

MS-101T00

Microsoft 365 Mobility and Security

Change Log

October 2022

Purpose

This document highlights the significant changes to the MS-100T00 – Microsoft 365 Mobility and Security course from the previous release. This document is for Microsoft Certified Trainers and Instructors to use before they deliver the class or during preparation for teaching the class.

This is not an error log or a supplement to the Course Materials. This document just provides additional context so that you can understand the major changes to the course content. Most of the course materials have been updated to fix typos, broken links, and formatting. So, we recommend you always download the latest copies.

✓ Please read the Trainer Prep Guide, which provides the overall strategy for implementing this training.

October 2022 Revision

Update: **MAJOR**

Type of change: **GENERAL/CONTENT/SLIDES/LABS**

GENERAL

- One of the most significant changes in this release was simply a change in course terminology. Microsoft World-Wide Learning (WWL) has moved to a more Learn-based model of courseware terminology in its ILT courses. The following table shows the old ILT terms and the new ILT terms.

Old ILT term	New ILT term
Module	Learning Path
Lesson	Module
Topic	Unit

The potentially confusing part is the term “Module”. The old “Module” is now a “Learning Path”, and the old “Lesson” is now a “Module”. This is something you will just have to get used to. All slides have been updated to reflect this new terminology. From this point forward, all terminology references will use the new Learn nomenclature.

CONTENT

- Content was updated to reflect changes agreed upon in the March 2022 JTA Refresh.
- Content changes across the entire course included:
 - All content was reviewed, and outdated content was either updated or removed.
 - Various units were moved to different Learning Paths and/or Modules for improved instructional design flow.
 - Renamed multiple units and modules to better reflect the purpose of the content.
- Learning Path 1 updates:
 - Module 3, unit 2. Renamed unit from “Enhance your email security using Microsoft Defender for Office 365” to “Enhance your email security using Exchange Online Protection and Microsoft Defender for Office 365”. Added more content on Exchange Online Protection.
 - Module 3. Added new unit 7 (Review the security reports in Microsoft 365 Defender) that summarizes the security reports in Microsoft 365 Defender.

- Learning Path 2 updates:
 - Module 1. Major revisions to units 2-5.
 - Module 1. Moved the old unit 5 (Explore the spoofing protection provided by EOP) to Module 2.
 - Module 1. Added new unit 6 (Examine outbound spam filtering).
 - Module 2. Added new units 2 (Climb the security ladder from EOP to Microsoft Defender for Office 365), 7 (Configure outbound spam filtering policies), and 8 (Unblock users from sending email).
 - Module 2. Deleted old units 4 (Configure Safe Attachment policy options) and 6 (Configure Safe Links policy options) as modules 3 and 4 already cover these items.
 - Module 2, unit 6 (Manage spoofed intelligence). Moved this in here from Module 1, where it was originally named "Explore the spoofing protection provided by EOP". Moved it in here and renamed it.
 - Module 3. Renamed unit 2 from "Create Safe Attachment policies in the SCC" to "Create Safe Attachment policies in Microsoft Defender for Office 365".
 - Module 4. Renamed unit 2 from "Create Safe Links policies in the SCC" to "Create Safe Links policies in Microsoft Defender for Office 365".
 - Deleted Module 5 (Explore reporting in the Microsoft 365 security services). Instead, created a new unit in LP1, Module 3 that provides a summary of the key security reports.
- Learning Path 3 updates:
 - Renamed LP from "Implement threat intelligence in Microsoft 365" to "Implement threat protection by using Microsoft 365 Defender".
 - Module 1. Added new units 3 (Explore alert policies in Microsoft 365" and 7 (Explore threat analytics in Microsoft 365).
 - Module 1. Deleted the old unit 3 (Examine the Security Dashboard in the Security & Compliance Center) per Job Task Analysis.
 - Module 1. Moved old units 4 (Investigate security attacks by using Threat Explorer), 5 (Identify cybersecurity issues by using Threat Trackers), and 6 (Prepare for attacks with Attack Simulation training) to Module 4.
 - Deleted the old Module 2 (Explore the Security Dashboard). Replaced it with new Module 4 (Implement threat protection by using Microsoft Defender for Office 365).
 - Deleted the old Module 3 (Implement Microsoft Defender for Identity).
 - Renumbered the old Module 4 (Implement Microsoft Cloud Application Security) to Module 2 and renamed it (Implement app protection by using Microsoft Defender for Cloud Apps).
 - Module 2. Major revisions to units 2-4 and 7, and renamed each to reference Microsoft Defender for Cloud Apps.
 - Module 2. Added new unit 6 (Configure Cloud Discovery in Microsoft Defender for Cloud Apps).
 - Added new Module 3 (Implement endpoint protection by using Microsoft Defender for Endpoint).

