Microsoft 365 Administration: Deploying and Managing an M365 Tenant

by Brian Alderman

This course will teach you how to create, configure, manage, and monitor a Microsoft 365 tenant, as well as discover several ways to manage access to M365, or specific workloads in M365, by using user accounts, groups, M365 roles, and licenses.

Course Overview

Course Overview

Hello, everyone, my name is Brian Alderman, and welcome to my course, Deploying and Managing a Microsoft 365 Tenant. A little bit about me, I'm a former MVP, MCT, and PMP, and have over 30 years of training. I've been an international speaker at over 150 conferences so far, author of four Microsoft technology books, and the CEO at my company called MicroTechPoint. Now, Microsoft 365 currently has over 345 million paid subscribers, so it's a popular, evergreen platform that requires careful planning for its deployment, as well as ongoing configurations and security measures. So in this course, we're going to introduce and discuss in the deployment of an M365 tenant, as well as explore important post-deployment configurations, and we're going to discover several ways for us to control access to your Microsoft 365 tenant. By the end of the course, you'll know what needs to be carefully considered when deploying Microsoft 365, understanding the steps necessary to deploy M365, and understand the best ways to control access to your Microsoft 365 tenant. Before beginning this course, you should be familiar with your organization's planning policies and have a general understanding of cloud-based software. Well, I hope you'll join me on this journey to learn about Microsoft 365 with the Deploying and Managing a Microsoft 365 Tenant course, here, at Pluralsight.

Implementing and Managing an M365 Tenant

Course Introduction

Hello, and welcome to Pluralsight's course on Microsoft 365 Administration, specifically, we're going to be focusing on deploying and managing an M365 tenant. We're going to begin with a discussion on the implementation and management of a Microsoft 365 tenant. However, before we do that, I want to make sure that we have an understanding of what we're going to cover throughout the entire course. In this very first module, we're going to talk about implementing and managing a Microsoft 365 tenant. We're then going to talk about managing users and groups within Microsoft 365, and in the third portion or module of this course, we're going to look at managing roles in Microsoft 365 by populating users within these roles or assigning roles to the users so they have the specific tasks associated with their accounts. So in this very first module, there are four primary concepts that we're going to be discussing. A thorough understanding of what a Microsoft 365 tenant is all about. I want to make sure you understand what you're getting into when you spin up a new tenant and what some of the thought processes are and planning requirements are for that tenant. We're then going to walk through the steps necessary to create your new Microsoft 365 tenant, we're then going to look at some post-tenant creation configuration options available to you, and then we're going to wrap up this module by talking about some items associated with managing and monitoring service health within Microsoft 365. Now, you may be wondering, wait a minute, what happened to Office 365? What is Microsoft 365 versus Office 365? Well, Office 365 really was just the apps, it was the services, it was like Word, Excel, PowerPoint, SharePoint, but it didn't include things like Windows Enterprise, which is included in Microsoft 365. It does include your Microsoft 365 apps, or those Office 365 apps I just mentioned, and in addition to that, it provides us functionality regarding mobile and security. Now, Microsoft 365 is a SaaS, it's a Software as a Service, which means we can access all of our services via the cloud. This could be SharePoint Online, OneDrive, Microsoft Teams, Exchange Online, as well as items or functions and features available within Power Platform. It's essential for us to do the proper planning for Microsoft 365, and I've really broken it down into two different categories; the Microsoft 365 tenant planning process, where you plan and

document the tenant name, deployment options, management options, as well as any security considerations associated with the tenant creation. The second part of that is after we've spun up our tenant is the data migration planning. This includes Active Directory users and groups, the users' mailboxes and PST files, and any data they may have in the cloud or on-prem that they want to move into Microsoft 365. When we're going through the consideration process for Microsoft 365, there's really five areas that I want you to think about, five considerations. First is what M365 subscription plan are we going to use? What does our organization need? We want to make sure we don't spend too much money, but we want to make sure we have all the features and functionality we need and our users are able to perform the tasks they need to perform. We also need to take into consideration the tenant options, and we'll be talking about these as we go through the creation and configuration of the tenant. We're going to determine which Windows Enterprise operating system that we want to deploy. We're going to take into consideration the types of mobile devices that are being used to access Microsoft 365, and, of course, we're going to be concerned about security, so we're going to be looking at security requirements as we're deploying Microsoft 365. When going through this planning process of Microsoft 365, it's not a me thing, it's a we thing. You should identify the deployment team members, document all of the decisions made by the team, get signatures from all the stakeholders as the decisions are being made and finalized, periodically update the documentation as changes occur through the deployment process, and periodically update the progress to your stakeholders so your stakeholders are aware of the progress of your deployment. Now when we're looking at deployment, one of the first questions, as I already mentioned, what subscription are we going to use? We have a Microsoft 365 Business subscription, a few different flavors in there. We also have a Microsoft 365 E3, E for Enterprise, Microsoft 365 E5, which is more advanced, and you have your Microsoft 365 F1 or F3 for your frontline workers. These are some of the options that we want to consider. We want to look at the features and functionality that is provided in each of these subscription plans to see what is going to meet our needs.

Creating a Microsoft 365 Tenant

All right, in our next section of this module, we're going to go through the steps necessary to create a brand new Microsoft 365 tenant. It's going to be asking us for some information, for instance, the country where the business headquarters reside. So if you have an international organization, wherever the headquarters are for your organization is the country you want to choose here. This is something that cannot be changed after you've created the tenant. Something else that can't be changed is the tenant name, so make sure that you have agreed on what the tenant name should be. It's also going to ask for some additional information, contact information like an email address and a phone number. And it's going to ask you to create a global administrator account, it's going to create it for you when it creates the tenant. And it's going to ask about payment information, so you'll have to supply a credit card. And lastly, your company domain name, and you're going to see it's going to come up with a funky suffix on the original tenant deployment and most likely we're going to want to change that. So let's step out and take a look at the options that we have and the steps necessary to create a new Microsoft 365 tenant. As you're about to see is there are a plethora of options for creating a Microsoft 365 tenant, or an Office 365 tenant, or a Business tenant, or Home. So let's do this, let's do Microsoft 365 plans, click on that. Compare all the plans, so let's go ahead and click on that, and it's going to bring up a screen, and I'm going to scroll down here, and you're going to see we have for home. We have the Family option and the Personal option. Click on For business. I mentioned there's a few different flavors there, so you'll want to look at these to see what it is that you need to see if one of these meets your needs without going to the Enterprise level. You have Basic, the Standard, the Premium, and then you have just the apps. If you scroll down, you'll see all the different services that are provided for each of these Business plans. If you scroll all the way to the bottom, you can expand and get more detail on what is happening with these different Business plans. The main reason I'm going to the bottom is because I want to find the Enterprise plans. So I want to go ahead and click on Compare enterprise plans, and when we come in here, notice we've got five varieties of Enterprise plans. We have the Microsoft 365 E3, E5, and F3, we have the Office 365, remember, there's not much difference between Office 365 and Microsoft 365, you get the operating system, and you get some advanced security options. If I show you the Office

365 options, we have the apps for Enterprise E1, E3, and E5. If I go to Frontline, we have the F1 and the F3 for the Frontline. And then under Government, we have Office 365 and Microsoft 365 options, G3 G5, for each of those. And then under Nonprofit, depending on your organization, you may want to peek at this one, you can come in here and take a look at this, and you'll see you have Business Standard for nonprofit and the Business Premium for nonprofit. So this is what I was talking about earlier is you have to have a conversation and find out based on your business needs, which one of these plans is going to be sufficient and provide you the functionality that your users need. Now, I'm going to go back to Microsoft 365 for a moment, and I'm going to scroll down here, and notice, in order to create a plan here, we have to contact sales. So what we're going to do is, because I don't need the operating system, and the functionality is pretty much the same in Office 365, and more importantly, what we can do in here is come in and create a trial version, try for free for any one of these options. The steps are exactly the same whether you create an Office 365 subscription or a Microsoft 365 subscription. So, I'm going to go ahead and just to show you a little bit of a comparison between E3 and E5. So, E3 has everything in E1, and you can install Microsoft 365 apps on up to five PCs, message encryption, rights management, and DLP, data loss prevention. If we go to E5, we get everything in E3, as well as advanced security and compliance capabilities, call control and PBX capabilities in the cloud, scalable business analytics with Power BI. Well, what we're going to be doing throughout this entire course and these courses for this exam prep is really most everything is going to be available to us for demo purposes through the Office 365 E3. If I scroll down and show all the icons, you can see everything that we're getting in this column here is the E3, this column is E5. So I'm going to create, and I'm going to ask you to create a try for free E3 subscription.

