page, select **Encrypt used disk space only** and select **Next**.
11. On the **Choose which encryption mode to use** page, ensure that **New encryption mode (best for fixed drives on this device)** is selected, and then select **Next**.
12. On the **Are you ready to encrypt this drive** page, select **Continue**. Wait for the encryption to complete.
13. At the **Encryption of C: is complete** message, select **Close**, and then restart **SEA-WS2**.
14. When **SEA-WS2** restarts, type **Pa55w.rd** and press **Enter** to unlock the drive.

#### 22.1.4 Task 3: Verify BitLocker protection

1. Sign in to **SEA-WS2** as **Diego Siciliani** with the PIN **102938**.
2. On the taskbar, select **File Explorer** and then select **This PC**.
3. In the navigation pane, right-click **Local Disk (C:)** and then select **Manage BitLocker**.
4. In the **BitLocker Drive Encryption** window, ensure that you see **C: BitLocker on** status. This means that drive is encrypted.
5. Close all open windows and sign out of **SEA-WS2**.

**Results**: After completing this exercise, you will have successfully configured BitLocker using Intune.

**END OF LAB**

# 23 Practice Lab: Deploying Windows 10 using Microsoft Deployment Toolkit

## 23.1 Summary

In this lab, you will use the Microsoft Deployment Toolkit to create and deploy a Windows 10 workstation image.

### 23.1.1 Scenario

You need to deploy a new Windows 10 workstation named SEA-WS4. You decide to use Microsoft Deployment Toolkit to deploy the operating system to new computer hardware. You will configure a new Deployment Share in MDT and then configure the task sequence that will perform the steps to deploy SEA-WS4.

### 23.1.2 Task 1: Create a new Deployment Share

1. On **SEA-SVR2**, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **File Explorer** and then browse to **E:\Labfiles\ISOs**.
3. Right-click **Win10_20H2_Eval.iso** and then select **Mount**. The ISO mounts as DVD Drive F.
4. Close **File Explorer**.
5. Select **Start**, expand **Microsoft Deployment Toolkit**, and then select **Deployment Workbench**.
6. In the **Deployment Workbench**, right-click **Deployment Shares** and then select **New Deployment Share**. The **New Deployment Share Wizard** opens.
7. On the **Path** page, under **Deployment share path**, change the value to **E:\DeploymentShare** and then select **Next**.
8. On the **Share** page, take note of the **Share name**, but do not change it. Select **Next**.
9. On the **Descriptive Name** page, accept the default value and select **Next**.
10. On the **Options** page, configure the following, and then select **Next**:

- Ask to set the local Administrator password: Enabled
- All other check boxes: Disabled

11. On the **Summary** page, review the information and then select **Next**.
12. On the **Confirmation** page, ensure that the process completed successfully and then select **Finish**.
13. Under **Deployment Shares**, expand the **MDT Deployment Share** folder. Take note of the various nodes that can be configured for the deployment share.

### 23.1.3 Task 2: Add Operating System files to the Deployment Share

1. In the Deployment Workbench, expand **Deployment Shares**, expand **MDT Deployment Share**, and then select **Operating Systems**.
2. Right-click **Operating Systems** and then select **Import Operating System**. The Import Operating System Wizard opens.
3. In the **Import Operating System Wizard**, on the **OS Type** page, select **Full set of source files** and then select **Next**.
4. On the **Source** page, under **Source Directory**, enter **F:** and then select **Next**.
5. On the **Destination** page, accept the default destination directory name and then select **Next**.
6. On the **Summary** page, review the information and then select **Next**. The operating system source files are copied into the deployment share.
7. On the **Confirmation** page, ensure that the process completed successfully and then select **Finish**.
8. In the **Deployment Workbench**, with **Operating Systems** selected verify that the Windows 10 Enterprise Evaluation operating system displays.

### 23.1.4 Task 3: Add Applications to the Deployment Share

1. In the Deployment Workbench, expand **Deployment Shares**, expand **MDT Deployment Share**, and then select **Applications**.
2. Right-click **Applications** and then select **New Application**. The New Application Wizard opens.
3. In the **New Application Wizard**, on the **Application Type** page, select **Application with source files** and then select **Next**.
4. On the **Details** page, configure the following, and then select **Next**:
    - Publisher: **Microsoft**
    - Application Name: **XML Notepad**

5. On the **Source** page, under **Source directory**, enter **E:\Labfiles\Apps** and then select **Next**.
6. On the **Destination** page, accept the default destination directory name and then select **Next**.
7. On the **Command Details** page, under **Command line** enter **XmlNotepad.msi /q** and then select **Next**.
8. On the **Summary** page, review the information and then select **Next**.
9. On the **Confirmation** page, ensure that the process completed successfully and then select **Finish**.

