Windows 10 Enterprise E3 in CSP // A technical overview

Do your small- and medium-sized customers need access to Windows 10 Enterprise edition, but they do not have a Microsoft Volume Licensing plan or Software Assurance? Windows 10 Enterprise E3 in CSP is designed to give small- and medium-sized organizations access to Windows 10 Enterprise edition with licensing terms that are friendlier for organizations of these sizes. Learn how you can sell Windows 10 Enterprise E3 to your customers and help them manage their Windows 10 Enterprise deployments.

Microsoft

INTRODUCTION

Windows 10 Enterprise E3 in CSP, available through Microsoft's Cloud Solution Provider (CSP) program, is an offering that allows CSP partners to upgrade their customers to Windows 10 Enterprise edition. Windows 10 Enterprise E3 in CSP provides a flexible, per-user subscription for small- and medium-sized organizations (from one to hundreds of users). Windows 10 Enterprise E3 in CSP is managed by using the Partner Center portal. To take advantage of this offering, the customer must have the following:

- Windows 10 Pro Anniversary Update or later installed on the devices to be upgraded
- Azure Active Directory (Azure AD) available for identity management

Starting with Windows 10 Anniversary Update, customers can move from Windows 10 Pro to Windows 10 Enterprise easier than ever before—no keys and no reboots. Upon entering the Azure AD credentials that were assigned a license to Windows 10 Enterprise E3, the operating system turns from Windows 10 Pro to Windows 10

IN THIS GUIDE:

Enterprise and all the appropriate Windows 10 Enterprise features are unlocked. When a subscription license expires or is transferred to another user, the Windows 10 Enterprise device seamlessly steps back down to Windows 10 Pro.

When you participate in the Windows 10 Enterprise E3 in CSP program, you can provide customers with the following benefits:

- **Windows 10 Enterprise edition.** You can provide customers currently running Windows 10 Pro Anniversary Update with Windows 10 Enterprise Current Branch (CB) or Current Branch for Business (CBB). This benefit does not include Long Term Service Branch (LTSB).
- **Support from one to hundreds of users.** You can support customers who may only need one Windows 10 Enterprise E3 license to organizations that need up to hundreds of licenses. Although the Windows 10 Enterprise E3 in CSP program does not have a limitation on the number of licenses an organization can have, the program is designed for small- and medium-sized organizations.
- **Install on up to five devices.** A per-user license entitlement allows a user to install Windows 10 Enterprise edition on up to five devices.
- **Roll back to Windows 10 Pro at any time.** When a user's subscription expires or is transferred to another user, the Windows 10 Enterprise device reverts seamlessly to Windows 10 Pro edition (after a grace period of up to 90 days).
- **Monthly, per-user pricing model.** Each Windows 10 Enterprise E3 subscription costs just $7.00 USD per user, per month, with a 1-year minimum subscription. This makes Windows 10 Enterprise E3 affordable for any organization.
- **Move licenses between users.** Licenses can be quickly and easily reallocated from one user to another user, allowing customers to optimize their licensing investment against changing needs.

How does the Windows 10 Enterprise E3 in CSP program compare with Microsoft Licensing programs and Software Assurance? Microsoft Volume Licensing programs are broader in scope, providing organizations with access to licensing for all Microsoft products. Software Assurance provides organizations with the

Previously, only organizations with a Microsoft Volume Licensing plan could deploy Windows 10 Enterprise to their users. Now, with Windows 10 Enterprise E3 in CSP, small- and medium-sized organizations can more easily take advantage of Windows 10 Enterprise features.

following categories of benefits:

- **Deployment and management.** These benefits include planning services, Microsoft Desktop Optimization (MDOP), Windows Virtual Desktop Access Rights, Windows-To-Go Rights, Windows Roaming Use Rights, Windows Thin PC, Windows RT Companion VDA Rights, and other benefits.

- **Training.** These benefits include training vouchers, online e-learning, and a home use program.

- **Support.** These benefits include 24x7 problem resolution support, backup capabilities for disaster recovery, System Center Global Service Monitor, and a passive secondary instance of SQL Server.

