Introduction to Microsoft Intune

by Dean Ellerby

This course will introduce you to Microsoft Intune and help prepare your lab environment.

Course Overview

Course Overview

Hi everyone. My name is Dean Ellerby, and welcome to my course, Introduction to Microsoft Intune. Microsoft Intune is Microsoft's flagship device management platform, intuating seamlessly into Azure Active Directory, Microsoft 365, and Microsoft 365 Defender. In this course, I help you understand the fundamental concepts around Intune and show you how to get up and running with your own lab environment. Some of the topics include an introduction to Microsoft Intune, a look at licensing, understanding the evaluation lab kit, and preparing your Azure AD and Intune environment. By the end of this course, you'll have everything you need to get started practicing device management concepts in your own lab and be ready to follow other related courses on Pluralsight. To follow along with all of the modules in this course, you'll need to have access to a Windows computer capable of running Hyper-V. I look forward to have you join me on this introduction to Microsoft Intune here, on Pluralsight.

Intune Fundamentals

Introduction

Microsoft Intune is well known as the industry standard for managing Windows and mobile devices in today's modern workplace. I've been working with Microsoft Intune since back when it was called

Windows Intune back in 2012. Back then, it was pretty limited in capability, even for managing Windows. The real powerhouse and focus for Microsoft was System Center Configuration Manager. Since then, a lot has changed. Most importantly for this course, Intune got a lot of attention from the program teams at Microsoft and is now arguably more feature-rich and capable than Configuration Manager. For now, I want to speak to the four main topics we're going to cover here. Firstly, I'll explain what Microsoft Intune is, walking through how this product can be used to manage Windows and mobile devices. Next, the Microsoft Intune product family. This is a relatively new name. It was released at Ignite in October 2022, and it essentially replaced the Microsoft Endpoint Manager branding. After that, I'll quickly walk through the relevant management portals that we'll be spending a lot of time in during this course. And finally, licensing, last but not least. Certainly true when it comes to how important this element is. Gone are the days of annual true-ups and trust-based licensing. If you need a user to have any benefit from Intune, you need to assign them a license. We'll talk through the type of Intune license available and any license bundled combinations that you're able to make use of.

Introduce Microsoft Intune

Microsoft Intune has been around for a long time. It's defined by Microsoft as a cloud-based service that focuses on mobile device management and mobile application management. So I guess before I can explain further about Intune, I need to touch on exactly what mobile device management is and how it contrasts with mobile application management. Mobile device management, as the name suggests, is about managing the device. Don't let the term mobile or mobile confuse you though. Mobile device management, or MDM, is not only about mobile devices. MDM is also a common means for managing Windows 10 and Windows 11 devices. The MDM reference actually refers to the interface that the management tool is leveraging to make changes to and manage the device. In Windows modern management, we've got something called an MDM provider, a unified way for mobile device management solutions like Intune to manage the Windows OS. So still on the subject of MDM, mobile device management might very well include some elements of managing applications on those devices, like deploying them, updating them, configuring them. But that's from the device perspective. Also, it's not all about Windows. The MDM part of Intune can absolutely manage mobile devices, such as iOS and Android, as well as Mac and Linux actually. We'll talk about those in a future course. When it comes to mobile application management, you guessed it. This is all about managing applications. When we talked about MDM, I mentioned a concept called modern management. That's the idea that we don't need to dig into the registry or local group policy to make changes to a Windows device. That same management concept is now built into many applications that include Windows, iOS, and Android apps. I say many applications, but obviously it's not all applications. It's a very small percentage of all apps in the world. The reason I use the word many is that well, firstly, it's almost all the Microsoft apps. That means that modern application management is probably built into a good proportion of the applications being used by organizations today. This capability allows us to manage the application of themselves irrespective of the state of the device. It could be managed by us, managed by someone else, or completely unmanaged, and we could still manage the MAM-enabled application.