#### 23.1.5 Task 4: Create an MDT Task Sequence

1. In the Deployment Workbench, expand **Deployment Shares**, expand **MDT Deployment Share**, and then select **Task Sequences**.
2. Right-click **Task Sequences** and then select **New Task Sequence**. The **New Task Sequence Wizard** opens.
3. On the **General Settings** page, configure the following and then select **Next**:
   - Task sequence ID: **001**
   - Task sequence name: **Deploy Windows 10 Enterprise**
4. On the **Select Template** page, select **Standard Client Task Sequence**, and then select **Next**.
5. On the **Select OS** page, select **Windows 10 Enterprise Evaluation** and then select **Next**.
6. On the **Specify Product Key** page, select **Do not specify a product key at this time**, and then select **Next**.
7. On the **OS Settings** page, configure the following and then select **Next**:
   - Full Name: **User**
   - Organization: **Contoso Corporation**
   - Internet Explorer Home Page: **about:blank**
8. On the **Admin Password** page, select **Use the specified local Administrator password**, and then enter **Pa55w.rd** in both text boxes. Select **Next**.
9. On the **Summary** page, review the information and then select **Next**.
10. On the **Confirmation** page, ensure that the process completed successfully and then select **Finish**.
11. In the **Deployment Workbench**, with **Task Sequences** selected verify that the **Deploy Windows 10 Enterprise** task sequence displays.
12. Right-click the **Deploy Windows 10 Enterprise** task sequence, and then select Properties.
13. Select the **Task Sequence** tab.
14. Expand the **Validation** node and then select **Validate**.
15. On the **Properties** page, remove the check marks next to **Ensure minimum memory** and **Ensure minimum processor speed**. Do not make any other changes.
16. On the **Deploy Windows 10 Enterprise Properties** window, select **OK**.

#### 23.1.6 Task 5: Configure Deployment Share Properties and Windows PE settings

1. In the Deployment Workbench, expand **Deployment Shares**, and select **MDT Deployment Share**.
2. Right-click **MDT Deployment Share** and then select **Properties**.
3. In the **MDT Deployment Share Properties** window, on the General tab, take note of the information that was provided when the deployment share was created.
4. Select the **Rules** tab. The Rules tab displays the content of the CustomSettings.ini file. These values were also provided during the creation of the deployment share.
5. Select the **Windows PE** tab. The Windows PE tab provides options for creating a Windows PE boot disk.
6. On the **Windows PE** tab, next to **Platform**, select **x64**.
7. In the **Windows PE Customizations** section, next to **Scratch space size**, select **64**.
8. Select the **Features** tab and then select the check box next to the following Feature Packs:
   - DISM Cmdlets
   - Windows PowerShell
   - Microsoft Data Access Components (MDAC/ADO) support
9. In the **MDT Deployment Share Properties** window, select **OK**.
10. Right-click **MDT Deployment Share** and then select **Update Deployment Share**. The Update Deployment Share Wizard opens.
11. On the **Options** page, select **Optimize the boot image updating process** and then select **Next**.
12. On the **Summary** page, select **Next**. The Deployment Share starts to update and create the Windows PE files. This will take a few minutes to complete.
13. On the **Confirmation** page, ensure that the process completed successfully and then select **Finish**.

### 23.1.7 Task 6: Deploy Windows 10 Using MDT

1. On SEA-SVR2, on the taskbar, select Hyper-V Manager.
2. In Hyper-V Manager, select **Virtual Switch Manager**.
3. Select **New virtual network switch** and then in the details pane, select **External**. Select **Create Virtual Switch**.
4. In the **Virtual Switch Properties** page, under **Name**, enter **External network**, and then select **OK**.
5. In Hyper-V Manager, select **SEA-SVR2** and then in the Actions pane, select **New** and then select **Virtual Machine**.
6. On the **Before you Begin** page, select **Next**.
7. On the **Specify Name and Location** page, in the **Name** box type **SEA-WS4**.
8. Select the check box next to **Store the virtual machine in a different location** and then next to **Location** type **E:\Labfiles\VirtualMachines**. Select **Next**.
9. On the **Specify Generation** page, ensure that **Generation 1** is selected and then select **Next**.
10. On the **Assign Memory** page, next to **Startup memory** type **8192** and then select **Next**.
11. On the **Configure Networking** page, next to **Connection**, select **External Network** and then select **Next**.
12. On the **Connect Virtual Hard Disk** page, select **Create a virtual hard disk** and enter the following and then click **Next**:
    - Name: **SEA-WS4.vhdx**
    - Location: **E:\Labfiles\VirtualMachines**
    - Size: **60 GB**
13. On the **Installation Options** page, select **Install an operating system from a bootable CD/DVD-ROM** and configure the following:
    - Image file (.iso): **E:\DeploymentShare\Boot\LiteTouchPE_x64.iso**
14. Select **Next** and then **Finish**.
15. In Hyper-V Manager, select **SEA-WS4**, select **Connect**, and then select **Start**. The computer starts and invokes the MDT Deployment Wizard. Maximize the window as needed.
16. On the **Welcome** page, select **Run the Deployment Wizard to install a new Operating System**.
17. On the **Specify credentials for connecting to network shares** window, enter the following and then select **OK**:
    - User Name: **Administrator**
    - Password: **Pa55w.rd**
    - Domain: **Contoso**
18. On the **Task Sequence** page, select **Deploy Windows 10 Enterprise** and then select **Next**.
19. On the **Computer Details** page, next to **Computer name** enter **SEA-WS4** and then select **Next**.
20. On the **Move data and settings from previous version of Windows** page, select **Next**.
21. On the **Specify whether to restore user data** page, select **Next**.
22. On the **Specify Locale and time preferences** page, select **Next**.
23. On the **Select one or more applications to install** page, select **Next**.
24. On the **Specify the Administrator account password**, enter **Pa55w.rd** in both text boxes and then select **Next**.
25. On the **Ready to begin** page, select **Begin**. The installation begins. It will take some time to complete and will reboot SEA-WS4 during the installation as needed.
26. After the installation is complete, the desktop will open and finalize the deployment. At the deployment summary, select **Finish**.
27. Shut down **SEA-WS4**.