Demo: Creating a Microsoft 365 Tenant

If you need to pause me so you can follow along and take these steps to create it, please feel free to do so. First thing it's going to ask me, what is an email address I can reach you at? Now, I already have my own company email, and that's brian@microtechpoint.com, and if I click on this and hit

Enter, it's like, well, looks like you're already using brian@microtechpoint with another Microsoft service. Do you really want to sign in with this account or create a new one? I'm going to create a new account instead. So it's going to ask me for this information here. You'll see the asterisks are required fields, middle name is not required, first name and last name is required. Business phone number, I'm going to use my company phone number. Company name, I'm going to use MTP instead of MicroTechPoint, I don't want to do anything to affect my subscription I already have for my MicroTechPoint company, and then it's just getting information about company size, it's really just me, but I'm going to say it's 5-9 people. Remember I mentioned country, this is extremely important. If you have an international organization, you're going to locate your headquarters, locate the country from this drop-down, and choose that country. Now, if I scroll down a little bit more here, what is Office 365 E3? Tells you what it's all about. Tells you have 30 days, you have 25 users that you can use during this trial period. Okay, let's move on, I'm going to go ahead and click Next here. It's going to verify I'm a real person, so I've got to put in my cell phone number here, and it's going to send me a verification code. I can choose text or call me. I'm going to have it just text me, and I'm reaching for my phone now, and here's the code, so let me type that in, 268853, and then quick Verify, and now we're ready to create the tenant and provide the information about the tenant. So, I'm going to create a user called Brian, I don't want to type in my entire name. It grabs us some weird tenant name, I believe I already have MTP out there, so I put 988 on the end of it. I'm going to create a tenant name, MS102, and notice it's going to create a tenant name called ms102.onmicrosoft.com. So let me save this, see if it's going to let me use MS102. Not available. Okay, so let me do MS102Exam, let me try that one. That should be working, okay, so I'm going to put a password on here, one I won't forget. I'm going to use one from my MCT training days. All right, so I'm going to create a brian@ms102exam.onmicrosoft.com, that's going to be my tenant name, with this account now becoming the one and only account within the tenant, and it's going to be a global admin. So I'm going to go ahead and click Next, and now I need to provide payment information. It used to be up until 6-7 months ago I didn't need to provide a credit card at this point in time. Microsoft has changed that, sadly, so now I need to provide a payment method. So, I'm going to go ahead and click on that,

and I'm going to share my credit card with you. No, I'm not, of course not. So I supplied all my credit card information, and you can see now I can start using my E3 trial by clicking on Start now. Again, I'll click on Start using Office 365 E3 Trial, and you can see we have created an E3 trial tenant, and it has some cards down here indicating what we should do next, install Office, add domain, add users, and then connect to domain, and we'll come back and work with some of these in the latter part of the module.

Post-tenant Creation Configuration

All right, coolness, we just completed the steps necessary to create a brand new E3 tenant, we're now going to go in in this section of the module and take a look at some of the post-tenant creation configuration options, and one of the big ones is getting rid of that .onmicrosoft.com option. So we need to implement our company domain name, and we do this a couple different ways. The first is using the steps as we're going to go through right now. Through the M365 admin center, go to Settings and go into Domains in there, and we'll see where this is located in just a few minutes here. We're going to choose the option to add a domain. We're going to then enter our company domain name. Remember, we created an ms102exam.onmicrosoft.com. Our users aren't going to want to type that in all the time, so let's go back to my company, MicroTechPoint. My users aren't going to want to type in microtechpoint.onmicrosoft.com, so I need to add my company domain so they can just log in using brian@microtechpoint.com. So we're going to add our company domain name. To do so, we need to verify we have the ownership of that domain. We also need to talk to our DNS registrar to make sure that DNS records are pointing to the new domain name. Now, alternatively, instead of going through these five steps, there's a Domain Connect wizard that's available to us that will allow you to perform or complete the same tasks by following these five steps above. Now these are the registrars that are partnered with Microsoft to work with the Microsoft 365 tenants. As you can see, there's a couple popular ones there: GoDaddy, WordPress.com, Plesk, MediaTemple. So any of these registrars could be used for pointing your domain name to your Microsoft 365 tenant.

Some other considerations after we've created our tenant, a big one, as always, is security. We want to make decisions on enforcing Azure multi-factor authentication registration for all of our users. We want to maybe just, instead of all of our users, maybe force admins to use MFA, or multi-factor authentication. We may want to look at blocking our legacy authentication protocols. These include POP and SMTP, IMAP, and MAPI. We could also require our users to use multi-factor authentication without enforcing it through Azure. And last, we want to look at making sure that we're protecting the privilege access. And, we can perform all of these unless we're using custom conditional access policies. So, if you've already deployed conditional access policies, we won't be able to use these controls for our M365 security implementation. In addition to the security settings, we're also going to want to go into the M365 admin center, back into the Settings category, and go into our Org Settings. In there, you're going to see three different tabs, you're going to see Services, Security & privacy, and Organization profile. We'll want to make sure we'll make all the appropriate changes to these areas to reflect our organization's name within Microsoft 365.

Demo: Post-tenant Creation Configuration

So let's step out to our brand new tenant and take a look at some of these post-tenant creation steps, such as managing your domains, configuring your organization-specific settings like the services, security & privacy, as well as the organization profile. We are back in the admin center on our new tenant. You'll see the four tiles here. In fact, let's go take a peek at this real quick, Go to guided setup. if we click on that, it kind of walks you through the finishing of the setup. So, like here, for instance, install the Microsoft 365 apps. If you click on that, it's going to download the Office setup, you can double-click on that and then install that. I already have them installed so I'm not going to do that, but that's how you can get the apps kicked off so that they're installed. Then you'll click Continue, and as we've gone through the steps already, you can add a domain here if you want to use this domain, and then we're going to say no, we're going to keep the MS102Exam.onmicrosoft.com for now, we're going to use this domain, and then you would go in and

start adding users. We're going to do that in the next module, so I'm not going to get into that here, but notice with the E3, we have 25 licenses, we've consumed one when I created the account, my Brian account, which is the global admin, but you can go in and add users and then you can connect to the domain. So that's something you might want to think about after you've created your new tenant. So I'm going to go back to the home page again just to make sure it's fresh here, there we go. Now, over in the left side, if you don't see all of these, there's an option to show all or show more, so we're back at home, and I mentioned we're going to go to the Settings option here, so I'm going to expand on that, and we're going to go into Domains. Here's the domain that we created when we spun up the tenant. If we wanted to add, and get rid of that .onmicrosoft.com, I'll go as far as I can with this, let's say we wanted to add MS102Exam.com. In addition to what we're talking about, there's a video that walks you through this as well. So I'm going to say use this domain. We're trying to get rid of that .onmicrosoft.com so users don't have to use that when they're logging in. To do this, we need to add a TXT record to the domain's DNS records. Or, if you can't add a TXT record, you can add an MX record to the domain's DNS records, depending on your DNS registrar. Or, you can add a text file to the domain's website. Let's go with the default, add a TXT record to the domain's DNS records, and we'll hit Continue. Remember, one of the steps was to verify ownership, this is probably where I'm going to have to stop because I don't own this domain, MS102Exam, but it's given me the information necessary, step-by-step instructions, to be able to complete the verification process and set up our MS102Exam.com domain. If I added these TXT record values, then I would click Verify, and our new domain would be added, but that's how we would go in and add our domain if we wanted to add our domain to minimize the need for our users to log in using the .onmicrosoft.com. Okay, back Home, back to Settings, we talked about Org settings, let's go ahead and click on that. We had three options here: Services, Security & privacy, and Organization profile. For instance, we can go in under, let's say we want to go in under Microsoft Forms. We'll click on Forms, we can configure some tenant-level external sharing options. Sending a link to the form and collect responses, share to collaborate on the form and layout, share the form as a template; all of these can be configured specifically for forms. So notice we have several different options here. We