Introduce the Microsoft Intune Product Family

Microsoft Intune is Microsoft's cloud-based endpoint management platform. It's also the name of a growing family of products related to endpoint management. Previously known as Microsoft Endpoint Manager, this product contains Intune itself, Configuration Manager for on-premises device management, as well as a suite of advanced solutions such as Remote Help for providing remote assistance, Microsoft Tunnel for allowing remote access to on-premises resources, and Endpoint Privilege Management for managing and securing local administrator access on devices. As I mentioned in the intro, this course is about Intune. We won't be covering Configuration Manager at all nor any of the advanced features I just mentioned. Next, let's take a quick look at the Intune portal.

Introduction to the Portals

Now I said we were going to go through the Intune portal, but anyone who's worked with Microsoft cloud services know that there's a lot of portals. There's a portal for almost everything, Office, Exchange Online, SharePoint Online, Azure Active Directory. Security. Actually, for a long time, there were more than seven portals for security alone. Anyway, in this clip, we're going to focus, and we'll set this focus on two specific portals. They are the Azure Active Directory portal and the Intune portal. So starting out at the Intune portal from endpoint.microsoft.com, you get to a home screen. From here, we can expand this left pane and see all the features that we can use. We're able to look at devices, apps, security, reports, users, and groups. Users and groups actually link me to the Azure Active Directory portal. Let's take a look. If we choose Users and take a look at some of the users we've got in our environment, you can see I've got Bob, Carrie, and Dan. Let's take a look in the Azure Active Directory portal. From here, you can see we've got Bob, Carrie, and Dan. So, one of the things I want to just quickly show you is that these panes are very similar. If I just flick between these two, you'll see that actually there's not a lot of difference between them at all. In fact, it's only the left pane that really changes because it's not just a view into this data. The Intune portal is actually just looking at the Azure Active Directory portal to get this information. It's the same with groups. If I choose Groups in this portal, you can see we've got SG-Office365Devices and ADSyncAdmins. And then going to Azure Active Directory admin center and choose Groups here, you can see we've got exactly the same groups there. They aren't a copy. They aren't two separate groups that are named the same. They're exactly the same groups, and that's something to be conscious of when we're going through this course. Next, we'll head back to the Intune portal and take a quick look at devices. The Overview screen shows us a very high-level overview of the devices in the environment. If we choose Apps, once again, a high-level overview of the installation status within our environment and security. We'll go through each of these in detail in future courses.

Licensing

When it comes to licensing, Intune is a user-based license. It's actually included with a load of other license bundles, so it's very possible that you've already got Intune licensing without even realizing it. Now for the purposes of this lab, we're going to be using a very specific development license, which definitely does include Intune. But this clip is about how you'd be typically licensing Intune in your environment in the real world. So we're not going to talk about my specific license right now. If you have any of these license bundles, these all include Intune. Let's run through each one of them one by one. I'll give you some context as to how they would be used. First up, we've got Microsoft 365 Enterprise E3 and E5. This is the type of license you'd usually have if you were a large organization with more than 300 users who want the typical fairly basic Microsoft offering. With E3, you get the basic level of security. And with E5, you have a really comprehensive security package. Microsoft 365 Frontline F3 is essentially the equivalent of Enterprise E3, but users aren't able to use full versions of Office or Windows. Microsoft 365 Education A3 and A5 are the education equivalent of E3 and E5. They're used for faculty staff. Microsoft 365 Business Premium is for organizations with fewer than 300 users. But this bundle is actually quite a bit more feature-rich than the Enterprise E3 version, and it's almost half the price per user per month, so it's a really great value. Enterprise Mobility and Security, E3 and E5, sometimes referred to as EMS E3 and E5, these are specific security bundles that contain Azure AD Premium and Intune, among other things. You'll find these come as part of Microsoft 365 E3 and E5 bundles. It's also possible to purchase Intune Standalone. This doesn't include Azure AD Premium, so it's not going to allow you to do autopilot. Finally, the Intune Device License. While some MDMs license their product per device, Intune is definitely licensed per user. That said, for specific userless scenarios, such as kiosks and terminals, it is possible to buy an Intune license per device.