28. Right-click **SEA-WS4** and then select **Settings**.
29. In the **Settings for SEA-WS4**, expand **IDE Controller 1** and then select **DVD Drive**.
30. In the details pane, under **Media**, select **None**, and then select **OK**.
31. On SEA-SVR2, close **Hyper-V Manager** and close the **Deployment Workbench**.
32. Open **File Explorer**, right-click **DVD Drive F** and then select **Eject**.
33. Close **File Explorer** and Sign out of **SEA-SVR2**.

**Results**: After completing this exercise, you will have successfully used the Microsoft Deployment Toolkit to create and deploy a Windows 10 workstation.

**END OF LAB**

# 24 Practice Lab: Deploying Windows 10 using Endpoint Configuration Manager

## 24.1 Summary

In this lab, you will use Microsoft Endpoint Configuration Manager to deploy a Windows 10 Enterprise image.

### 24.1.1 Scenario

Contoso uses Microsoft Endpoint Configuration Manager to manage on-premises workstations. You need to refresh a Windows 8.1 computer named SEA-W81 to contain the Windows 10 Enterprise operating system. You will configure the operating system deployment features of Configuration manager and deploy a task sequence to SEA-W81 to perform the operating system refresh.

### 24.1.2 Task 1: Create a device collection

1. On **SEA-CFG1**, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Configuration Manager Console**. The Microsoft Endpoint Configuration Manager console opens.
3. In the **Assets and Compliance** workspace, select **Device Collections**.
4. Right-click **Device Collections** and then select **Create Device Collection**. The Create Device Collection Wizard opens.
5. On the **General** page, configure the following and then select **Next**:
   - Name: **Windows 10 Deployment**
   - Comment: **Devices targeted to install Windows 10**
   - Limiting collection: **All Systems**
6. On the **Membership Rules** page, select **Next**. At the Configuration Manager warning, select **OK**. You will add a direct member at a later step.
7. On the **Summary** page, select **Next** and then at the **Completion** page, select **Close**. The **Windows 10 Deployment** collection is displayed in the Device Collections list.

### 24.1.3 Task 2: Assign a Device to an existing Collection

1. In the **Assets and Compliance** workspace, select **Devices**. Take note of the devices listed. Any device that has a green circle with a white checkmark are currently active.
2. In the details pane, select **SEA-W81**.
3. Right-click **SEA-W81**, point to **Add Selected Items**, and then select **Add Selected Items to Existing Device Collection**.
4. On the **Select Collection** dialog box, select **Windows 10 Deployment**, and then select **OK**.
5. To verify, in the **Assets and Compliance** workspace, select **Device Collections** and then double-click **Windows 10 Deployment**. SEA-W81 should be listed as a member of this collection.

### 24.1.4 Task 3: Import an Operating System Image

1. In the Microsoft Endpoint Configuration Manager console select the **Software Library** workspace.
2. In the **Software Library** workspace, expand **Operating Systems** and then select **Operating System Images**.

3. Right-click **Operating System Images** and then select **Add Operating System Image**. The **Add Operating System Image Wizard** displays.
4. On the **Data Source** page, select **Browse** and then enter **\\sea-cfg1\Software\ISO\sources\install.wim** and then choose **Open**.
5. On the **Data Source** page, next to **Architecture**, select **x64** and next to **Language** select **English (United States)** and then select **Next**.
6. In the **General** page, configure the following and then select **Next**:
   - Name: **Windows 10 Enterprise**
   - Version: **20H2**
7. On the **Summary** page, select **Next**.
8. On the **Completion** page, select **Close**.

#### 24.1.5 Task 4: Distribute content to distribution points

1. With **Operating System Images** selected, in the details pane, right-click **Windows 10 Enterprise** and then select **Distribute Content**.
2. On the **General** page, select **Next**.
3. On the **Content Destination** page, select **Add** and then select **Distribution Point**.
4. On the **Add Distribution Points** dialog box, select the check box next to **SEA-CFG1.CONTOSO.COM**, and then select **OK**.
5. On the **Content Destination** page, select **Next**.
6. On the **Summary** page, select **Next** and then select **Close**.
7. In the Ribbon, select **Refresh** and verify that the **Content Status** circle turns green and **Success** shows **1** to indicate that the content has been distributed to 1 distribution point.