- Added new Module 4 (Implement threat protection by using Microsoft Defender for Office 365).
- Learning Path 4 updates:
 - Renamed LP from “Explore Data Governance in Microsoft 365” to “Explore data governance and compliance in Microsoft 365”.
 - Added new Module 1 (Examine governance and compliance solutions in Microsoft Purview).
 - Renumbered old Module 1 (Explore archiving in Microsoft 365) to Module 2 and renamed it to “Explore archiving and records management in Microsoft 365”.
 - Module 2, unit 2 (Explore data governance in Microsoft 365). Moved it to the new Module 1.
 - Module 2. Deleted the old unit 3 (Compare in-place archiving and records management).
 - Module 2. Renumbered old unit 4 (Explore in-place archiving in Exchange) to unit 2 and renamed it to “Explore archive mailboxes in Microsoft 365”. Made major revision to content.
 - Module 2. Renumbered old unit 5 (Explore in-place records management in SharePoint) to unit 4 and renamed it to “Explore records management in Microsoft 365”. Made major revision to content.
 - Module 2. Added new units 3 (Enable archive mailboxes in Microsoft 365), 5 (Implement records management in Microsoft 365), 6 (Recover deleted data in Exchange Online), and 7 (Recover deleted data in SharePoint Online).
 - Renumbered old Module 2 (Explore retention in Microsoft 365) to Module 3.
 - Module 3. Major revisions to units 2, 5, and 6. Also renamed each
 - Module 3. Deleted units 3 and 4, which dealt with Messaging Records Management (MRM). Since MRM is being replaced by retention policies and labels for records management (even for email messages in Exchange), we replaced these two units with new units 3 and 4.
 - Module 3. Added new units 3 (Compare capabilities in retention policies and retention labels) 4 (Define the scope of a retention policy), and 7 (Restrict retention changes by using preservation lock).
 - Module 4. Renamed from “Explore Office 365 Message Encryption” to “Explore Microsoft Purview Message Encryption”.
 - Module 4. Major revisions to all units, and renamed each.
 - Module 4. Added new unit 5 (Add organizational branding to encrypted email messages).
 - Module 4. Deleted unit 6 (Examine additional encryption methods in Microsoft 365).
 - Deleted Module 5 (Explore In-place Records Management in SharePoint). It was for SharePoint Server and not SharePoint Online. SP Online uses retention policies and labels covered in Module 3.
 - Moved Module 5 (Explore Data Loss Prevention in Microsoft 365) to Learning Path 5, Module 4, where it’s a better fit.
- Learning Path 5 updates:
 - Renamed LP from “Implement Data Governance in Microsoft 365” to “Implement compliance in Microsoft 365”.