have Microsoft 365 on the web, Mail, Microsoft 365 Groups, Graph, Planner, Teams, Microsoft Teams, let's click on that real quick. That's pretty popular nowadays. Turn on Microsoft Teams for all users, and we can also manage guest access in here. So this is where we can do some tenant-level settings for the different services that we have. Now if we go to Security & privacy, you'll notice in here we've got some options. Idle session timeout, if we click on that, right now a session can remain connected to Microsoft 365 for as long as they want, we can set it up so it times out after 90 minutes just by setting up an idle session timeout option for our tenant. Password expiration policy, by default set password should never expire, so if we want to change that, when we're working with some R&D environment or in an intellectual property environment and we want the passwords to be changed every 60-90 days, we can enforce that here as well. Self-service password reset, we can configure it so that our users can reset their passwords themselves without going through the help desk. And Sharing is another one that we have available to us to let users add new guests to the organizations on by default. This is a brand new tenant, so we're seeing our default settings. So this is somewhere you'll want to come in and peruse through and check all these options that you have available to you under Services, Security & privacy, and the Organization profile. In here, we can come in and look at items like Custom tiles for Apps, we can come up and add a custom tile if we have some third-party software we want to add. We have Custom themes. Keyboard shortcuts. We can set up the help desk information here, so we can add our help desk contact information after spinning up our new tenant. Send email notifications from your domain instead of from Microsoft. Release preferences is a big one. Standard release for everyone, which means you don't see anything until it's been general availability is what they call it, GA, that's the default setting. Targeted release for everyone, that's where we get releases of features and functionality that's not fully baked yet or fully tested yet, but we can get some updates earlier sooner than later. And then targeted release, if you have a group of super users, we can actually specify we want to receive the updates early, but only these users can receive those updates. So you'll want to take some time and cruise through these three categories of settings to make sure they're configured for your organization.

Managing and Monitoring Service Health

The next piece of this model is managing and monitoring service health. We've deployed Microsoft 365, we've gone in and modified some of the configuration settings associated with Microsoft 365, the next thing we need to be aware of and doing quite often is monitoring it. So, what we're going to look at here is the different options that we have available to us within Microsoft 365. We have an option to view the current health status of all of the different services. We can also view the history of the services, maybe you went on vacation for a week and you came back, you want to see what happened while you were away, you can look at what are called advisories and incidents. Incidents are much more critical, either the service is not available or a major portion or functionality of that service is not available. And advisory is more or less, yeah, we're having some issues, a few users with a unique situation are having issues with that service. So there's a couple different categories of health status when you're looking at the history of the health. The history view allows you to look at information in 7-day view, a 30-day view, and every incident that's in there, or advisory, you can click on it and get some additional details, so you're going to get a better understanding of what it was all about, if it affected you, if it's in the past, or if it's going to affect you if it's something that's current. And it's easier for us to access this, we go into the Microsoft 365 admin center, we choose the Health->Service health or click on the Service Health card on the home page. There's a couple different ways you can end up on the same page. You select the tab for the information that you want to view, and there's going to be an overview option, issue history, and reported issues, so there's three different categories of service health that you can look at. You can also click on any of these issues and get much more detail about the issue. When dealing with health service, we need to understand the different terminology. Investigating means they're aware of the issue and they're gathering more information. Service degradation, confirmed issue, slower performance for that service than usual. Service interruption affects user access to the service. And restoring service means they're taking the action necessary to get the service up and running at full capacity. Extended recovery, taking corrective action, but lengthy process to do so. Investigation suspended,

they began the investigation, but they had to suspend it because they need some additional information in order to take the corrective action. Service is restored, we're back hunky dory, everything's working well, the service is back up and healthy. False positives determined service is healthy and no impact to service was ever observed. Now someone may have reported it and they did some research on it, and they never discovered anything wrong with the service. Post-incident report published, usually they'll write up what happened after an incident occurs so you have an idea of what was it about and what caused it, and what actions were taken by Microsoft to correct it. Now, in order for us to be able to view these reports and get this information, we have to be in one of these roles, obviously the Global admins, they have full-party rights, they can get into anything they want at any part of your tenant. Also your Exchange admins, your SharePoint admins, your Skype for Business admins. There's a role called the Global reader. We also have a role called the Usage summary reports reader. We have the Reports reader, it's not the summary information, it's more detailed information. Teams admins, Teams communication admin, and User experience success manager. All of these individuals in any of these roles can access these reports. Now, one of the things we're going to focus on as a Microsoft 365 admin is the adoption score. This adoption score is gathered by the total of people experiences and technology experience scores, which are comprised of several categories of data. Those categories are broken into two sections: people experiences, and within there we have communication, we have meetings, we have content collaboration, we have teamwork, and we have mobility. The other category is technology experiences. Within here, we have endpoint analytics, network connectivity, and then your Microsoft 365 apps health. The best possible score you could get is an 800, so that's when everything is running perfectly, all 8 categories are firing on all cylinders, we'll have an adoption score of 800.

Demo: Exploring Microsoft 365 Service Health

Let's take a minute to step out to our tenant and explore the Microsoft 365 service health. We're going to look at the overview category, the issue history, and reported issues. We'll also look at

exploring usage reports by product and where to find our adoption score. We are back on our tenant landing page, and on the left-hand side, notice we have an option for Health and an option for Reports. Let's jump to Reports first. Here's where the adoption score would be found. This is a brand new tenant so there's not going to be any information. Remember, we have 8 categories, with a highest score of 800, there's 100 per category. So this is where we would come in and be a breakdown of the different categories and how are their rankings based on the total of 100 per category? This is also under Reporting where we'd find Usage, and we can go by product, again, it's a new tenant, so we don't have anything going on yet. This tenants only about 6-7 hours old. So we have Exchange, and Forms, and Teams, and OneDrive, and SharePoint; this is where I can come in take a look at usage for the different services and apps. And, we have reports that are available by 7-day windows, 30-day windows, 90-day windows, and 180-day windows. So this is where we'd find information about product usage, as well as the adoption score. So let's go back to Home, and we'll go collapse Reports and go down to Health now. If you come in on the dashboard, you're going to see it has some of the services shown here; OneDrive is healthy, SharePoint, Microsoft Teams, Yammer, all healthy. Ooh, Exchange Online, two advisories. What's going on with that? We click on that, and one advisory is users may intermittently be unable to reply all to email messages using a group mailbox in Outlook on the web. The other one is some users' email with attachment sent from Outlook for Mac may be delivered without the attachments. So a couple advisories that are going on, nothing that's a show stopper, but some issues that a few people are encountering. So we'll close that out. Notice we're on dashboard on the left, I'm going to click on View all in service health. It's going to drop me down to Service health, which is another page. Here's where we had those three options. We had the Overview, Issue history, and Reported issues. So I can come in here and on Overview, Active issues Microsoft is working on. We saw that where there's three advisories here, Admins may see incomplete usage report for SharePoint online and OneDrive for Business. And here's my two other ones about Exchange. Server status, Exchange Online's got two advisories, SharePoint Online has one, and everything else is getting a green checkmark, so everything else is healthy. But, this is a good place to start your morning when you grab your first cup of coffee, and