- **Specialized.** These benefits include step-up licensing availability (which enables you to migrate software from an earlier edition to a higher-level edition) and to spread license and Software Assurance payments across three equal, annual sums.

Table 1 on page 4 shows a comparison between Windows 10 Enterprise E3 in CSP and Software Assurance. In addition to the information in Table 1, another difference is license management. In Windows 10 Enterprise E3 in CSP, you (the partner) can manage licenses for your customers. With Software Assurance, customers manage their own licenses.

In summary, the Windows 10 Enterprise E3 in CSP program is an upgrade offering that provides small- and medium-sized organizations easier, more flexible access to the benefits of Windows 10 Enterprise edition, whereas Microsoft Volume Licensing programs and Software Assurance are broader in scope and provide benefits beyond just access to Windows 10 Enterprise edition. If your customers need the benefits of Microsoft Volume Licensing programs and/or Software Assurance, then you should continue to recommend them.

Table 1. Comparison between Windows 10 Enterprise E3 in CSP and Software Assurance

PHASE	WINDOWS 10 ENTERPRISE E3	SOFTWARE ASSURANCE
Pricing	$7 per user per month	$219 (3 years) to $317 (2 years)
License type	Per user	Per device or per user (depending on program)
Devices per seat	5	1–5 (depending on program)
Commitment	1 year	Up to 3 years
Billing cycles	Monthly	Annual
Seat minimum	1	5–250 (depending on program)
Seat maximum	None	None
Qualifying operating system	Windows 10 Pro Anniversary Update edition	Windows Pro edition (versions: XP, Vista, 7, 8)
Partner managed seat assignment	Yes	No
License activation	Digital license based on Azure AD identity	MAK or KMS keys
Volume discounts	No	Limited or yes (depending on program)
Long Term Servicing Branch (LTSB)	No	Yes
Downgrade rights	No	Yes
Microsoft Desktop Optimization Pack	No	Yes
Microsoft support and training benefits	No	Yes
Virtual Desktop Infrastructure rights	No	Yes

COMPARE WINDOWS 10 PRO AND ENTERPRISE EDITIONS

Windows 10 Enterprise edition has a number of features that are unavailable in Windows 10 Pro. Table 2 lists the Windows 10 Enterprise features not found in Windows 10 Pro. Many of these features are security-related, whereas others enable finer-grained device management. Ultimately, users who will benefit from Windows 10 Enterprise edition are those who need one or more of the features in the following sections.

CREDENTIAL GUARD

This feature uses virtualization-based security to protect security secrets (e.g., NTLM password hashes, Kerberos Ticket Granting Tickets) so that only privileged system software can access them. This helps prevent Pass-the-Hash or Pass-the-Ticket attacks.

Credential Guard has the following features:

- **Hardware-level security.** Credential Guard uses hardware platform security features (such as Secure Boot and virtualization) to help protect derived domain credentials and other secrets.

INFORMATION

Protect derived domain credentials with Credential Guard

- **Virtualization-based security.** Windows services that access derived domain credentials and other secrets run in a virtualized, protected environment that is isolated.
- **Improved protection against persistent threats.** Credential Guard works with other technologies (e.g., Device Guard) to help provide further protection against attacks, no matter how persistent.
- **Improved manageability.** Credential Guard can be managed through Group Policy, Windows Management Instrumentation (WMI), or Windows PowerShell.

DEVICE GUARD

This feature is a combination of hardware and software security features that allows only trusted applications to run on a device. This means that even if an attacker manages to get control of the Windows kernel, he or she will be much less likely to run executable code after the computer restarts. Device Guard uses virtualization-based security in Windows 10 Enterprise E3 to isolate the Code Integrity service from the Windows kernel itself, which lets the service use signatures defined by customer-defined policies to help determine which code is trustworthy.

Device Guard does the following:

- Helps eliminate malware
- Helps protect the Windows system core from vulnerability and zero-day exploits
- Runs only those apps trusted by the customer

INFORMATION

Device Guard overview

APPLOCKER MANAGEMENT

This feature helps IT pros determine which applications and files users can run on a device (also known as "whitelisting"). The applications and files that can be managed include executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers.