- Module 1. Renamed from “Evaluate your compliance readiness” to “Explore compliance in Microsoft 365”.
- Module 1. Major revisions to units 2 (Plan for security and compliance in Microsoft 365) and 6 (Analyze the Microsoft compliance score).
- Module 1. Added new units 3 (Plan your beginning compliance tasks in Microsoft Purview), 4 (Manage your compliance requirements with Compliance Manager), and 5 (Examine the Compliance Manager dashboard).
- Module 1. Deleted old units 4 (Explore the Microsoft 365 Compliance Center), 5 (Examine the Compliance Score components), and 6 (Examine the Compliance Score assessments).
- Module 2. Renamed from “Implement compliance solutions” to “Implement Microsoft Purview insider risk management”.
- Module 2. Major revisions to units 2, 5, and 6.
- Module 2. Added new units 3 (Plan for insider risk management), 4 (Explore insider risk management), and 7 (Explore insider risk management cases).
- Module 2. Deleted old units 5 (Explore communication compliance in the Compliance Center) and 6 (Explore the compliance toolset in Microsoft 365).
- Module 3. Major revisions to units 2-3.
- Module 3. Added new units 4 (Examine information barriers in Microsoft Teams), 5 (Examine information barriers in OneDrive), and 6 (Examine information barriers in SharePoint).
- Module 3. Deleted old units 4-6, all dealing with ethical walls.
- Module 4 (Explore Data Loss Prevention in Microsoft 365) was moved in from Learning Path 4, module 5.
- Module 4. Major revisions to units 2 (Examine data loss prevention) and 4 (Examine DLP policies).
- Module 4. Added new units 3 (Explore Endpoint data loss prevention), 5 (View DLP policy results), and 6 (Explore DLP reports).
- Module 4. Moved old units 7 (Configure email notifications for DLP policies) and 8 (Configure policy tips for DLP policies) to Module 5.
- Deleted old Module 4 (Create a DLP policy from a built-in template).
- Added new Module 5 (“Implement data loss prevention policies”).
- Module 5. Added new units 2-5. Moved in units 6-7 from Module 4.
- Deleted old Module 5 (Create a custom DLP policy).
- Deleted old Module 6 (Create a DLP policy to protect documents).
- Deleted old Module 7 (Implement policy tips for DLP policies)
- Learning Path 6 updates:
 - Renamed LP from “Manage data governance in Microsoft 365” to “Manage compliance in Microsoft 365”.
 - Deleted old Module 1 (Manage retention in email).
 - Added new Module 1 (Implement data classification of sensitive information).
 - Deleted old Module 2 (Troubleshoot data governance).

- Module 3. Deleted old unit 2 (Develop a data classification framework for your sensitivity labels). This was about data classification framework, which was covered in Module 1.
- Module 3. Added new unit 2 (Plan your deployment strategy for sensitivity labels).
- Deleted module 5 (Implement Windows Information Protection, which has been deprecated).
- Learning Path 7 updates:
 - Module 1. Renamed from “Search for content in the Microsoft 365 Compliance center” to “Search for content in the Microsoft Purview compliance portal”.
 - Module 1. Major revisions to units 2-6.
 - Module 1. Deleted old unit 7 (Search for items from a third-party data source).
 - Module 1. Added new unit 7 (Search for and delete email messages).
 - Deleted old Module 2 (Conduct audit log investigations).
 - Added new Module 2 (Manage Microsoft Purview Audit (Standard)).
 - Deleted old Module 3 (Manage Advanced eDiscovery).
 - Added new Module 3 (Manage Microsoft Purview Audit (Premium)).
 - Added new Module 4 (Manage Microsoft Purview eDiscovery (Standard)).
 - Added new Module 5 (Manage Microsoft Purview eDiscovery (Premium)).
- Learning Path 8 updates:
 - Module 1. Renamed from “Explore Co-management of Windows 10 devices” to “Explore device management using Microsoft Endpoint Manager”.
 - Module 1. Added new units 2 (Explore device management in Microsoft Endpoint Manager), 6 (Create device profiles in Microsoft Intune).
 - Module 1. Major revision to unit 3 (Explore Co-management of Windows devices).
 - Module 1. Moved old unit 3 (Plan your Co-management strategy) to Module 2.
 - Module 1. Deleted old unit 5 (Enable Co-management by using Azure Active Directory).
 - Module 1. Added a new Discussion slide (Device management methodology) at end of the module.
 - Module 2. Moved in unit 2 from Module 1, and units 6 and 7 from Module 3.
 - Module 2. Major revision to unit 5 (Enroll Windows devices to Intune).
 - Deleted old Module 3 (Transition from Configuration Manager to Intune).
 - Deleted old Module 4 (Examine the Microsoft Store for Business), since Microsoft Store for Business is being deprecated in Q1 2023 and being replaced with Windows 11 Store.
 - Renumbered old Module 5 (Plan for application management) to Module 3 and renamed to “Plan for mobile application management”.
 - Module 3. Deleted units 3 (Explore app management using Configuration Manager), 4 (Explore app management using Intune), and 5 (Explore app management using Azure AD).
 - Module 3. The only unit kept from the old module 5 was old unit 2 (now unit 4; Protect company data by using app protection policies).