just kind of jump in here to see what's going on. Issue history, if we click on that option, we can go back and look at some history. Notice over here we can change the view, we can filter based on product or service. We can come up here, 7 days or 30 days. We could do a search for a specific topic that we're trying to locate regarding an issue in the history. We can customize the interface. If I click on Customize, let's say, for instance, I scroll down here, I don't do anything with Planner, or I don't do anything for Project for the web. I can filter those out so those won't be displayed on my screen. So I'll go ahead and save that out. It gives me a little bit less information to have to filter through when I land on this page. But as you can see here, if I come in here, some users were receiving large amounts of spam messages for Exchange. If I scroll over on that one, you'll see the service has been restored. If I scroll back and I click on that, you're going to see we've got a plethora of information about this; the date, the affected services, it was an incident versus an advisory, the user impact was listed here, all the updates as to the resolution of it are all stored in here as well. So it provides you a lot of information about the issues, even at a later date, so if you want to do some research on that, you're certainly able to do so. Let me go back to Service health here. And the last one is the Reported issues, but if there's any issues here that we wanted to report, we could come in here and report an issue to Microsoft. And, first option, Is this causing a significant impact to your business? We can say No. Where is the issue occurring? Ah, we'lll pick on SharePoint Online. How would you categorize this issue? Users can't connect or sign in, sites or content are slow to load, issues viewing, editing, or saving content. We'll just pick the middle one there, and we can enter a brief description, and then we would click Submit. I'm not going to submit this to Microsoft because it's not a real issue. So I'll go ahead and just close this out, but this is where I can go in and report an issue to Microsoft, as well as track the issues that I've reported from this interface here. So this is where you'll find information on health and on your adoption score in usage by clicking on the Reports option. Well, in this module, we covered a lot of territory. We began with an introduction and an understanding of a Microsoft 365 tenant. Then we stepped out and created a brand new trial E3 tenant, so we walked through all the steps necessary to complete that task. Then afterwards, we went and discussed and configured some of the post-tenant settings that we want to be familiar with

and to customize the tenant for our particular organization. And we wrapped it up by looking at ways we can manage and monitor the health of our tenant. Up next, we're going to take a look at managing users and groups that are going to be able to access our tenant.

Managing Users and Groups

Managing Users and Groups

In our next module of Deploying and Managing an M365 Tenant, we're going to be focusing on managing users and groups. With that said, we're going to be discussing four primary topics. We're going to talk about creating and managing contacts, as well as users. We're going to talk about managing users in bulk within Microsoft 365. We're going to introduce and discuss Microsoft 365 groups. And, we're going to talk about how we manage and monitor the Microsoft 365 licenses to ensure our users have access to Microsoft 365 and can perform the tasks they need to perform. When we're looking at adding our users or contacts, we can add a contact for use within Outlook. We can do this through the Microsoft 365 admin center, or we can do this through the Exchange admin center. As we're talking about users versus a contact, we can add and manage Microsoft 365 users, as well as guest users - individuals external to the organization, we can add them, we can remove them, we can restore them from the recycle bin and we can perform this operation in bulk as well. So we can manage our users whether they be guest or Microsoft 365 in bulk, or individually, and we'll see that when we do a demo, shortly. Well, let's talk a little bit more about Microsoft 365 guests because depending on where you create that guest account will determine the type of access that they have. If we go into Teams, and within Teams, we can create an external access for an individual, which gives them access to the entire domain, or we can give someone individual access by granting them guest access. So we have a couple different options for within Teams. A Microsoft 365 Group guest user is going to be able to communicate using that Microsoft 365 Group email inbox. If we create an account within SharePoint Online or OneDrive, we can create them at the organizational level and apply some restrictions, or we can create them at an individual site level

within SharePoint Online or OneDrive. As I mentioned, we can create these accounts individually through the admin center, or using PowerShell, or we can create them in bulk. So let's expand a little bit on bulk user management in Microsoft 365. First, I want to look at how we're going to manage our users in bulk. We're going to become familiar with a CSV file. We're going to populate our users in a CSV file. We can import this CSV file from the Microsoft 365 admin center, or we can import it from PowerShell using the Import-Csv cmdlet. If we use the Microsoft 365 admin center, there is a sample CSV file that we can download and we can use that as a template to populate our users that we want to bulk import. If we're going to use PowerShell, we have a couple of different flavors. We have Azure AD PowerShell for Graph, and we have Azure AD Module for PowerShell, and I'll expand on both of those in just a few moments. Let's talk about this CSV file that's so important to bulk user management. We're going to create a .csv file, and the fields in there are going to be separated by a comma. The first row has to contain the exact titles that match what you would see in Azure AD, or enter ID. They will include username, which is the user principal name, including the @ sign, so their email address, if you will, the display name, first name and last name, if you wish, and then the last name. Those are the three titles, as an example, that we would have in the first row of a comma-delimited CSV file. Now, what is required? We have two values that are required: the username, which is that UPN, and the display name. You don't need any other information except for these two fields here. And we also have to think about adding users in bulk from multiple countries. If we're going to do so, we have to create a CSV file for each country in the organization, and then import them using the Microsoft 365 admin center. Now I mentioned we have a couple ways for us to be able to use PowerShell. This is the Azure AD PowerShell for Graph, which requires PowerShell 3.0 or later. We're going to first connect to Azure AD using this PowerShell cmdlet. At that point, we're going to use some AzureADUser cmdlets. We can use New, Get, Remove, even Set, when we're working with the AzureADUser cmdlets. We're also going to need to assign a password, so we'll use a Set-AzureADUserPassword to assign a password to the users as we create them. And if you want to populate these users into a group, we're going to use AzureADGroup cmdlet, this also has a New, Get, Remove, Set, as an example of the type of cmdlets that we would be using to

populate our users into these Azure AD groups. The other option we had is to use the Microsoft Azure AD module for Windows PowerShell. We'll now connect using the Connect-MsolService that will connect us to Microsoft 365. We'll have the MsolUser cmdlets: the New, the Get, the Remove, the Set, to manage our users. We'll have the Set-MsolUserPassword to assign a password to the users after we've created them. We'll have the New, Get, Remove, and Set for managing the groups within Microsoft 365, and we'll also have the New, Get, Remove, and Set for managing the group memberships within Microsoft 365. The cmdlets you need to be most familiar with when managing your users using PowerShell are Connect-MsolService, New-MsolUser, Get-MsolUser, Set-MsolUser, Set-MsolUserPassword, and Add-MsolGroupMember. This allows us to create the user, get information about the user, change properties about the user, set the password for the user, and ultimately, add the user to a group.

Demo: Managing Users in Microsoft 365

Let's go ahead and step out and take a look at how we manage our users. We're going to look at creating contacts from within Microsoft 365 admin center. Then we're going to look at managing the users in Microsoft 365 admin center, and we're going to do that by creating a Microsoft 365 user. We're going to look at how we would manage our users using bulk user management, and we're going to look at creating guest users from within Microsoft 365. We have returned to our landing page in our new tenant, and over on the left-hand side, you see we have an option called Users. We're going to expand on that, and in there you can see we have Active users, Contacts, Guest users, and Deleted users. Let's begin with contacts because that's where we began in the module, and when we come in here, I can go ahead and add a contact interactively here. So let me go ahead and add Don Alderman, and that'll be the display name it picks up. Required field is an email address, it'll be Don@ms102Exam.onmicrosoft.com, and I can choose to hide it from my organization's global address list because this is a contact versus a user. I can add some additional information about Don. If I click on that option to expand that, we can add company, office phone,