INFORMATION

AppLocker

MICROSOFT APPLICATION VIRTUALIZATION (APP-V)

This feature makes applications available to end users without installing the applications directly on users' devices. App-V transforms applications into centrally managed services that are never installed and don't conflict with other applications. This feature also helps ensure that applications are kept current with the latest security updates.

INFORMATION

Application Virtualization

MANAGED USER EXPERIENCE

This feature helps customize and lock down a Windows device's user interface to restrict it to a specific task. For example, you can configure a device for a controlled scenario such as a kiosk or classroom device. The user experience would be automatically reset once a user signs off. You can also restrict access to services including Cortana or the Windows Store, and manage Start layout options, such as:

- Removing and preventing access to the Shut Down, Restart, Sleep, and Hibernate commands
- Removing Log Off (the User tile) from the Start menu
- Removing frequent programs from the Start menu
- Removing the All Programs list from the Start menu
- Preventing users from customizing their Start screen
- Forcing Start menu to be either full-screen size or menu size
- Preventing changes to Taskbar and Start menu settings

DETERMINE WHICH USERS NEED WINDOWS 10 ENTERPRISE E3

How do you help customers determine which users need Windows 10 Enterprise edition? Clearly, the users will require one or more of the features listed in the previous section. But what types of users are typical candidates for Windows 10 Enterprise edition? The following list shows example user scenarios that can help you identify users who need Windows 10 Enterprise edition:

- **Users who access confidential information.** These users need additional attack protection because of the confidential information they routinely access. This information could be payroll, human resources, emerging products, or other types of confidential information. All the security-related technologies can help protect these users.
- **Anonymous users who use kiosks or other public devices.** These users access devices that are publicly available—for example, running apps on kiosks. All the security-related and managed user experience control features help protect these users.
- **Users with elevated privileges.** These users have elevated privileges (such as administrator privileges) for access to user accounts, file resources, and other secured resources. All devices used by IT pros to administer customers' IT services

need the added security protection in Windows 10 Enterprise edition. All the security-related technologies can help protect these users.

- **Users who must comply with governance or compliance standards.** These users work with information that is subject to governance or compliance standards, such as Payment Card Industry (PCI) or Health Insurance Portability and Accountability Act (HIPAA) standards. The devices used by these users must be protected to prevent malware or malicious attacks. All the security-related technologies can help protect these users.

- **Users who travel with devices.** These users often work over public Internet connections, and their devices are more accessible to unauthorized users. They often work at customer locations or from home. These locations are typically not as secure as a direct connection to an organization's private intranet. These devices need to be protected to prevent malware or unauthorized access to the information on the device. In addition, the device needs protection in case the device is lost or stolen.

PREPARE THE CUSTOMER ENVIRONMENT

Many of your customers will have on-premises Active Directory Domain Services (AD DS) domains. Users will use their domain-based credentials to sign in to the AD DS domain. Before you start deploying Windows 10 Enterprise E3 licenses to the customer's users, you need to synchronize the identities in the on-premises AD DS domain with Azure AD.

You might ask why you need to synchronize these identities. The answer is so that users will have a *single identity* that they can use to access their on-premises apps and cloud services that use Azure AD (such as Windows 10 Enterprise E3). This means that users can use their existing credentials to sign in to Azure AD and access the cloud services that you provide and manage for them.

FIgure 1 on page 11 illustrates the integration between the on-premises AD DS domain with Azure AD. Microsoft Azure Active Directory Connect (Azure AD Connect) is responsible for synchronization of identities between the on-premises AD DS domain and Azure AD. Azure AD Connect is a service that you can install on-premises or in a virtual machine in Azure.