- Module 3. Added new units 2 (Explore mobile application management in Microsoft Intune), 3 (Add apps to Microsoft Intune), 5 (Explore app configuration policies for Intune), and 6 (Troubleshoot app protection policy deployment in Intune).
- Learning Path 9 updates:
 - Renamed LP from “Plan your Windows 10 deployment strategy” to “Plan your deployment strategy for Windows devices”.
 - Module 1. Renamed module from “Examine Windows 10 deployment scenarios” to “Examine Windows client deployment scenarios”.
 - Module 1. Major revisions to all units.
 - Module 1. Added new Discussion unit (Deployment methodology) at end of module.
 - Module 2. Major revisions to units 4, 5, and 8.
 - Module 2. Added new Discussion unit (Autopilot deployment model) to end of module.
 - Module 3. Renamed module from “Plan your Windows 10 subscription activation strategy” to “Plan your Windows client subscription activation strategy”.
 - Module 3. Major revisions to units 2 and 3.
 - Module 3. Renamed unit 4 from “Deploy Windows 10 Enterprise licenses” to “Deploy Windows Enterprise licenses”.
 - Deleted Module 4 (Resolve Windows 10 upgrade errors). The module applied to the Modern Desktop Admin role and not the Enterprise Admin role (it was too detailed for the EA role).
 - Deleted Module 5 (Analyze Windows 10 diagnostic data using Desktop Analytics). Desktop Analytics will be retired in Nov 2022.
- Learning Path 10 updates:
 - Module 3. Added new units 2 (Review device enrollment methods) and 6 (Examine device enrollment in Intune).
 - Module 3. Major revisions to units 3-5 and 7-8.
 - Module 4. Added new units 3 (Implement compliance policies for Intune managed devices), 4 (Monitor results of your Intune device compliance policies), and 7 (Build Conditional Access policies).
 - Module 4. Renumbered old unit 3 (Configure conditional users and groups) to unit 5 and renamed to “Implement user and device groups to monitor device compliance”.
 - Module 4. Renumbered old unit 4 (Create Conditional Access policies) to unit 6 and renamed to “Explore Conditional Access policies”.
 - Module 4. Major revisions to unit 6 (Explore Conditional Access policies).
 - Added new Module 5 (Implement endpoint security in Microsoft Intune).

SLIDES

- Updated all slides to map to content changes.

LABS

- All labs were reviewed and re-tested step-by-step. Lab instructions were updated to reflect product UI changes since the prior release.
- Lab 1. Moved Exercise 1 (Initialize your Microsoft 365 tenant) so that it's after Module 4 rather than at the end of the Learning Path.
- Lab 1. Moved Exercise 2 (PIM Resource Workflows, which we renamed to PIM Administrator approval) so that it's after Module 5 rather than at the end of the Learning Path.
- Lab 1. Added new Exercises 3 (PIM Self-Approval) and 4 (PIM Teammate Approval), which are right after Exercise 2.
- Lab 3, Exercises 1 and 2. Moved to follow new Module 4 rather than Module 1. Renumbered remaining exercises from 3-6 to 1-4. Renumber Ex 1 and 2 to 5 and 6.
- Lab 4, Exercises 3 and 4. Moved to follow Module 3 rather than be at the end of the Learning Path. Renumbered exercises to 1 and 2. Renumbered old Ex 1 to Ex 3.
- Deleted Lab 4, old Exercise 2 (Validate Information Rights Management). Remove IRM lab because IRM is now activated by default for new and existing tenants.
- Deleted Lab 4, Exercise 3, Task 1 (Enable Azure Rights Management for Exchange Online). Removed Azure RMS lab because it's now activated by default for new and existing tenants. If a company did not deactivate Azure RMS manually, it is activated for everybody without any additional steps required.
- Lab 5, Exercises 1 and 2. Moved down following Module 5.
- Deleted Lab 5, Exercise 2, Task 1 (Test a MRM policy to archive email messages). Removed MRM content and lab from course.
- Lab 5, Exercise 2. Added new Task 1 (Test the first DLP policy rule) to replace the old task 1 that we deleted.
- Lab 5, Exercise 2, Task 2. Renamed from "Test a DLP policy for sensitive information" to "Test the second DLP policy rule".
- Lab 6. Renamed from "Implement data governance" to "Implement information protection".
- Deleted Lab 6, Exercise 2 (Implement Windows Information Protection) since we removed the WIP content from the course.
- Lab 7, Exercise 1. Added new task 3 (Export the search results).
- Deleted the old Lab 8 (Implement the Microsoft Store for Business), since the corresponding module was removed from the course. The old Lab 9 in Learning Path 10 was renumbered to Lab 8.
- Deleted Lab 8, Exercise 3, Tasks 3 (Manually create an EFS DRA Certificate) and 4 (Recover data using the EFS DRA certificate).