mobile phone, fax number, title, website, street address information, and location - country or region - which is very important when we're working with individuals who are international. And then there's also an option for a mail tip down here if you want to send them a little extra information. So I'm going to go ahead and click Add, and you can see now I can edit the details for Don or add another contact. So that's how easy it is for us to add a contact through the M365 admin center. Don't forget we can also do this through the Exchange admin center. Let's go to our active users now, you're going to see this is the one that we created when we spun up the tenant, so let's go ahead and add a user here, and we're going to type in Linda. This is a little bit more helpful with the email, so it says Linda@ms102Exam.onmicrosoft.com, so I don't have to type all that in. Automatically create a password, it's usually some very difficult password, so I normally just go in and create my own. And, we can also require this user to change their password when they first sign in. I strongly suggest you do that, so that way when they sign in using this password that you've defined for them, they are forced to change that password so you don't have any access to their account, you can't log into their account because you don't know what their new password is. So require this user to change their password I would leave turned on. Send password in email upon completion. If it's a password that you don't use very often, you can have it sent to you so you don't forget it, or you can come up with a fairly generic welcome password for all new users. I'll go ahead and click Next here, and now it's asking me about licensing. So as I'm creating a user, it'll allow me to assign a license to the user. Now, I'm not going to assign the licensing yet, so I'm going to click this over to create user without product license, and then I'm going to click Next here. I'm not going to assign roles yet because we haven't talked about that, so I'm going to go ahead and click Next again, and I'm going to finish adding this new user. So now we've added a user, haven't assigned a license and I haven't assigned this user, Linda, to any roles yet, we're going to do that later on in this module. So that's where we can come in and add a user. I can click on Linda's account and go to the vertical ellipses and click on More actions. Notice I can manage product licensing here, groups, edit the username, and delete the user. I'm going to go ahead and delete the user for a moment, I know I just created it, it's kind of goofy. It's been deleted, and then I'm going to come over to the Deleted

users, and you're going to see Linda's in here, and notice I can click on Linda, Export all deleted users, Restore the user, and Periodically refresh if I want to. I'm going to go ahead and restore the user back. By default, it's set to auto-generate the password, or we can go back and let me create the password. It's picking up the same password I just put in a few seconds ago, make this user change their password when they first sign in. I'm going to go ahead and restore this account with the same password I assigned and requiring Linda to change the password when she logs in. So that's how I can add a user and delete a user. Now, if we go back to my active users, you're going to see there's an option for adding multiple users. I'm going to click on that, and it gives me some rows to add information: first name, last name, username, first name, last name, username. So I can enter up to 249 users, and all users here are given temporary passwords. However, if I scroll down, let's say I want to upload 30, 40, 50 users. Here's the CSV file I've been mentioning, I can click on that and tell it I'd like to upload a CSV with user information. Now it shows some common errors to try to avoid. You can't upload more than 249 users per CSV file. Email addresses can't begin or end with a period. Alternate email address may only use letters, numbers, and the following special characters. So just take a peek at this before you start creating your CSV file and adding information into that CSV file. I mentioned we had a blank CSV file with the required headers, so let me go ahead and click on that and then open this file, and you're going to see when I come in here, there's username, first name, there's last name, and there's display name. Now, remember I said there were two required fields? They should have a little asterisk next to it. The username, or the user principal name, is required, and the display name is required. Those are the only two fields that we'd have to supply values in in order for me to be able to complete an upload of these accounts into Microsoft 365. So this is where I would grab that CSV file in the fields associated with this CSV file, and notice, like I said, they're already in there on that first line as required by the CSV bulk management upload process. So I'll go ahead and close that out, I'm not going to save anything here, and you can also download a CSV file that includes example user information. And, after you've downloaded and populated the information into that blank CSV file, this is where you would browse to that CSV file and upload those new accounts, which would be created for you automatically. There's a video

available to you that discusses how to add multiple users. If I had added users, the next thing would be licensing, and then I could be finishing out. But again, we're not going to do that because we haven't gone into the details about licensing yet. So I'm going to go ahead and cancel on this here, but I wanted to show you how to add a user, how to add a contact, how to delete a user, and restore that user, and how we can work with the CSV file for adding users in bulk. Now, if I go to guest users, I'm going to go ahead and add a guest user now. When you come in here, if I click Create user, it's as if I'm creating an organization user, but I want to invite an external user, someone that I want to be able to collaborate within your organization that's external. So I would come in here, give them a name, and then I will supply an email address, an external email address, and then, optionally, I can put in the first name and the last name, and if I scroll down, there's some other options here as well. Personal message, looking forward to collaborating with you on the new project. And if I scroll down a little bit more, I can assign a group, we haven't talked about them yet, but just remember once we get to discussing groups, which is our next topic, this is where I could come in, as I'm creating or inviting an external user or guest I can add them to a group and can also assign roles, which we'll be talking about shortly as well. If for some reason I want a box there to sign in, I can do that right here. I can specify what location they're in, I'll put them in American Samoa. And if I want to provide some information about them, the job title, department, company name, manager, I can do so. And I'll click Invite, and it's going to send an email to Brian@microtechpoint.com, inviting me to join and collaborate with other users in this organization. So, these are the steps necessary for adding a contact, guest users, creating a new user, deleting that user, and restoring that user, all done through the Microsoft 365 admin center.

Understanding Groups in Microsoft 365

Several times throughout this module so far, whether it being in a demo or some slides, we had mentioned the idea of using groups for managing access to our resources. So what I want to do now is provide you an understanding of the different types of groups that we have available in Microsoft

365 for use for managing access to your resources. The first type is called a Microsoft 365 group. This is used for collaboration between your users, both internal and external, and you can use this for working within SharePoint, Planner, even Teams. Our next option is a distribution list. This is a group that's used for sending email to a group of individuals. Our next option is mail-enabled security, granting access to resources like SharePoint and then getting notified via email about the actions associated with those resources. We also have security groups, granting access to resources like in SharePoint, we have dynamic distribution groups, which expedite the mass sending of email within your organization, and we have a shared mailbox, which is used when multiple users need access to the same mailbox. So these are the different types of groups that we have available to us when working within Microsoft 365. Let's take a look at this table here. We had the different types of groups we just talked about: the Microsoft 365 groups, distribution, security, mail-enabled, shared, dynamic distribution groups. When we're talking about integration, we look at mail-enabled versus dynamic membership in Azure AD or Entra ID. As you can see, the Microsoft 365 groups are compatible with both. Your distribution groups are only compatible with mail-enabled, it makes sense, it's a mail distribution group. Security groups are a security for resources, so they're not going to be compatible with mail-enabled, but will be compatible with dynamic membership in Azure AD. Mail-enabled security group, of course, that's going to be compatible with mail-enabled, and no, it's not going to be compatible with dynamic membership in AAD. And shared mailbox, yes for mail-enabled, no for dynamic membership in AAD. And your dynamic distribution group, yes with mail-enabled, no with dynamic membership in Azure AD. So just an idea of how these are integrated as we're were working with the groups throughout Microsoft 365. One of the group types that we talked about was a Microsoft 365 group. When I create a Microsoft 365 group, there's a lot of action going on behind the scenes. We create a shared Outlook inbox for that Microsoft 365 group. They're going to have a shared calendar, they're going to have a SharePoint document library for collaboration. We're going to have a Planner created for this group, a OneNote notebook for this group, as well as Power BI associated with this Microsoft 365 group. So it's pretty extensive with what happens behind the scenes when you're creating a Microsoft 365 group. Each of our groups

has three group roles associated with it. Owners, which allows anyone as part of the owner's role to be able to add, remove members, rename the group, update the picture and description associated with that group. We also have members, which allows you to access all the content within the group, but you're unable to change any of the group settings as the owner can. And then we finally have guests, which are group members from outside your organization, and they're pretty limited to collaborating with others within the group. When you're thinking about creating groups, there's some considerations you need to be thinking about. The management of groups can be done by your global admins, your user admins, and your group admins. So a member of one of these roles has to be associated with the management of your groups. You should also create a naming policy for your groups, defined prefix and a suffix of your group. Here's an example, US_Holidays_HR, we're using Country_groupname (holidays), then _department for HR. That way if you have groups from around the world, you have a way to identify the region for these groups. You also have the option to set up an expiration policy for groups to expire after a set amount of time. So if you have a project that's going on for several months, and you know the project is supposed to end at the end of October, we'll say, you can have that group expire at the end of October. So, groups allow us to manage access to resources, as well as disseminate information to the members of the groups. Now, we've already looked at creating the different types of users, and now we've talked about adding these users to the different types of groups. The next thing we need to be aware of is the managing and monitoring of our licenses. We can add 100 users, but until they have a license, they can't do anything. So we have to make sure that we go in and assign a product license to our individual users. When I create them through the graphical user interface in Microsoft 365, one of the screens, as you saw in the demo previously in this module, was to assign a license. If you create a user using PowerShell, you have to use a separate command to assign a license to that individual. You can assign licenses based on group membership through Azure AD. You can assign product licenses to multiple users. If you use the graphical user interface, you can assign up to 20 users at a time. You can also use PowerShell to write a script to assign licenses to an unlimited number of users. There are three roles that allow us to manage licenses. We have a global admin, we have a license admin,