#### 24.1.6 Task 5: Configure Boot Images

1. In the Microsoft Endpoint Configuration Manager console select the **Software Library** workspace.
2. In the **Software Library** workspace, expand **Operating Systems** and then select **Boot Images**. Notice the **Boot image (x64)** and **Boot image (x86)** objects already created in the details pane. These are created when you first install Endpoint Configuration Manager.
3. Right-click **Boot image (x64)** and then select **Properties**.
4. In the **Customization** page, select the check box next to **Enable command support (testing only)** and then select **OK**.
5. At the Configuration Manager message box, select **No**. You will distribute both boot images in the next task.

#### 24.1.7 Task 6: Distribute Boot Images to distribution points

1. With the **Boot Images** node selected, in the details pane, right-click **Boot image (x64)** and then select **Distribute Content**.
2. On the **General** page, select **Next**.
3. On the **Content Destination** page, select **Add** and then select **Distribution Point**.
4. On the **Add Distribution Points** dialog box, select the check box next to **SEA-CFG1.CONTOSO.COM**, and then select **OK**.
5. On the **Content Destination** page, select **Next**.
6. On the **Summary** page, select **Next** and then select **Close**.
7. Repeat steps 1-6 for **Boot image (x86)**.
8. Select each boot image, and then in the Ribbon, select **Refresh**. Verify that the **Content Status** circle turns green and **Success** shows **1**.

#### 24.1.8 Task 7: Create an Install image Task Sequence

1. In the Microsoft Endpoint Configuration Manager console select the **Software Library** workspace.
2. In the **Software Library** workspace, expand **Operating Systems** and then select **Task Sequences**.
3. Right-click **Task Sequences** and then select **Create Task Sequence**. The **Create Task Sequence Wizard** displays.
4. On the **Create a new task sequence** page, select **Install an existing image package**, and then select **Next**.
5. On the **Specify task sequence information** page, in the **Task sequence name** box, enter **Deploy Windows 10 Enterprise**.
6. Next to **Boot image**, select **Browse**.

7. In the **Select a Boot Image** dialog box, select **Boot image (x64) en-US**, and then select **OK**.
8. Select the check box next to **Run as high performance power plan,** and then select **Next**.
9. On the **Install Windows** page, select **Browse**, select **Windows 10 Enterprise 20H2 en-US**, and then select **OK**.
10. Remove the check mark next to **Configure task sequence for use with BitLocker**.
11. On the **Select an Operating System Upgrade Package** dialog box, select **Windows 10 Enterprise 20H2 en-US** and then select **OK**.
12. Select **Enable the account and specify the local administrator password**, and then in the **Password** and **Confirm password** boxes, enter **Pa55w.rd**.
13. On the **Install Windows** page, select **Next**.
14. On the **Configure Network** page, select **Join a domain**.
15. Next to **Domain**, select **Browse**, and then select **Contoso.com**, and then select **OK**.
16. Next to **Domain OU**, select **Browse**, and then select **Seattle Clients**, and then select **OK**.
17. On the **Specify the account that has permissions to join the domain**, select **Set**. Provide the user name **Contoso\Administrator** and the password of **Pa55w.rd**.
18. On the **Configure Network** page, select **Next**.
19. On the **Install Configuration Manager** page, ensure that **Configuration Manager Client Package** is selected and then select **Next**.
20. On the **State Migration** page, remove the check mark next to **Capture user settings and files**, and then select **Next**.
21. On the **Include Updates** page, select **Do not install any software updates**, and then select **Next**.
22. On the **Install Applications** page, select **Next**.
23. On the **Confirm the settings** page, select **Next**.
24. On the **Completion** page, select **Close**.
25. Right-click the **Deploy Windows 10 Enterprise** task sequence and then select **View**. Review the steps of the task sequence and then close the window.

#### 24.1.9 Task 8: Deploy the Windows 10 Task Sequence

1. In the Microsoft Endpoint Configuration Manager console select the **Software Library** workspace.
2. In the **Software Library** workspace, expand **Operating Systems** and then select **Task Sequences**.
3. In the details pane, right-click the **Deploy Windows 10 Enterprise** task sequence and then select **Deploy**.
4. On the **General** page, next to **Collection**, select **Browse**. At the warning, select **OK**.
5. Select the **Windows 10 Deployment** collection, and then select **OK**.
6. On the **General** page, select **Next**.
7. On the **Deployment Settings** page, select **Next**.
8. On the **Scheduling** page, select **Next** to make the deployment be available as soon as possible.
9. On the **User Experience** page, take note of the default settings and then select **Next**.
10. On the **Alerts** page, select **Next**.
11. On the **Distribution Points** page, select **Next**.
12. On the **Summary** page, select **Next**.
13. On the **Completion** page, select **Close**.