Summary

In this module, we've talked through a brief introduction to Intune and had a quick first look at the portals or admin centers. We've also walked through each of the licensed bundles you can use to get your hands on an Intune license for each of your users. In the next module, we're going to get ourselves set up with an on-premises lab environment so we can follow along.

Preparing Your On-premises Lab Environment

Understand the Windows 11 and Office Deployment Lab Kit

In order to get up and running with a realistic lab environment, we need to roughly resemble a typical organization. A typical organization today leverages on-premises Active Directory. Whilst on-premises devices are rapidly becoming a thing of the past, on-premises user identities are sticking around for a while. For that reason, in this module, we're going to leverage Microsoft Windows 11 and Office 365 Deployment Lab Kit, a freely available self-deploying lab by Microsoft. To get access to this lab, all we need to do is head to aka.ms/windows11labkit. This will take us to the Windows 11 and Office 365 Deployment Lab Kit. As you can see, we get an overview of the environment, and it explains that actually it contains everything you need to get up and running with Windows 11 Enterprise and Microsoft 365 Enterprise apps managed by Enterprise Mobility and Security. It provides a virtual environment, including domain-joined desktop clients, a domain controller, an internet gateway, and a fully configured Configuration Manager instance. Now I mentioned earlier on that we aren't actually going to be talking about Configuration Manager in this course. We're actually just going to get this and turn it off. We don't need this virtual machine for Intune management. Let's just scroll down to the bottom, and we get some prerequisites. This self-deploying lab environment is based on Hyper-V. We're going to need the Hyper-V role installed. Other hypervisors will not work for this self-deploying lab. We need administrative rights on the device and at least 150 GB of free disk space. It does say in this website that we need 300 GB, but that's when you're using the Configuration Manager environment, and we're going to just turn that off. It says you need a high-throughput disk subsystem, which is SSDs rather than HDDs. It will probably work even if you don't have SSDs though. It mentions you need 16 GB of available memory, but 32 GB is recommended. In this case, we'll probably fine with 16 GB. You need a high-end processor for faster processing, which is generally true. It mentions that you should use a broad bandwidth to download this content because it's 22 GB in size. Scrolling on down one little bit more, and right at the bottom it says Windows 11 VMs expire 90 days after the lab is provisioned. Now that's provisioned by Microsoft, not provisioned by you. So, this lab will actually expire 90 days after Microsoft uploaded it to their website. In my case, it will expire on November 5, 2022. For you, this is most likely to be different, and you will need to download a new version when it expires. Microsoft will publish a new version on or before the expiration date. Scrolling back up to the top, it's simply a case of choosing Download the Lab Environment. We need to enter in our details. And once you're done, just click Download now. Once you've chosen Download now when it's finished downloading, you'll end up with a Microsoft365DeviceLabKit.zip in your Downloads folder. From here, it's simply a case of right-clicking and choosing Extract All and then choosing the place you want it to go to. In my case, I would like it to go to F:\M365-DLK. I'll choose Extract. Once it's finished extracting, it gives you three files. There's a large file containing all the content. There's a setup file and a zpaq.exe. So, all we're going to do is double click on exe, and we're presented with a welcome screen. It mentions the process can take approximately 20 minutes. We'll choose Next. We read through the end user license agreement. I have previously read this, so I'm going to choose Next. And it's ready to be provisioned. So just a case of choosing Next and waiting for the provisioning to take place. Once it's finished provisioning, we end up with a set of folders and files. The folders contain the virtual machine configuration information, and the files contain the hard disk image file. There's also some snapshots. So how do we use these? Well, actually, what it went through and did while we were using this provisioning process is it set up some Hyper-V virtual machines. So from our Hyper-V manager, you can see we've got some configured virtual machines. We have client 1 to 6, CM1, DC1, GW1, INET1, and VPN1. Now client 1 to 6 are Windows virtual machines. They're off by default, and they're in various stages of configuration. We're going to look through those in a future course. CM1 is the Config Manager environment. It's turned off by default, and we're not going to turn it on. If you'd like, you can delete it and delete the source files. Next, we have DC1, which is the domain controller. And following that, GW1. GW is the gateway server. The gateway server allows the other virtual machines to access the internet. Let's take a brief look at how that works. From the host PC, we're going to right-click and choose Virtual Switch Manager, and we've got a few virtual switches that are already created. We have External Wireless, which actually is a virtual switch that I created prior to this course. The following two switches are provided by the lab environment. We've got HYD-CorpNet, which is a private virtual switch, and HYD-InterNet, which is also a private virtual switch. The External Wireless, in this case, is the only network with access to the internet. So how do these virtual machines have access to the internet? Let's take a look at domain controller. We'll right-click and choose Settings, and you can see we've got a network of HYD-CorpNet. That means that it doesn't have access to External Wireless. Yet when we connect to this computer, you'll notice that we do actually have internet access. So how does that work? Well, it actually uses the gateway. So if we right-click on the gateway and choose Settings, you can see this has both HYD-CorpNet and External Wireless. These are completely configured by the lab environment, and I didn't need to do this. Let's connect to HYD-DC1. Upon connecting, as you can see, it says your Windows license will expire soon, and you need to activate it in Settings. In my case, when I'm recording this, I only have 22 days left before it expires. If this is the case for you, be sure to download the new environment when it's provided by Microsoft. For now, I want to choose Close, and we'll take a brief look at the environment. Got to Start and Active Directory Users and Computers. And from here, we're going to corp.contoso.com and take a look at the organizational units that are provided. We have the Builtin and Computers as normal. We have CORP, which has been created for us, Domain Controllers as usual, and Users. Let's go into CORP. We have Administrators, GROUPS, SERVICE ACCOUNTS, and USERS. Moving into Administrators, there are no items in this view. USERS, we have test users 1 to 4. As part of setting up the course, we're going to change these users to something more meaningful so that when they are synchronized to Azure Active Directory later in the course, there'll be a bit more pleasing on the eye. If we head down to Users, these are the default users that you get in a typical Active Directory environment. In the next module, we're going to set up our cloud environment and synchronize our users.