and we have the user admins. Anyone in any of these roles can manage those licenses. I always like to talk about PowerShell when we're talking about the different options available for us in managing Microsoft 365, so let's take a look at some of the popular license management PowerShell cmdlets. Get-MsolAccountSku, this is going to go out and retrieve the different SKUs that you have, the different subscription plans that you have in your organization. You can Get-MsolUserLicense to determine what license a user has. Set-MsolUserLicense to change that license for an individual user. Get-AzureADSubscribedSku, now we're getting information regarding the SKU associated with Azure AD. Set-AzureADUserLicense, assign an Azure AD license to a user. Get-MsolUser-All-UnlicensedUsersOnly. This goes out and returns a list of individuals, but do not have a license associated with that account. And as we saw previously, we can use a CSV file for bulk management of our users, and that does include assigning licenses to our users.

Demo: Managing Groups and Licensing in Microsoft 365

Back out to our tenant and take a look at a couple things here. We're going to explore management of groups in Microsoft 365, take a peek at a couple different types of groups, and assign some users to those groups, and then we're also going to take a look at managing and monitoring the Microsoft 365 licenses associated with our tenant. As always, we're going to start on the landing page of our tenant that we created earlier in this module. We're going to go to the left-hand side, we have an option called Teams & groups. If you expand on that, you've got Active teams & groups, Policies, Deleted groups, and Shared mailboxes. Remember, shared mailboxes was a type of group. If I click on the Active teams & groups, we're going to come in here, we're going to see that we have Teams & Microsoft 365 groups as our main tab, and we can add a team underneath that or add a Microsoft 365 group. Also notice it's added a couple different options, we have an All Company group and we have an MTP team that was created for us automagically when we spun up our tenant. So I'm going to go ahead and click on the Add a Microsoft 365 group, I'm going to call this the Holiday Prep Group, and we're going to prepare for upcoming holidays. We'll hit Next here, and now it's saying we

have to assign at least one owner, so I'm going to go ahead and click on Assign owners. There are two of us in here, so I'm going to assign myself to this one, add myself as an owner. I'm going to go ahead and click Next again. Now we can start adding members, we talked about the difference between these earlier. So I'm going to go in and add Brian, the external email address guest account that I created, I'm going to add Brian in here, and I'll click Next. And I'm going to create a group email address, remember, this gets its own mailbox, we're going to call this Holiday, and we're going to make this a public group. The other option, of course, is private, and create a team for this group. Go ahead and click Next. It's going to give me one more chance to see if everything is accurate, if so, click Create group. So, it went off in the background, created a OneNote notebook, the SharePoint site, all the cool stuff it was supposed to create for me. I'm going to go ahead and close on this, and you'll see we have our new Holiday Prep Group. Let's go over to distribution list. Here we also have the option of adding a distribution list, same type of deal, basics, owners, members, and settings. So the steps are pretty similar regardless of the type of group that you create. Here's our security groups. We can add a security group here. Notice this is a little bit slimmer as far as what's required of it, so I'm going to go ahead, and I'm going to call this SPO Resources, access to SPO, I'll click Next. Very minimal what I need to do here, I can change the type of group or I can go into the basics, which is the name and the description, and then go ahead and click Create group, and then I have the option of adding another security group. I'm going to go ahead and close this out, just want to give you a general idea on how that works. So we looked at security groups, we created a Microsoft 365 group, and we looked at the distribution list. Over here, we have the shared mailboxes that we talked about, and we can go in and add a shared mailbox. So we would identify the name on the mailbox, and then the email address, and we can use this as the to and from, this email address of the shared mailbox rather than using an individual mailbox. So that's where I would create the shared mailbox option. If I go to my Active teams & groups now, you're going to see that we have our All Company, which was created earlier, the one that we created, and MTP. Now remember I created an account for Linda earlier? I'm going to go to Active users, I'm going to go to Linda's account, and I'm going to manage groups, I'm going to assign a membership, and I'm going to put

her in the Holiday Prep Group, click Add (1), and now she's been added to that group. Now remember, I didn't add a license for Linda yet, so let's go take a look at licenses. So let's collapse Users, and let's go to Billing, and in here is your licenses, and under here we see that we have just the one subscription, the Office 365 E3 that we created. You'll see that we have 24 licenses available, one assigned license, so I can go in here and click on the Office 365 E3 and I can click on Assign licenses. Then I'll come in and I'll type in Linda, just a part of it, and then it'll find it, and then I'll click Assign, and I can add a personalized message that she'll receive in her inbox. I'm going to go ahead and just close out on that, but you'll see now we have 23 licenses available and that Linda has been assigned a license. So that's how we can manage the licenses and see who has licenses from within the Microsoft 365 tenant. So we've assigned a license to Linda and we added her to the new group that we created. Let me go back up to groups for a second, go to Active teams & groups, Holiday Prep Group, and click on the vertical ellipses, and here's where I can edit the name and description, edit the email address, delete the team, or export group members. So this is being handled as a Microsoft team instead of just a group. And if I click on All Company, you'll see that this is a group because it's showing it is a Delete group option, so this is a standard group, not a Microsoft 365 group. So that's how we monitor and manage our licenses and our groups, and how we can license a user and add that user to a group. Well, we went through several ways for us to provide access to our users to our new Microsoft 365 tenant. We began by discussing the creation and management of contacts, as well as the different types of users that we have that are able to access our tenant. We then went through the steps necessary for performing bulk user management in Microsoft 365, whether it be adding users, customizing users' properties, or even licensing our users. We introduced and discussed several different types of groups that are available in Microsoft 365, and we wrapped up by introducing the ways we have available to us for managing and monitoring the Microsoft 365 licenses. Next up, we're going to look at another way for managing access to the Microsoft 365 tenant by managing roles in Microsoft 365.

Managing Roles in Microsoft 365

Managing Roles in Microsoft 365

We are going to continue our discussion on deploying and managing a Microsoft 365 tenant by digging into the idea of using roles and how to manage roles in Microsoft 365, which is going to involve a discussion in three key areas. The first topic is going to be understanding and managing Microsoft 365 role types. We're then going to look at what are called administrative units, very powerful option for us to allocate permissions to manage portions of your organization, and then we'll introduce and provide an understanding on Privileged Identity Management, or PIM. So we'll begin by talking about administrator role introduction. In Microsoft 365 admin roles, there are about 30 of these babies. We can assign them to users, which are mapped to common business functions, and they provide pre-defined sets of permissions and tasks that can be performed that are associated with that role. We have also Azure AD admin roles, we have about 60 of those. These are also built-in roles, we can create custom roles, and these also provide pre-defined sets of permissions or tasks that can be completed if you are a part or a member of these roles. Role management can be done a couple of different ways - through admin centers or by using PowerShell. Now, when looking at administrative roles, there's a few considerations I want you to be thinking about as you roll out your Microsoft 365 tenant. First off, you should have two to four global admins. Right now, I'm the only global admin in my new tenant. If I get hit by a Guinness truck tonight, there's no one that can go in and manage the information or the tenant. So you want to have at least two, and maybe up to four if you're an international organization and you have different time zones that you need to be worrying about. While we're working with these roles, we want to make sure we assign the least permissive role. I don't want to give everyone global admin when I can go out and assign a role with less permissions and they're still able to perform the task they need to perform. We may want to require multi-factor authentication for our admins, specifically our global admins, and we'll want to take advantage of service administrators. These are individuals that can fully manage SharePoint, Exchange, Teams, and it lets them manage those specific products and services without giving them full-party rights to the entire tenant. There are six different categories associated with Microsoft 365