#### 24.1.10 Task 9: Run the Windows 10 Task Sequence

1. Switch to SEA-W81, and sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. Click **Start** and then enter **Control Panel**.
3. In the results, select **Control Panel**.
4. In the **Control panel**, select **System and Security**.
5. In **System and Security**, select **Configuration Manager**. Configuration Manager Properties is displayed.
6. In the **Configuration Manager Properties** dialog box, select the **Actions** tab.
7. On the **Actions** tab, select **Machine Policy Retrieval & Evaluation Cycle**, and then select **Run Now**. At the message prompt, select **OK**.
8. Select **OK** to close the **Configuration Manager Properties**, and then close **Control Panel**.
9. In the notification area, select **New Software is Available** and then select **Open Software Center**. You might need to expand the notification area arrow to display the icon.
10. In the **Software Center**, on the **Operating Systems** page, notice the new operating system available named **Deploy Windows 10 Enterprise**.
11. Select **Deploy Windows 10 Enterprise** and then select **Install**.

12. On the **Confirm you want to upgrade the operating system on this computer**, select **Install**. The software will download and the task sequence begins. It will take a while to complete the install and will restart the computer as needed.
13. After the installation is complete, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
14. Verify that the computer has successfully been refreshed and then sign out of SEA-W81.

**Results**: After completing this exercise, you will have successfully used Microsoft Endpoint Configuration Manager to deploy Windows 10.

**END OF LAB**

# 25 Practice Lab: Deploying Windows 10 with Autopilot

## 25.1 Summary

In this lab you will learn how provision a Windows 10 device with Autopilot using User-driven mode.

### 25.1.1 Scenario

Contoso IT is planning to roll out a deployment of new Windows 10 devices using Autopilot. The devices have a default installation of Windows 10. Users should be able to connect the device, turn it on, and answer minimal questions during the OOBE, using their Azure AD credentials to sign in. The process should automatically enroll and join the Azure AD domain. You have been asked to configure and test the experience using the SEA-WS4, which you recently installed and configured using Hyper-V.

### 25.1.2 Task 1: Create group in Azure AD

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, in the address bar, type **https://aad.portal.azure.com**, and then press **Enter**. If prompted, sign in with your **Admin@yourtenant.onmicrosoft.com** and the default tenant password.
4. In the navigation pane, select **Azure Active Directory**.
5. Under **Manage**, select **Groups**.
6. In the **Groups | All groups** blade, select **New group**.
7. In the **New Group** blade, in the **Group type** list, select **Security**.
8. In the **Group name** box, type **IT Devices**.
9. In the **Group description** box, type **IT Department Devices**.
10. In the **Membership type** list, select **Dynamic Device**.
11. Select **Add dynamic query**.
12. On the **Dynamic membership rules** blade select **Edit** above the **Rule syntax** box.
13. In the Edit rule syntax text box, add the following simple membership rule and select **OK**.

```
(device.devicePhysicalIDs -any (_ -contains "[ZTDId]"))
```

14. Select **Save** to close **Dynamic membership rules**, and then select **Create** to create the group.

### 25.1.3 Task 2: Generate a device-specific comma-separated value (CSV) file

1. Switch to **SEA-SVR2** and sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. Select **Hyper-V Manager** in the taskbar.
3. Under Virtual Machines, right-click **SEA-WS4** and select **Connect**.
4. On the **SEA-WS4** window, select **Start**. When the computer starts, maximize the window.
5. Sign in to **SEA-WS4** as **Administrator** with the password of **Pa55w.rd**.
6. Right-click **Start**, select **Windows PowerShell (Admin)**, and then select **Yes** at the **User Account Control** prompt.
7. At the Windows PowerShell command-line prompt, type the following cmdlet, and then press **Enter**:

```
Install-Script -Name Get-WindowsAutoPilotInfo
```

8. You will receive three prompts. Each time, type **Y**, and then press **Enter**.
9. At the Windows PowerShell command-line prompt, type the following cmdlet, and then press **Enter**:

```
Set-ExecutionPolicy RemoteSigned
```

10. When prompted, type **Y**, and then press Enter.
11. At the Windows PowerShell command-line prompt, type the following cmdlet, and then press **Enter**:

```
Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Computer.csv
```

12. At the Windows PowerShell command-line prompt, type the following command, press **Enter**, and then review the file content:

```
type C:\Computer.csv
```

13. At the Windows PowerShell command-line prompt, type the following command, press **Enter**. This will copy the file to SEA-SVR2:

```
copy c:\computer.csv \\sea-svr2\labfiles
```

14. Close the Windows PowerShell command prompt.

#### 25.1.4 Task 3: Work with a Windows Autopilot deployment profile

1. Switch to **SEA-CL1**.
2. In **Microsoft Edge**, open a new tab and navigate to **https://endpoint.microsoft.com**. If prompted, sign in with your **Admin@yourtenant.onmicrosoft.com**.
3. In the **Microsoft Endpoint Manager admin center**, select **Devices**.
4. In the **Device enrollment** section, select **Enroll devices**.
5. In the details pane scroll down to **Windows Autopilot Deployment Program**, and then select **Devices**.
6. In the **Windows Autopilot devices** blade on the menu bar, select **Import**, select the **folder icon** and then browse to **\\SEA-SVR2\Labfiles**, select **Computer.csv**, select **Open**, and then select **Import**.