July 2021 Revision

Update: **MAJOR**

Type of change: **GENERAL/CONTENT/SLIDES/LABS**

GENERAL

- All the Modules, Lessons, and Topics were retitled to incorporate Microsoft Learn's title-naming guidelines. The new format for each title is: ***present-tense verb > task > product***

In the past, we often just had the product name as our Module, Lesson, or Topic title. In the new Learn formatting world, all titles must start with a verb associated with the task that's being covered in the Module, Lesson, or Topic. For example, the old "Planning your mail migration" unit is now titled "Select the mail migration strategy for moving your mail data to the cloud".

CONTENT

- Per Learn guidelines, a new Summary unit was added to the end of each Lesson that recapped what was covered in the lesson.
- In the past, a Knowledge Check (KC) unit was added at the end of each module. Per Learn guidelines that strive for more student interactions, a KC question was added to the end of several units in each lesson, and a KC unit was added to the end of each lesson rather than at the end of the module. Each KC unit at the end of the lesson has, on average, 3 questions.

In the KC topic at the end of each lesson, we tried to have these questions cover the topics that didn't have a KC question within the lesson. That way, the student would ideally get at least one question on each topic in a lesson. That being said, some topics just didn't lend themselves to a KC question, so it didn't always happen that way. Other times, we just felt that a given topic was so important that we would have a question at the end of the topic and then another one (or two) at the end of the lesson. But all in all, the goal of having one question per topic was the guideline we tried to follow so that every topic had at least one question on it for review, whether the question was in the topic itself or in the KC topic.

- Module 1, Lesson 3 (Explore security solutions in Microsoft 365) had two new units added to it – Protect your organization's identities using Microsoft Defender for Identity, and Protect your enterprise network against advanced threats using Microsoft Defender for Endpoint.
- Module 2, Lesson 2 (Examine Microsoft Defender for Office 365) was completely renamed from the prior version. It was Introduction to Advanced Threat Protection. This was changed

due to a branding change (ATP to Microsoft Defender). All the content in this Lesson was updated as well.