Preparing Your Cloud Lab Environment

Introduction

Now we're ready to get started building our cloud lab environment. We'll use the work we've done so far to populate our new environment. But first, we have to set it up. As we go through this module, we'll talk about the difference between and importance of Azure AD tenants and subscriptions. They're not the same thing. We'll then jump into the portal and get our Microsoft 365 and Azure AD tenant completely free of charge. Next, we'll synchronize the on-premises environment with Azure. And finally, we'll take a look at how all of this is secured. Let's start with tenants and subscriptions. I'll read this to you, but feel free to pause it and make sure you fully understand it. An Azure AD tenant is a reserved Azure AD service instance that an organization receives and owns once it signs up for a Microsoft cloud service, such as Azure, Microsoft Intune, or Microsoft 365. Each tenant represents an organization and is distinct and separate from other Azure AD tenants. Tenants contain devices, users, groups, and act as an identity provider for other Microsoft services like Microsoft 365 and Intune. Conversely, a subscription is a billing container. This allows you to purchase Azure-based services, such as virtual machines. A subscription relies on Azure AD as the identity provider. It's possible to have more than one subscription relying on a single Azure AD. Some organizations do this to allow different business units to purchase services. When it comes to licensing Microsoft 365 services like Office 365 and Intune, we don't actually need a subscription at all. These services are paid for either directly to Microsoft through the admin portals, via a partner such as a cloud service provider, or via an enterprise agreement. With any of these, you don't need an Azure subscription. You just need an Azure AD tenant. So to be clear, for the purposes of this course and pretty much every course around Intune, you don't need an Azure subscription. You need an Azure AD tenant and some licensing. Up next, we're going to sign up for the Microsoft 365 Developer Program so we can get started.