   *Note: The import process can take up to 15 minutes, but normally takes around 5 minutes.*

   ***Important**: After the process is complete, the device may not show. If this is the case, select the **Sync** button, wait a few minutes, and then select **Refresh**.*
7. Select **X** to close the **Windows Autopilot devices** blade.
8. On the Windows enrollment blade, in the details pane, select **Deployment Profiles**.
9. On the **Windows AutoPilot deployment profiles** blade, select **Create profile** and then select **Windows PC**.
10. In the **Basics** tab, in the **Name** text box, type **Contoso profile1**.
11. For **Convert all targeted devices to Autopilot** select **No**, and then select **Next**.
12. On the **Out-of-box experience (OOBE)** tab, ensure that the **Deployment mode** is set to **User-Driven**.
13. Ensure that **Join to Azure AD as** is set to **Azure AD Joined**.
14. Ensure that the following options are set:
    - Microsoft Software License Terms: **Hide**
    - Privacy Settings: **Hide**

- Hide change account options: **Hide**
- User account type: **Administrator**.
- Allow White Glove OOBE: **No**.
- Apply device name template: **No**.

15. Select **Next**.
16. On the **Assignments** tab, under **Included groups** select **Add groups**.
17. Select the **IT Devices** group and select **Select**. Select **Next**.
18. On the **Review + create** blade, review the information and then select **Create**.

#### 25.1.5 Task 4: Reset the PC

1. Switch to **SEA-SVR2**. The SEA-WS4 computer should be still maximized.
2. On **SEA-WS4**, select **Start**, type **reset** and select **Reset this PC**.
3. Under **Reset this PC**, select **Get started**.
4. Select **Remove everything**, and then select **Local reinstall**.
5. Select **Next** and then select **Reset**.

   *Note: Normally this task is not required for new deployment of physical devices. The device's autopilot info is either provided by the manufacturer or can be obtained from the device prior to the OOBE. For the purposes of this lab, we must initiate a reset to simulate a new device OOBE.*

   *Note: This process can take 30-45 minutes and will reboot several times during the process.*

#### 25.1.6 Task 5: Verify Autopilot deployment

1. At the **Welcome to Contoso** screen, enter **Aaron@yourtenant.onmicrosoft.com** and select **Next**.
2. At the Password page, enter **Pa55w.rd1234** and select **Next**.
3. At the **Use Windows Hello with your account**, select **OK**.
4. On the **More information required** page, select **Next**.
5. On the **Keep your account secure** page, enter your phone number of a mobile device that can receive text messages, and then select **Next**.
6. In the **Enter code** page, enter the verification code and then select **Next**.
7. On the SMS verified message, select **Next** and then select **Done**.
8. On the **Setup up a PIN** dialog box, in the **New PIN** and **Confirm PIN** fields, enter **102938**, and then select **OK**.
9. On the **All set!** page, select **OK**.
10. Select **Start** and select **Settings**.
11. Select **Accounts**, and then select **Access work or school**. Verify the device is connected to Contoso's Azure AD.
12. Select **Connected to Contoso's Azure AD** and select **Info**.
13. On the **Managed by Contoso** page, scroll down and then select **Sync**.
14. On **SEA-WS4**, close the **Settings** window.
15. Shut down **SEA-WS4** and close the SEA-WS4 window.
16. On SEA-SVR2, close Hyper-V Manager.
17. Switch to **SEA-CL1**.
18. In the Azure Active Directory admin center, select **Azure Active Directory** and then **Devices**. Note that the new device displays with an icon that indicates an Autopilot device. Also note that the Join Type is Azure AD joined with Aaron Nicholls as the owner.
19. On **SEA-CL1**, close Microsoft Edge.

**Results**: After completing this exercise, you will have provisioned a Windows 10 device with Autopilot using User-driven mode.

**END OF LAB**

# 26 Practice Lab: Configuring Co-Management Using Configuration Manager

## 26.1 Summary

In this lab, you will configure Co-Management using Microsoft Endpoint Configuration Manager and Microsoft Intune.

### 26.1.1 Scenario

Contoso has both a Microsoft Endpoint Configuration Manager implementation and Microsoft Intune. You need to configure integration between the two services and enable co-management for your managed Windows 10 devices. You will configure co-management and then validate the settings using SEA-CL1.