- Module 3, Lesson 1 (Explore threat intelligence in Microsoft 365) was updated. Plus we added two new units – Explore threat hunting with Microsoft Threat Protection, and Explore advanced threat hunting in Microsoft 365 Defender.
- Module 3, Lesson 5. The old Lesson was Configuring Advanced Threat Analytics. We replaced all this content with new content and renamed the lesson Implement Microsoft Defender for Identity. All units in this Lesson are new.
- Module 4, Lesson 2 (Explore Retention in Microsoft 365) had unit changes. We moved in three units from the old Module 5, lesson 3 (Manage retention by using retention policies, Create a Retention Policy in the Security and Compliance Center, and Manage a Retention Policy in the Security and Compliance Center).
- Module 4, Lesson 4 (Introduction to Security Multipurpose Internet Mail Extension (S/MIME) was deleted.
- Module 4, Lesson 6 (Explore In-place Records Management in SharePoint) was moved here from the old Module 5, Lesson 1. Also, the content in topic 5 (Benefits of In-Place Records Management) was moved to topic 2 (Examine in-place Records Management in SharePoint).
- Module 4, Lesson 7 (Data Loss Prevention in Microsoft 365), the content in unit 3 (Sensitive Information Types in DLP) was moved to unit 2 (Explore Data Loss Prevention in Microsoft 365). And the content in unit 4 (Conditions and Actions) was moved into unit 3 (Examine DLP policies). These two old units were then deleted.
- The old Lesson 5 (Archiving and Retention in Microsoft 365) was deleted. We moved lesson 1 (In-place Records Management in SharePoint) to Module 4, Lesson 6. We moved lesson 3 (Retention policies in the SCC) to Module 4, Lesson 2. And we deleted lesson 2 (Archiving and retention in Exchange).
- We renamed the old Module 6 to Module 5 (Implement data governance in Microsoft 365). All other modules after the old Module 6 were renumbered accordingly.
- Module 5, Lesson 1 (Evaluate your compliance readiness). We updated unit 3 (Explore the Microsoft 365 Compliance Center) and unit 4 (Analyze the Microsoft Compliance Score) with information regarding Compliance manager.
- Module 5, Lesson 3 (Create information barriers in Microsoft 365; which was renamed from Building Ethical Walls in Exchange Online) had two new units added to it – Explore information barriers in Microsoft 365 and Define information barrier policies.
- Module 6, Lesson 3 (Explore sensitivity labels). The old lesson was Implementing Azure Information Protection. We replaced all this AIP content with new sensitivity label content and renamed the lesson Explore sensitivity labels. All units in this Lesson are new.

- Module 6, Lesson 4 (Implement sensitivity labels). The old Lesson was Implementing Advanced features of AIP. We replaced all this AIP content with new sensitivity label content and renamed the Lesson Implement sensitivity labels. All units in this Lesson are new.
- Module 6, Lesson 6 (Implement Windows Information Protection). We deleted the unit titled Implementing WIP.
- Module 7, Lesson 1 (Search for content in the Microsoft 365 Compliance center). We added two new units – View the search results and statistics, and Export the search results and search report. We also deleted the unit titled Conduct a data subject request.
- Module 8, Lesson 4 (Examine the Microsoft Store for Business). We added a new unit (Add apps to your private store).
- Module 9, Lesson 2 (Explore Windows Autopilot deployment models). We added a new unit titled Plan the settings for Windows Autopilot profiles. We also deleted two units – Create and assign a Windows Autopilot profile, and Deploy and validate Windows Autopilot. The unit titled “Autopilot White Glove deployment” was renamed to “Examine the Windows Autopilot pre-provisioned deployment model.”
- Module 9, Lesson 4 (Resolve Windows 10 upgrade errors). We rearranged topics 4, 5, and 6. 4 moved to 5, 5 moved to 6, and 6 moved to 4.
- Module 10, Lesson 1 (Explore Mobile Device Management), topic 3 (Explore the MDM services in Microsoft 365) was updated.

SLIDES

- Updated all slides to map to content changes.

LABS

- All labs were reviewed and re-tested step-by-step. Lab instructions were updated to reflect product UI changes since the prior release.

Because the old module 5 was deleted, the module number in the lab file names were renumbered accordingly.

Important: See the note in the Trainer Prep Guide for Lab 6 – Implement Sensitivity Labels. This has an import note regarding scheduling of this lab. In short, there are 4 tasks in this lab; the students can complete tasks 1 and 2, but then they must wait 24 hours to complete tasks 3 and 4. **See the Trainer Prep Guide for a complete explanation.**

November 2020 Revision

Update: **MINOR**

Type of change: **GENERAL/CONTENT/SLIDES/LABS**

GENERAL

- Product branding changes were updated throughout the course. The course was reviewed for references to products that have undergone branding changes. While previous revisions updated branding changes such as Office 365 to Microsoft 365 and Office 365 Pro Plus to Microsoft 365 Apps for enterprise, some references were missed and were updated in this revision.

Additional new branding changes were implemented. For example, System Center Configuration Manager, which has been moved out of the System Center family and is now part of Microsoft Endpoint Manager, is now referred to simply as Configuration Manager.