Sign up for the M365 Developer Program

So to start out, we're going to go to aka.ms/m365devprogram This takes us directly to the Microsoft 365 Dev Center where we can sign up for the Microsoft 365 Development Program. I invite you to scroll down the page and read more about the program to understand more, but the most important bit is right underneath this blue box, which says that you get a free Microsoft 365 instant sandbox with pretty much everything you need. It's got 25 user licenses, which expire 90 days after you load them. So, this is renewable. As you can see, it says on this page, it expires January 5th, 2022. Once you've expired, once it comes to exploration, it will renew it provided that you've continued to use that tenant within that period. One thing that we must understand is that it's not possible to apply these developer licenses to an existing tenant. So you can't, for example, have an existing tenant with some Microsoft 365 E3 licenses and then sign up for the developer program and convert that to Microsoft 365 E5 somehow. This needs to be a fresh tenant, a greenfield tenant, that is brand new and you sign up for it right here. So let's do that. We'll click Join now, and we get to sign into a Microsoft account. Now as I say, if you have a Microsoft account that you would like to use that doesn't already have a tenant attached to it, then you could use this. But in my case, I'm going to create a new one. Once you've completed the sign up, you get to this page here. As you can see, it's a renewable E5 subscription, which expires in the future. I have 92 days left, and you can see my administrator username right there. I have 25 users, but none of the sample data packs are installed, and that's fine because we have other ways to get our users into the environment. We're going to create some on-premises users and synchronize them via Azure AD Connect in a future module. For now, we're just going to hit Go to subscription, which takes us to the Office portal so that we can start using the environment. In this case though, we don't want to use Office. We want to administer Office. So we're going to head to the waffle on top left and choose Admin, and we're heading to the admin.microsoft.com portal so we can start doing some admin tasks. Here, I'm just going to quickly browse into Billing and then Licenses so that you can see that we have some licenses available. We have the Microsoft 365 E5 Developer license (without Windows and Audio Conferencing). We've got

24 licenses available because one of them has already been assigned to my admin user that we created during this process. Now a point on without Windows and Audio Conferencing. Audio Conferencing is not a big deal. I'm not going to be going into any of the features of Audio Conferencing or even Teams or any other collaboration tool during this course. So that's not such a problem. Windows though, a lot of the things we're going to be talking about will rely on having a Windows PC and Windows license in order to do some testing. So, that might be a problem. However, the Windows 11 and Office Deployment Lab Kit that we created earlier on in the previous module gives us those Windows licenses that we need. Next, we're going to configure our custom domain name so that when our users finally sign in, they have a familiar email address-like username to sign in with.

Prepare Custom Domain Names

Heading into the Azure Active Directory admin center, we're going to go to Azure Active Directory. Scroll down to Custom domain names. And from here, you see we have that one domain already set, this firstcoffee3.onmicrosoft.com domain. It's status is Available, and its primary. Now, this is the domain that users would need to type when they're logging in. For example, I would need to type dean@firstcoffee3.onmicrosoft.com, and that's not particularly short or easy to remember. So, what we're going to do is use this custom domain to add in something more familiar to the users, so something more like their email address. So we'll just go to Add custom domain and type in the custom domain that we own, which is firstcoffee.co.uk. Now that we've added this domain to Azure AD, we now need to prove that it's ours. We need to prove to Azure that we own this domain. And that's really simple to do. As you can see, it says that we need to add a text record, a txt record, within the domain name registrar, and that's just a DNS record that we need to add that. So what we simply do is get this information here. It's the text. The hostname is @, a specific destination that Microsoft has provided, and a time to live value. So we're just going to take these, and if you manage your domain, then you can take these and start entering these into your DNS management section of your domain provider right now. If you don't, you can share these details via email or just send them over to the admin who manages your domain name. For now, I'm going to put these into my DNS management section of the domain name provider that I use. So from the DNS Records section, I'm just going to hit Add. I'm going to choose the TXT type record. I'm going to hit @ because that's what Microsoft said it needed to be, the string that Microsoft provided, which is MS=ms and then a number, and the time to live was 3600 seconds, which is 1 hour. Simply a case of choosing Add record, and now that gives Microsoft a chance to verify that we are able to make changes to that domain, and therefore we most likely own it. Give that a few seconds and then head back to Azure AD and choose Verify, and that's it verified. So heading back into Custom domain names, you can see we've got these two domains here now. We've got the custom domain that I want to use. We also have the onmicrosoft domain that we could use if we wanted to. But the onmicrosoft domain here is primary, and that's not ideal because I would prefer to use firstcoffee.co.uk as my primary domain. So we're going to go back into firstcoffee.co.uk and choose Make primary, and we're sure that we want to do that. Now that we have the custom domain applied and it's set to Primary, the next step is to ensure that our company branding is in place as this ensures that the users' login experience on the web and in Autopilot are personalized to the organization.