INFORMATION

For more information about integrating on-premises AD DS domains with Azure AD, see the following resources:

- Integrating your on-premises identities with Azure Active Directory
- Azure AD + Domain Join + Windows 10

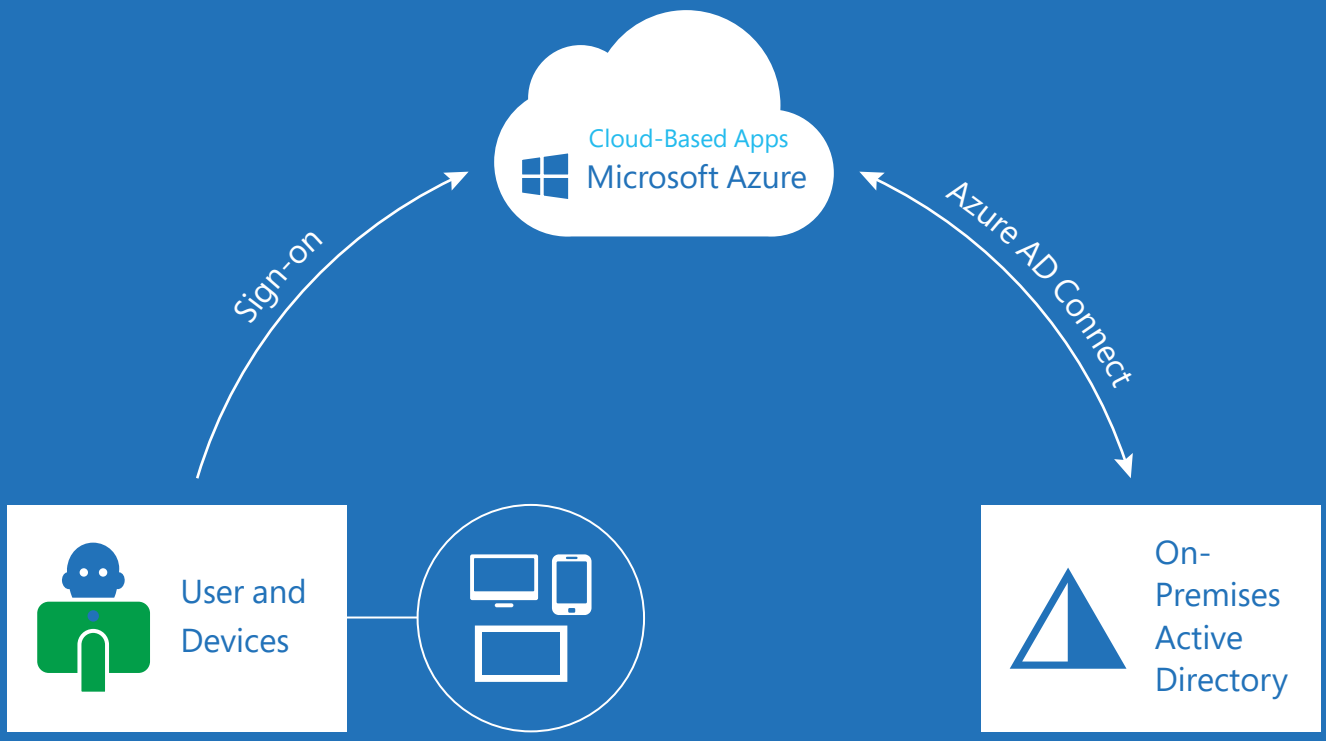

FIgure 1. On-premises AD DS integrated with Azure AD

MANAGE THE CUSTOMER SUBSCRIPTION

What does the process for managing Windows 10 Enterprise E3 in CSP subscriptions for customers look like? You manage your customers' Windows 10 Enterprise E3 subscriptions by using the Partner Center, which you use for managing other CSP programs. The following sections will walk you through the common tasks that you will perform to set up and manage Windows 10 Enterprise E3 subscriptions for your customers by using the Partner Center.

STEP 1: SIGN IN TO THE PARTNER CENTER

The first step is to sign in to the Partner Center. Use your CSP tenant credentials to perform the following:

1. In Microsoft Edge or Internet Explorer 11, browse to https://partnercenter.microsoft.com, as FIgure 2 shows.

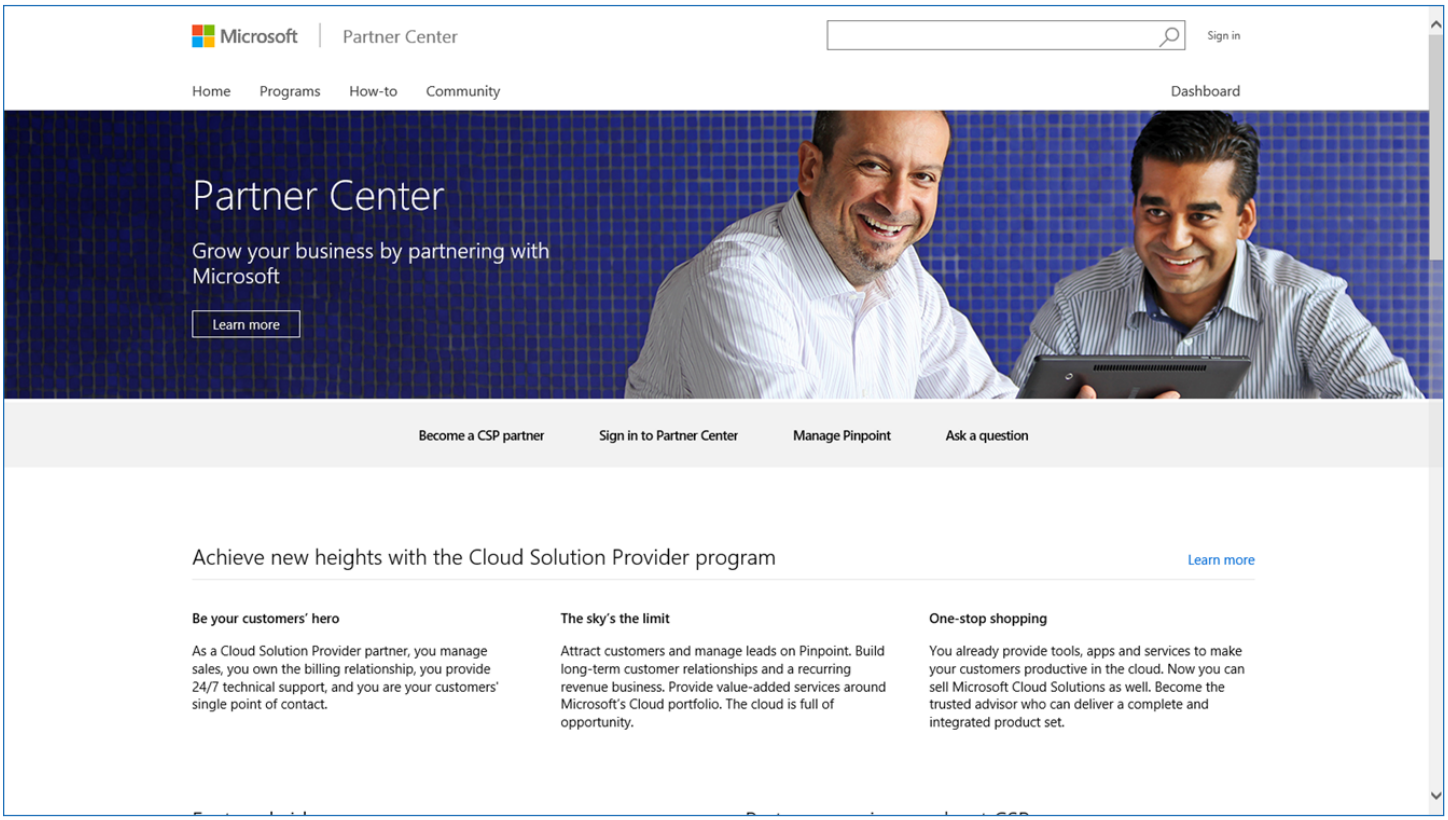

FIgure 2. Partner Center portal

2. In the Partner Center portal, click **Sign in to Partner Center**.

3. Sign in by using your CSP tenant credentials, as illustrated in FIgure 3.

TIP

These are the same credentials that you use in the Partner Admin Center.