### 26.1.2 Task 1: Prepare the environment

1. Switch to **SEA-SVR1** and sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. Select **Start**, expand **Windows Administrative Tools**, and then select **Active Directory Users and Computers**.
3. In the navigation pane, select **Seattle Clients**.
4. Right-click **SEA-CL1** and then select **Move**.
5. In the **Move** dialog box, select **Azure AD clients** and then select **OK**.
6. Close **Active Directory Users and Computers**.
7. On the taskbar, right-click **Start** and select **Windows Powershell (Admin)**.
8. In the **Windows PowerShell** window, type the following command, and then press **Enter**:

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

9. Close the PowerShell window.
10. Switch to **SEA-CL1**.
11. On the taskbar, right-click **Start**, select **Shut down or sign out** and then select **Restart**.

    *Note: The reboot will trigger the hybrid Azure AD join on SEA-CL1.*

12. After **SEA-CL1** has restarted, sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
13. On the taskbar, right-click **Start** and select **Windows PowerShell (Admin)**.
14. In the **Windows PowerShell** window, type the following command, and then press **Enter**:

```
dsregcmd /status
```

15. In the output under **Device State**, verify that **AzureAdJoined : YES** and **DomainJoined : YES** are displayed.

*Note: If the device is not yet joined to Azure AD wait for the Azure AD Connect sync to complete and reboot SEA-CL1 again.*

16. Close all windows on SEA-CL1.

### 26.1.3 Task 2: Create a device collection

1. On **SEA-CFG1**, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Configuration Manager Console**. The Microsoft Endpoint Configuration Manager console opens.
3. In the **Assets and Compliance** workspace, select **Device Collections**.
4. Right-click **Device Collections** and then select **Create Device Collection**. The Create Device Collection Wizard opens.
5. On the **General** page, configure the following and then select **Next**:
   - Name: **Co-managed Devices**
   - Limiting collection: **All Desktop and Server Clients**
6. On the **Membership Rules** page, select **Next**. At the Configuration Manager warning, select **OK**. You will add a direct member at a later step.
7. On the **Summary** page, select **Next** and then at the **Completion** page, select **Close**.

### 26.1.4 Task 3: Assign a Device to an existing Collection

1. In the **Assets and Compliance** workspace, select **Devices**. Take note of the devices listed. Any device that has a green circle with a white checkmark are currently active.
2. In the details pane, select **SEA-CL1**.
3. Right-click **SEA-CL1**, point to **Add Selected Items**, and then select **Add Selected Items to Existing Device Collection**.
4. On the **Select Collection** dialog box, select **Co-managed Devices**, and then select **OK**.
5. To verify, in the **Assets and Compliance** workspace, select **Device Collections** and then double-click **Co-managed Devices**. SEA-CL1 should be listed as a member of this collection.

### 26.1.5 Task 4: Tenant attach Endpoint Configuration Manager

1. In the Microsoft Endpoint Configuration Manager console, select the **Administration** workspace.
2. In the **Administration** workspace, expand **Cloud Services** and then select **Co-management**.
3. In the ribbon, select **Configure co-management**. The **Co-management Configuration Wizard** opens.
4. In the **Co-management Configuration Wizard**, on the **Tenant onboarding** page, select **Sign In**.
5. Sign in as as **admin@yourtenant.onmicrosoft.com** with the default tenant password. After you are signed in, select Next.
6. On the **Create AAD Application** warning, select **Yes**.
7. On the **Configure upload** page, accept the default and select **Next**.
8. On the **Enablement** page, next to **Automatic enrollment in Intune**, select the drop-down and then select **Pilot**.
9. On the **Enablement** page, next to **Intune Auto Enrollment**, select **Browse**.
10. In the **Select Collection** dialog box, select **Co-managed Devices** and then select **OK**. Select **Next**.
11. On the **Workloads** page, drag the slider to **Pilot Intune** for the following workloads, and then select **Next**:
    - **Compliance policies**
    - **Client apps**
    - **Windows Update policies**
12. On the **Staging** page, select **Browse** next to **Compliance policies**, **Client Apps**, and **Windows Update Policies** and select the **Co-managed Devices** collection for each workload. Select **Next**.
13. On the **Summary** page, select **Next** and then on the **Completion** page, select **Close**.

### 26.1.6 Task 5: Validate that SEA-CL1 is co-managed

1. Switch to SEA-CL1.
2. On the taskbar select **Microsoft Edge**, in the address bar type **https://aad.portal.azure.com**, and then press **Enter**.
3. Sign in as user **Admin@yourtenant.onmicrosoft.com**, and use the tenant Admin password. If the **Stay signed in?** prompt appears, select **No**. The Azure Active Directory admin center opens.
4. In the Azure Active Directory admin center, in the navigation pane, select **Azure Active Directory**.
5. In the **Contoso|Overview** page, under **Manage**, select **Devices**.
6. Verify that **SEA-CL1** is listed and that **Join Type** is **Hybrid Azure AD Join**.
7. In Microsoft Edge open another tab and type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
8. In the navigation pane, select **Devices** and then select **All devices**.
9. Verify that **SEA-CL1** is listed with the **Managed by** setting set to **Co-managed**. It may take some time to appear. Refresh the details pane as needed.
10. Select **SEA-CL1** and in the details pane scroll down to display information related to the Co-managed state.
11. Close Microsoft Edge.