roles. We have collaboration, which is associated with OneDrive, and SharePoint, and Teams. We have devices, where we can actually assign a role to someone to manage the devices associated with our tenant. We have identity management for accessing the content and providing access to our tenant. We have security and compliance to make sure that we are adhering to everything that is required as far as the organization is concerned in both security and compliance, if we have any compliance requirements. Read-only, which means I can peek at information, but I can't make any changes. This is how we can provide someone the option to review information and provide us some feedback to those administrators who can make changes. And then there's the other category, which is everything that we didn't discuss in the first five categories. Most common Entra ID roles that we're going to be concerned with. Contributor. They get granted full access to manage all the resources, but they can't assign roles, manage assignments, or share image galleries. The owner, however, gets granted full access to manage all the resources, including assigning roles in Azure. The reader can view all resources, but cannot make any changes to the resources. The user access administrator allows you to manage user access to all your Azure resources. So these are four common Entra ID or Azure AD built-in roles that we can begin to work with. Let's expand a little bit more on Entra ID roles and some considerations that you'll want to be thinking about. First off, these permissions are based on RBAC, role-based access control. These roles grant permissions to complete tasks within the tenant or specific services within the tenant. A role group is a set of roles, in fact, there are some default role groups, which combines the tasks associated with several different out-of-the-box roles available to us. And the management of roles are done through the admin centers, which could be the Microsoft 365 admin center or the Microsoft 365 security admin center. And of course, we can use PowerShell for managing these roles as well. Some of the popular role management PowerShell cmdlets I want you to be familiar with. First one is Get-AzureADUser. If I want to see all the users that are in Azure, I can issue this command here. Get-MsolRole gets me all the roles available in Microsoft 365. Add-MsolRoleMember allows me to add a user to a role. Get-MsolRoleMember gives me all the users associated with the role. Get-AzureADMSRoleDefinition gives you information about the ADMS roles that are available to us,

which controls access to the Active Directory migration services. New-AzureADMSRoleAssignment allows you to create a new ADMS role assignment. Get-AzureADRoleAssignment allows you to look at all the roles that are being assigned through Azure AD. And, if we want to do this in bulk, we're going to create a CSV file and we're going to use the ever-so-popular Import-CSV command. Now, within the Purview governance portal, we have some specific roles in there. We have a collection administrator, which is a role for users that will need to assign roles to other users in purview or manage collections. Your collection admins can add users to roles on collections wherever they're an admin. We have data curators, a role that provides access to the data catalogs, manages the assets, configure custom classifications, create and manage glossary terms, and view data estate insights. Data readers are provided read-only access to your data assets, the classification rules, your collections, and your glossary terms. Data source administrator is a role that allows a user to manage your data sources and perform scans using existing scan rules. And we have insights reader, which is another role that provides read-only access to your insights reports for collections. We have the policy author, which is a role that allows the user to view, update, and delete Microsoft Purview policies through the Data Policy app within Purview. And we have the workflow administrator. This role allows a user to access the workflow authoring page, which is located in the Microsoft Purview governance portal.

Demo: Exploring Role Management in M365 and AAD

Let's take a moment to step out to our tenant and explore role management in Microsoft 365, as well as explore role management in Azure AD. We are going to look at a couple ways for managing roles for our users. So let's go to my Users, and Active users. We peeked at Linda's account earlier. I'm going to go ahead and click on that account, and I mentioned I could come back and assign a role to her later on, I can actually go right into her account and you'll see there's an option for managing roles. So I'm going to click on Manage roles. Notice, by default, all users have no admin center access. If I click over to Admin center access, it's got the most popular ones or suggested ones, the

Exchange Admin, Global Admin, Global Reader, Helpdesk, Server Support, SharePoint, Teams, and User Administrator. If I scroll down a little bit further, we have User Experience Success Manager, and then we can really blow this up by opening this baby, and now we have those categories we talked about. Collaboration. In here we have Exchange, Groups Administrator, Knowledge Administrator, Power Platform Administrator, Search, SharePoint, Teams, several different types of Teams Administrators. We have our devices. Cloud devices, Printers. Global Admin. Identity. Authentication Administrator, Domain Name Administrator, Helpdesk Administrator, License Administrator, Password Administrator, User Administrator. Then we have others. Billing Administrator, Edge Administrator, Service Support Administrator. Then we have a read-only. Global Reader, Reports Reader, Security Reader. So, all sorts of options, including Security & Compliance, where we have Compliance Administrator, Security Administrator, and Security Operator. So, as I mentioned, there's about 90 different roles that are available between Azure and Microsoft 365. Let's go ahead and make Linda a SharePoint administrator, and I'm going to save my changes, and I'll close this out, and I'm going to collapse this for a second. And then underneath here, we have Roles. So I'm going to go into Role assignments, and you'll see we have a similar interface, and if I click Show all roles, you know it's going to blow up and go and show us all of these different options again. I'm not going to scroll through all of them again, but notice also in here we have a category for Exchange, Helpdesk, Hygiene Management - get our teeth cleaned, Organization Management, Privacy Management, Records Management, Security. So some of the ones that we saw on the previous page, of course, and then we have just a few in billing. We have Billing account contributor, Billing account owner, and Billing account reader. So there's a couple of avenues for you to assign roles to a user within Microsoft 365. If we go over to the Azure AD environment, here's the Microsoft Entra admin center, if you will. Notice that we have Roles & admins over here as well. We'll go into Roles & admins. Here's all the roles. We have the Office 365 E3 tenant, so we don't have Microsoft Entra ID Premium 1 or Premium 2, but we don't need that unless we want to create a custom role. Remember I said we could create custom roles in addition to the built-in roles? Again, not scroll too fast, but these are pretty much what we saw over in Microsoft 365, numerous roles to choose from.

And notice, it's a checkbox, so I can go in and add someone as a SharePoint administrator, a Teams administrator, and an Exchange administrator if I want to, it's not one and done. So, two avenues for managing the roles for our users, through the Microsoft 365 admin center or through the Entra ID admin center.

Exploring M365 Administrative Units and PIM

In our next section of this module, I want to introduce and explore administrative units, as well as PIM, Privileged Identity Management. Let's begin with an introduction to admin units. With an admin unit, we can divide an organization into separate units. It could be regional, as an example. Within each of the units, we'll add users, groups, and devices, and then we'll assign an administrator to each of the units. So I can have a unit for the UK and a unit for the US and have separate license administrators associated with each of those units. The prerequisites for taking advantage of administrative units are Azure Active Directory Premium P1 or P2 for each of the unit administrators, so each of them has to have a P1 or P2 license to manage their respective units, Azure AD free licenses for admin unit members, privileged role administrator, and Microsoft.Graph module or the Azure AD module for PowerShell because we will be performing some tasks using PowerShell. There are about 10 administrative unit admin roles: Authentication, Groups, HelpDesk, License, Password, SharePoint, Teams, Printer, and User. Now I'm going to do a quick demo on this and I'll give you more of an explanation and expand on these when I get into that demo in just a few moments here. Some of the common PowerShell cmdlets we'll use for administering these administrative units include Get-AzureADMSAdministrativeUnit, New-AzureADMSAdministrativeUnit, Remove-AzureADMSAdministrativeUnit, New-AzureADMSRoleAssignment, and Get-AzureADMSRoleAssignment; and this goes back to the prerequisite for the PowerShell requirements that we talked about on the previous slide. Now, let's talk about PIM, Privileged Identity Management. This requires EMS E5 or AAD Premium P2. It provides just-in-time access to Azure AD, as well as Microsoft 365 resources. The beauty of these is we can assign time-bound access to