Prepare Company Branding

So from the Azure Active Directory admin center, pretty much where we left off, we go down to Azure Active Directory. Just scroll down to Company branding. And at the moment, it says the status of this company branding is not configured. The tooltip there says configure the text and graphics your users see when they sign into Azure Active Directory. Now remember, our users are going to be signing into Azure Active Directory when they're using their computer, when they're using Microsoft 365 or Intune. So our users are going to be seeing these a lot. Just hit Configure, and we have some requirements around the size and type of file that we use for this company branding. You can see the possible images we can change our the sign-in page background image and the banner logo. Heading back to the sign-in page background image, this needs to be 1920 x 1080, smaller than 300 KB, and either PNG, JPG, or JPEG. In my case, in order to hit that 300-KB limit, I need to actually use the JPG file type. Simply a case of choosing Select a file, finding the asset you're looking for, choosing Open. It will upload that straightaway, and it's ready to go. Doesn't quite look correct when you look at it from this perspective because this is a square image and a one-to-one aspect aspect ratio. But when it comes to users viewing on their screen when they're logging in, typically that will be presented in 1920 x 1080. Typically, that will be presented not in a one-to-one aspect ratio, so it will look perfect on their screen. Next, the banner logo needs to be 280 x 60 px and smaller than 10 KB. It can be a transparent PNG, a JPG, or a JPEG. Again, just going to grab my JPEG file here. All done. Now it's possible for you to give a user name hint to remind users to use their email address as the username and also sign-in page text, which will allow the users to become familiar with the sign-in page if it's not something they're used to. Next, we're going to choose Save, and we're all done. So, with the branding all sorted, we're almost ready to get our on-premises environment synchronized with Azure AD. In the next module, we're going to get prepared for that synchronization.