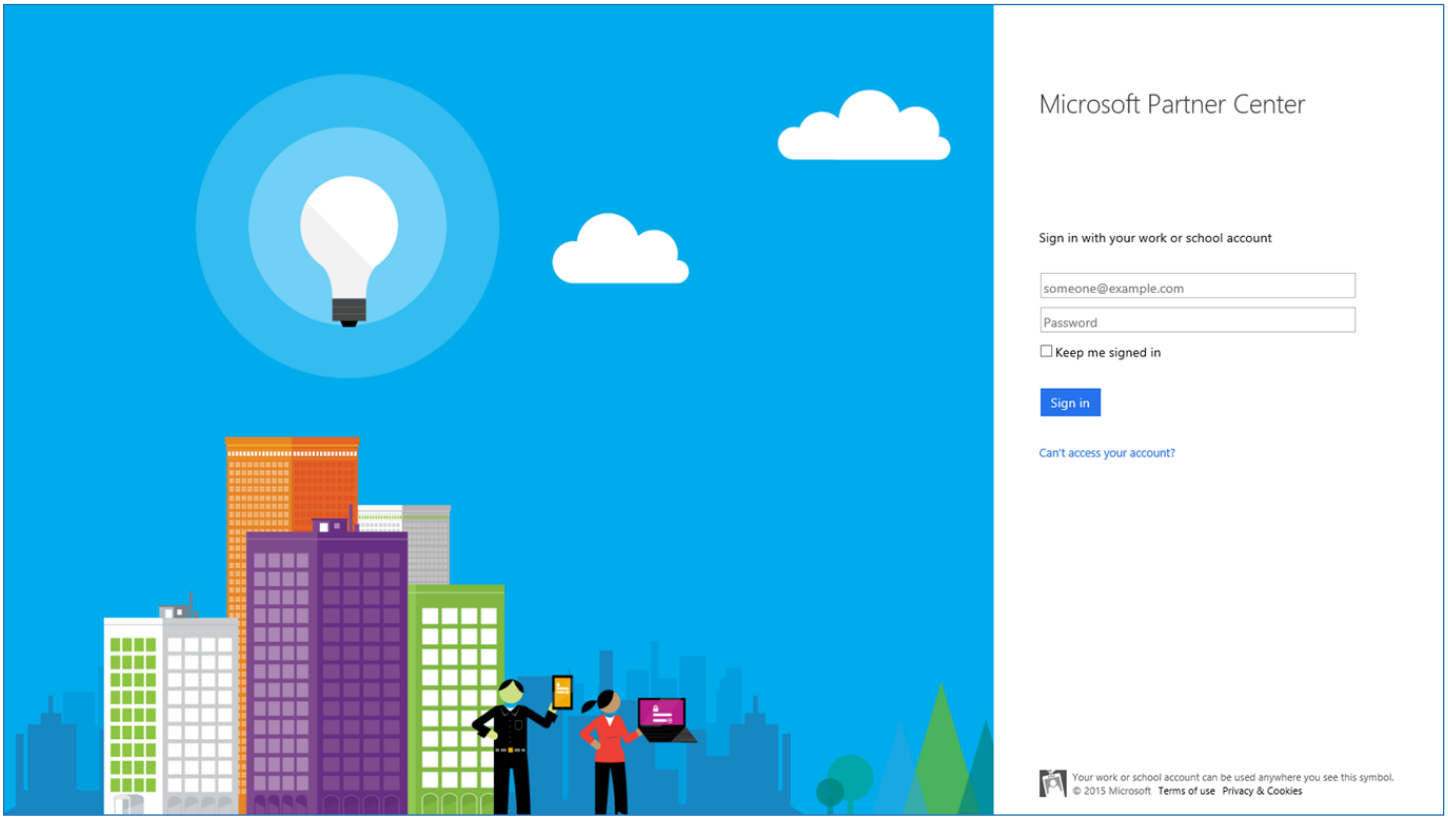

FIgure 3. Microsoft Partner Center portal sign-in page

STEP 2: ADD SUBSCRIPTIONS TO CUSTOMER

After you are signed in to the Partner Center portal, you need to select the Windows 10 Enterprise E3 offering for a client. You will

select the customer and then add the Windows 10 Enterprise E3 offering to the customer by performing the following steps:

1. In the Partner Center portal, in the **Dashboard**, under **Customers**, select the customer, and then click the **Add subscriptions** hyperlink, as FIgure 4 shows.