In addition, 12 graphics were updated to reflect branding changes as well.

CONTENT

- With the move of Config Manager from System Center to Endpoint Manager, all content in Module 9 affected by this was updated to reflect the change. Also in Mod 9, the Configuring Microsoft Store for Business topic (student manual and slide 25) was updated to reflect the fact that connectors are available from Exchange and Microsoft Store for Business to Intune and Config Manager.
- Module 10, lesson 5 was renamed from Introduction to Windows Analytics to Introduction the Desktop Analytics to reflect product change. Replaced screen shot, fixed references, and updated both slides and student manual content.
- Because Device Management has moved from the old Azure portal to Endpoint Manager, all MDM content in Module 11 has been updated to reflect this change.

SLIDES

- Updated all slides to map to content changes.

LABS

- All labs were reviewed and re-tested step-by-step. Lab instructions were updated to reflect product UI changes since the prior release. One specific callout is in Lab 10 in Module 11. Because

Device Management has moved from the old Azure portal to Endpoint Manager, all lab steps were updated to reflect this change.

- In Module 7, Lab 7, Exercise 1, the lab was changed from implementing AIP labels to implementing sensitivity labels with an AIP Unified Label client.

August 2020 Revision

Update: **MINOR**

Type of change: **SLIDES**

SLIDES

- Microsoft World-Wide Learning is in the process of converting all course PowerPoint slides to a new template. The only change in this release was to the PPT slides, which were converted to the new template. There was no change to the content of the slides; they have simply been updated to reflect the new template design.

May 2020 Revision

Update: **MAJOR**

Type of change: **GENERAL/CONTENT/SLIDES/LABS**

GENERAL

- We added approximately 25 new graphics to the course (student manual and slides).

CONTENT

- In module 1, we added a new lesson 2 on The Zero Trust Model and a new lesson 5 on Privileged Identity Management.
- In module 1, we also added a new lab exercise on Privileged Identity Management.
- In module 1, we updated all the content in lesson 4 (Introduction to Microsoft Secure Score) to reflect the changes made to this functionality since the prior course release. All the topics in the lesson were updated since this was a significant product update.

- In the module 1 lab exercise on initializing your M365 tenant, we moved task 7 into this exercise from lab 8 due to propagation time requirements. By moving this task to lab 1, the newly assigned permissions will have time to fully propagate by the time the students get to lab 8.
- In module 3, lesson 1, we added three new topics on Threat Attackers, Attack Simulator, and Automated investigation and response. We then added a new lab to this module (Lab 3, Exercises 1 and 2) that focused on the Attack Simulator. Exercise 1 was about creating a spear phishing attack using the Attack Simulator, and Exercise 2 was about conducting password attacks using the Attack Simulator.

Note: Please read the note in the Trainer Prep Guide regarding the Attack Simulator lab, especially the part concerning Microsoft Secure Score propagation once the tenant is provisioned.

- In module 6, we added two new lessons – lessons 1 (Evaluating your Compliance Readiness) and lesson 2 (Implementing Compliance Center Solutions).
- In module 8, lesson 3, topic Audit Log Search Overview, we removed the section on OMS, which has been deprecated. The OMS portal has been moved to Azure.
- In module 8, we updated all the content in lesson 4 (Managing Advanced eDiscovery) to reflect the changes made to this functionality since the prior course release. All the topics in the lesson were updated since this was a significant product update.
- At the end of each module, we added a discussion question slide that has 2 questions: 1) What are your key takeaways from this module, and why? and 2) What are the key features discussed in this module that you foresee implementing at your organization?

These discussion questions were included to get the students more actively involved in the course, and specifically to think about the content from each module and discuss what they learned and whether they can implement it.

- We updated any product features that changed since the last release of the courseware.

SLIDES

- Updated all slides to map to content changes.

LABS

- In the prior release, each lab was presented as a separate module. In this release, we moved the labs into their respective modules as module lessons. This reduced the number of modules down to 8, plus this format is consistent with MOC standards.
- In the lab instruction, we performed a complete review and test of every lab task to ensure that the lab steps were current with the product UI at the time of course release.