Prepare the On-premises Directory for Synchronization

So let's get started. Firstly, there's a few things we need to do in the lab environment to tidy things up and get things ready for synchronization. So we'll head there now. So I'm currently logged into DC1. And in Active Directory Users and Computers, you can see we've got some computers in the Computers OU. And that's not ideal really because most organizations wouldn't have a single Computers OU where they keep all their computers, whether it be clients or servers or whatever. They would have specific OUs for those particular computers. So let's jump in and do that. We're going to go into CORP, right-click. New, OU. I'm going to call it Client Computers. And then we also have a new one for servers. Obviously, use your own naming standards and naming schemes. So here, we're going to go with some nice and simple like that. And for the clients, just going to move those. And for the servers, I'm just going to move those as well. Okay, that's tidied up. Next, we want to head into CORP and USERS and see what we've got there. Now this originally, when I started, had TestUser1, 2, and 3 and 4. As you can see, I've started renaming these users already. I left the last one though just so we can do that together. So on TestUser4, quickest way to rename this user so it's more relevant to us is to Rename and type in the example username I've got for this user. And you can see the full name is there, Erin Hall. First name is Erin, last name Hall. User logon name, I'm going to go with something nice and simple and do erin and choose OK. I need to jump back into this user though. Go into Properties, into Profile, and you can see we've got a home directory there that we're going to rename as well. When you choose Apply, it will say that this folder needs to be created manually. We'll go ahead and do that. Choose OK and OK. So now we've got our four test users, and we're going to make sure they're in specific groups as well. So let's jump into Erin again and see what she's a member of. So we have Finance, and she's also in the TestUserGroup, which sounds great. Let's check Morgan, Marketing, and the TestUserGroup. Great. So we've got a good spread there. Next, there was one other thing that caught my eye. When we go back into Erin's user here, you can see that the email address is @contoso.com, and the account actually is @contos.com as well. So we have a couple of UPN suffixes here. We've got corp.contoso.com and contoso.com. Now in my example, we're using firstcoffee.co.uk as the top-level domain name that we're using for this environment. So it would be really useful if I could have this on-premises environment match firstcoffee.co.uk. So we're going to go ahead and do that. Now I don't think for the purposes of this lab and for the learning that we're trying to do here, it would be relevant or make sense to change the full domain at the top here, this contoso.com domain. But I do think would be useful to allow Erin to log in with erin@firstcoffee.co.uk. And the way we do that is by adding an additional UPN suffix. So let's go ahead and do that. So we head down to the Start menu and go to Windows Administrative Tools and then Active Directory Domains and Trusts. From here, be careful when you're right-clicking here. So we're not right-clicking on the domain here. We're right-clicking on the Active Directory Domains and Trusts title just here. Right-click and choose Properties. And you can see we've got these alternative UPN suffixes. So, we need to add in firstcoffee.co.uk. In your environment, please choose the UPN suffix that makes sense for you. Choose OK. And we can close down domains and trust now and go back to Erin's account, Properties, Account, and then we've got firstcoffee.co.uk right here for us. We'll choose that and then choose OK, and we're good to go. Now Erin, in the on-premises environment, could log in with erin@firstcoffee.co.uk. And we're going to synchronize that up to the cloud so that she can log in to Azure AD using erin@firstcoffee.co.uk. I'll go ahead and change Gordon, Morgan, and Hugo's accounts so they can also do the same. And we're all done tidying up this environment. Next, we need to synchronize this environment with Azure Active Directory. We'll do that by installing and configuring Azure AD Connect.