**Results**: After completing this exercise, you will have successfully configured co-management using Microsoft Endpoint Configuration Manager and Microsoft Intune.

**END OF LAB**

# 27 Practice Lab: Managing Windows 10 security and feature updates

## 27.1 Summary

In this lab you will configure Windows 10 security and feature update settings using Intune.

### 27.1.1 Scenario

You have been asked to configure Update Rings in Intune to manage Windows update settings. Devices should be configured to be in the Semi-Annual channel and Feature updates deferred 45 days after release. You would like to test the settings using SEA-WS2.

#### 27.1.1.1 Task 1: Verify current update settings for a single device

1. On **SEA-WS2**, sign in as as **Diego Siciliani** with the PIN **102938**.
2. Select **Start**, and then select the **Settings** icon.
3. In **Settings**, select **Update & Security**.
4. Select **Delivery Optimization**.
5. On the **Delivery Optimization** page, verify that the **Allow downloads from other PCs** option is enabled.
6. Select **PCs on my local network, and PCs on the Internet**.
7. In the navigation pane, select **Windows Insider Program**. Notice that you must change the level of diagnostic data before you can get Insider Preview builds.
8. Select the **Go to Diagnostics & Feedback settings to turn on optional diagnostic data** link.
9. On the Diagnostics and feedback page, set **Diagnostic data** setting to **Optional diagnostic data**.
10. In the Settings navigation on the left, select **Home**. Select **Update & Security** and then select **Windows Insider Program**.
11. Note that the **Get Started** option is now available.
12. In the navigation pane, select **Home** and then select **Update & Security**.

#### 27.1.1.2 Task 2: Review applied settings

1. On the **Windows Update** page, select **View update history**.
2. Review the updates listed, if any, and then select **Uninstall updates**.
3. Review the updates listed in **Installed Updates**. Close Installed Updates.
4. On the **View update history** page, select **Back**. Close the **Settings** app.

#### 27.1.1.3 Task 3: Configure update settings by using Intune

1. Switch to **SEA-CL1** and sign in as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In Microsoft Edge, type **https://endpoint.microsoft.com** in the address bar, and then press **Enter**.
4. In the navigation pane, select **Devices** and then select **Windows 10 update rings**.
5. On the **Devices | Windows 10 update rings** blade select **Create profile**.
6. In the **Basics** blade, enter the following information, and then select **Next**:
   - Name: **Contoso Updates - standard**
   - Description: **Standard Windows updates configuration**
7. In the **Update ring settings** blade, enter the following information, and then select **Next**:
   - Servicing channel: **Semi-Annual Channel**
   - Feature update deferral period (days): **45**
   - Option to pause Windows updates: **Disable**
8. On the **Assignments** blade, under **Included groups** select **Add groups**.

9. On the **Select groups to include** blade, in the **Search** box, select **Contoso Developer devices** and then select **Select**.
10. Select **Next** and on the **Review + create** blade select **Create**.
11. From the navigation bar select **Configuration profiles**.
12. On the **Devices | Configuration profiles** blade, in the details pane, select **Create profile**.
13. In the **Create a profile** blade, select the following options, and then select **Create**:
    - Platform: **Windows 10 and later**
    - Profile type: **Templates**
    - Template name: **Delivery Optimization**
14. In the **Basics** blade, enter the following information, and then select **Next**:
    - Name: **Contoso Developer - Delivery optimization**
    - Description: **Delivery optimization for Developer**
15. In the **Configuration settings** blade, enter the following information, and then select **Next**:
    - Download Mode: **HTTP only, no peering (0)**
16. On the **Assignments** blade, under **Included groups** select **Add groups**.
17. On the **Select groups to include** blade, select **Contoso Developer devices** and then select **Select**.
18. Select **Next** twice, and on the **Review + create** blade select **Create**.

#### 27.1.1.4 Task 4: Verify that the device's update settings are managed centrally

1. Switch to **SEA-WS2**.
2. Select **Start**, and then select the **Settings** icon.
3. In the **Settings** app, select the **Accounts** tile and then select **Access work or school**.
4. In the **Access work or school** section, select the **Connected to Contoso's Azure AD** link and then select **Info**.
5. In the **Managed by Contoso** dialog box, select **Sync**. Wait for the synchronization to complete.
6. Select the left arrow in the upper left corner twice. Select **Update & Security**.
7. Notice the red banner **Some settings are managed by your organization**.
8. Select **Advanced options**. Notice that you are not able to pause updates.
9. Select **Delivery Optimization**. Notice that **Allow downloads from other PCs** is not available.
10. In the navigation pane, select **Windows Insider Program**.
11. On the **Windows Insider Program** tab, notice the **Some settings are hidden or managed by your organization** banner.
12. Notice that the **Get started** button is unavailable. Close the **Settings** app.
13. Close all open apps and windows.

*Note: These labs are configured to prevent Windows Updates from being applied to avoid delays and unintentional impact during the labs.*

**END OF LAB**