these resources using a start and an end date, so I can assign access to resources in Azure AD that begins on October 1st and ends on October 31st. That's the only time these resources can be accessed. We can also configure it to receive notifications when a privileged role has been activated, and we can enforce the use of MFA to activate a role. Let's introduce the three major PIM components. The first is Azure AD roles, second are the Azure resources or Microsoft 365 resources, and then we have PIM for groups, the groups that are associated with the Privileged Identity Management. We then assign users and groups to these components, and when doing so, we'll assign the least privileges necessary for them to perform the tasks associated with these roles. And, there are two types of role assignments that we can use; the first is eligible, which means the user can activate the assignment whenever they need to, and the second is active, which means the role has already been activated to perform the tasks. Let's step out and explore our administrative units available to us in our Microsoft 365 tenant. I am on the home page of our Azure AD admin center, and over on the left-hand side we have Roles & admins, we were just in here a few minutes ago talking about the roles that we can manage through the Entra admin center. But underneath the Roles & admins, we have Admin units, and of course, we don't have any at this point in time, and we don't have the proper licensing to create one, but if I go through some of the steps to get us there, I'm going to click Add, I'm going to enter UK, and I'm going to say UK Unit, and I'm going to restrict management administrative unit. So I'm going to click that to Yes, that way I can restrict who can access and manage this unit. I'll click Next to assign the roles, and you'll see these are the roles that we talked about: the Authentication Administrator, Cloud Device Administrator (specific to devices), Groups Administrator, Intuitive, Helpdesk, License, Password, Printer, SharePoint, Teams, Teams Devices Administrator, and User Administrator. So these are the administrator roles to associate with your administrative units. So let me scroll back up, and let's go ahead and click on License Administrator, and although we can't quite see the checkbox, I'm going to choose Linda, I'm going to click Add, I'm going to click Review + create, and you're going to see the name and the description of the administrative unit and that Linda has been assigned as a licensed administrator. Now, we don't have the proper licensing to actually complete the creation of this administrative unit, but these

are the steps necessary to create the administrative unit and assign an administrator to that unit. Your PIM, your Privileged Identity Management, is located under Identity governance. Click on Privileged Identity Management there, and we'll see we have the Azure AD roles, the groups, and the Azure resources that we talked about, and this is where I could come in and identify the resources to be accessed and the timeframe they can be accessed. So, in this module, we introduced and explored the management of Microsoft 365 roles that are available to us in Microsoft 365, as well as Azure AD, we introduced and discussed administrative units, and we provided an introduction and an understanding of PIM, Privileged Identity Management, in Azure AD. Up next is a course review on the highlights and the major topics that we discussed throughout the course.

Course Review

Course Review

In our final module, I just want to provide a course review. And what I'm going to do in this module is I'm going to be focusing on some of the key concepts and topics that we discussed throughout the course. Remember, we talked about the difference between Office 365 and Microsoft 365. Microsoft 365 includes Windows Enterprise, as well as mobile and security, where Office 365 just included the end-user apps, as well as some of the services like SharePoint, Teams, Exchange. We also introduced and discussed some planning ideas for your deployment of Microsoft 365. First concept in the planning process is planning and documenting the tenant name, deployment and management options, as well as your security considerations. The second piece is how we're going to get our data from either the cloud or on-prem into Microsoft 365. This includes Active Directory users and groups, the mailboxes, any PST files, as well as the data itself that we want to migrate to Microsoft 365. We also talked about setting up our company domain, and we do so by going into the Microsoft 365 admin center and going into Settings and Domains, then you choose to add a domain, you enter the company domain name, you choose how you're going to verify the ownership of the domain, and you choose how to make the required DNS changes; and if you remember correctly, we

needed to make a DNS TXT record to point to our Microsoft 365 tenant. Or we can walk through a wizard called Domain Connect, which is about three clicks, and that will automatically create your domain's DNS records for you. We talked a little bit about health. We want to be able to view the current health status. When we look at the history of our health, we have advisories and we have incidents. Incidents are a little bit more critical, so we'll to want to take those a little bit more seriously. We also looked at the view of history. We can slice and dice it in 7-day view, a 30-day view, we can do a search for specific information, and we can click on any of the information that we find and get specific details for each of the historical issues. We then talked about the idea of the adoption score, remember, there's two categories that it looks at; people experiences, which includes communication, meetings, content collaboration, teamwork, mobility. The other option is technology experiences, we have three categories in there, endpoint analytics, network connectivity, M365 apps health. These could all run up to a total of 100, and, if everything is running on all cylinders, the highest possible score you can get here is an 800. We also talked about adding users into our tenant, and we may want to take advantage of bulk user management for doing so. That requires the use of a CSV file and us populating our users in that CSV file. Then we can pop into the Microsoft 365 admin center and import that CSV file. Or, we can import it from PowerShell using the Import-CSV cmdlet. In the Microsoft 365 admin center, you'll find an option for browsing to locate your CSV file. From within PowerShell, we have a couple flavors: Azure AD PowerShell for Graph, or Azure AD module for PowerShell. Both of those will allow us to use the Import-CSV cmdlet to import multiple users that are stored in a CSV file. We also introduced the different Microsoft 365 group types. There is the powerful Microsoft 365 group, which includes activity with SharePoint, Exchange, OneNote, and Planner. We have a distribution list group type, which allows us to email information to multiple users, mail-enabled security, security, which is used for providing access to our resources, as is the mail-enabled security. And we have dynamic distribution groups, as well as shared mailboxes. These are the six different types of groups that we can create. You'll want to do your research to find out which group type is going to be necessary to allow you to complete the tasks that you want to complete. Remember, our groups have three roles. The owners, which allows

you to add and remove members, rename the group, update the picture and description of that group. Your members can access everything in the group, but they're unable to change any of the group settings, as the owners can. And your guests are group members from outside your organization who can collaborate and obviously they can't perform the tasks that the owners can perform. In order for our users to access our content in Microsoft 365, we need to assign a product license to our users as individuals. An alternative is to assign licenses based on group membership, and this is done through Azure AD. We can also use the CSV file to assign product licenses to multiple users, or we can use the GUI if we're trying to assign licenses to 20 users or less. PowerShell is always an option for assigning licenses, with an unlimited number of licenses that can be assigned, and you have to be either a global admin, a license admin, or a user admin to manage the licenses in Microsoft 365. We introduced the administrator role. There are about 30 of them in Microsoft 365 we can assign to the users, they map to common business functions, and it provides the users a pre-defined set of permissions. The Azure AD admin roles, there's about 60 of those babies, and there are built-in roles, as well as custom roles within Azure AD, which also provide pre-defined sets of permissions. Role management can be done through admin centers, the Azure AD admin center, as well as the Microsoft 365 admin center, and of course, by using PowerShell. Some considerations for your administrator role, have at least two, maybe up to four global admins, assign the least permissive role when you are assigning roles to your users or groups, require MFA, especially for your admins, assign service administrators, this would include services like SharePoint, Exchange, and Teams, and this allows them to perform administrative tasks within their respective services. We also introduced administrative units, which allows you to divide your organization into units. We then add users, or groups, or devices to those units. We assigned administrators to those units. We had about 10 different administrator roles that we could assign. The prerequisites for using admin units are Azure AD Premium P1 or 2 for each unit admin, Azure AD free licenses for your admin unit members, privileged role administrator, and we talked about the role administrators available to the admin units, and we can manage our admin units using Microsoft Graph module or the Azure AD module from within PowerShell. There are three major PIM

components. Those include the Azure AD roles, your Azure resources, and PIM for your groups. You can assign users and groups to these components, you'll want to, again, assign the least privileges necessary. There are two types of role assignments. We have the eligible, which users can activate whenever they need to, and we have active, which means the role has already been activated so they can perform the tasks associated with that role. So in our final module, we went in through a course review, and we reviewed some of the key concepts and topics from the course. Again, my name is Brian Alderman, thank you very much for watching, and I hope to see you in another Pluralsight course very soon. Take care.