Install and Configure Azure AD Connect

Back at the Azure Active Directory portal, just a case of scrolling down in this list to Azure AD Connect. And from here, just scrolling down a little bit so we can see this Download Azure AD Connect button. We'll choose that. It opens up a download page from microsoft.com, which is perfect. So we'll just scroll down here. You can see we can download--- Now depending on your environment, you may want to download this and then copy it over to your server. In my case, I'm going to just grab this URL, head back to the server, and then I'm going to just tap in this URL. And from here, scroll down. Choose Download. Now setting up Azure AD Connect has become a lot easier over recent years. Hopefully, you'll see that this actually is not too painful an experience. And you can see we've got Azure AD Connect right here. Let's double-click on that. And we'll just drive through this wizard. The welcome page explains that the tool will give you a guide to selecting a solution, for example password hash sync or federation with AD FS. It will install an identity synchronization tool and other components required for deployment and also will enable application telemetry and component health by default. Make sure you read and agree to the license terms and privacy notice. I've done that. I'm going to choose Agree. Now we have the option of choosing express settings or Customize. The express settings, in this case, actually would work pretty well. But I want to choose Customize. And then from this page, I don't actually have any additional things I want to choose, so I'm just going to choose Install. And I'm going to allow it to install the required components. Now we get to choose the user sign-in method. We went through this earlier on. But we're going to choose password hash synchronization, and we're also going to enable single sign-on to allow our desktop users to have a single sign-on experience when accessing cloud services from their domain-joined desktop machines. We'll choose Next. And here, we need to enter the global administrator credentials for Azure AD. In this case, that's me. Next, we choose the directory type, there's only one, and the forest that we want to synchronize. Next, we need to have Azure AD Connect create a forest synchronization account. The preferred option is to create a new AD account, and the way we do that is by typing in the enterprise admin credentials, which, in my case, is just the admin for this lab. So we've configured corp.contoso.com Active Directory domain for this synchronization. We'll choose Next. And here we have a list of the Active Directory UPN suffixes that we have in the environment. You remember from earlier on that we've got corp.contoso.com and contoso.com along with the new one that we created, firstcoffee.co.uk. Now it also matched those with Azure AD, and it knows that corp.contoso.com and contoso.com are not verified within Azure AD, but firstcoffee.co.uk is. It asks us to select the on-premises attribute to use as the Azure AD username. Now the best thing to do is to use the UPN because the UPN looks very familiar to users as an email address. So for the user principal name, we're going to go with userPrincipalName. And it asks us now to verify that we will continue even though we aren't matching all the UPN suffixes to verify domains because really I don't own contoso.com or corp.contoso.com, so I'll never be able to verify those in Azure AD. It warned us that users who have a UPN suffix that doesn't match a verified domain won't be able to log into Azure AD. We'll choose Next, and we'll select the OUs that we want to sync. In my case, I want to limit my synchronization to CORP because that contains my users and devices. We'll choose Next. And because this is a lab, we know that our users are represented only once across all directories, and we're happy for Azure to manage the source anchor for these identities. We'll choose Next. In this environment, I don't need to use a filter for a pilot deployment of synchronization. What I'm going to do is just choose Next. And in the optional features, I'm going to enable password writeback because that enables things like SSPR, self-service password reset. We don't need it for this course, but I might use it in the future. Finally, we choose Next. And just to enable single sign-on, very simply we need to enter the credentials and tap in our domain administrator account. We'll choose Next. And finally, Install, and off it goes to configure the environment. So, that configuration is now complete. We get a few messages here to just read through. So firstly, the configuration is complete. We can now log into Azure or Office 365 to verify that the user accounts from the local directory have been created. Then we can do a test sign-on. It mentions that an Active Directory Recycle Bin has not been enabled for the forest, but is strongly recommended. It lets us know that Azure Active Directory is configured with the ms-DS-ConsistencyGuid as the source anchor attribute. And we can also configure Seamless SSO through Group Policy. Last thing to do is just to hit Exit. Finally, we're going to head back to Azure Active Directory and take a look at the environment. So we'll scroll back up to the top here, choose Users, and you can see we've got some additional users in this environment right now. We have Erin Hall, Gordon Reilly, Hugo Armstrong, and Morgan Fields. They're all configured as on-premises synchronized users, and we're ready to go. Next, it's just a case of checking that Intune is enabled and that the environment is secure.

Enable Intune (MDM) and Security Defaults

Security is incredibly important when it comes to Intune and endpoint management. Once we've enabled Intune as the MDM, we'll go ahead and configure some basic security using a feature called security defaults. First, let's take a look at the MDM settings. We'll just scroll down this list to Mobility (MDM and MAM). That stands for mobile device management and mobile application management. As you can see, Microsoft have helpfully put Intune in this mobility list for us. I will highlight though that Azure Active Directory works with many other cloud-based MDMs aside from Intune. By clicking Add application, you can see this ever-growing list of supported MDMs. Back to the mobility list, and we can select Intune. We're able to configure just two things here. That's the MDM setting and the MAM setting. With MDM, we're essentially deciding which users can access the MDM application. It's a choice of no one, some people, and everyone. If you think back to the idea of having more than one MDM in the environment, you can see how it might be useful to have some users using this MDM and some other users using a different MDM. As we're going to be working with Autopilot in a future course, we're going to set MDM to All. It's important that we set MAM to None in this case. Having MAM set to All will almost always cause a conflict, so it's best to avoid that. Next, back to the Azure AD admin portal and back to the top so we all know where we're starting from. Now we need to ensure that we have some basic security enabled via security defaults. We actually find security default in the Properties pane all the way at the bottom. Security defaults enables things like multifactor authentication for admins, which is a great start. Bear in mind, enabling security defaults means you can't use conditional access, so we'll be turning this feature off once we're working with conditional access further down the road. For now, we'll set that to On. And just like that, our hybrid lab environment is up and running, ready for us to get started with Intune.