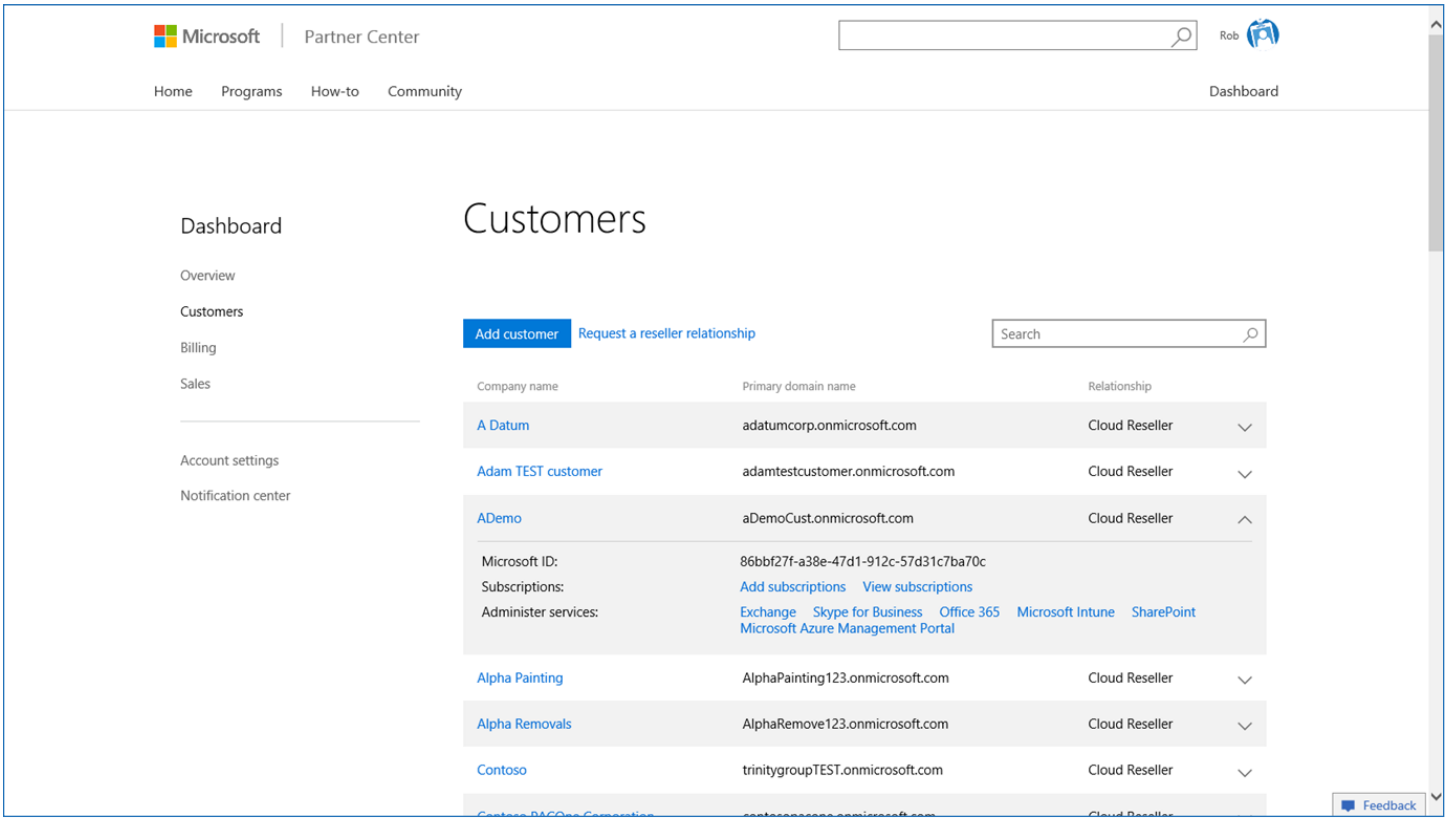

FIgure 4. Customers in the Partner Center portal

2. In the Partner Center portal, in **New subscription**, select the **Windows 10 Enterprise E3** checkbox (and other offerings as required), as illustrated in FIgure 5.

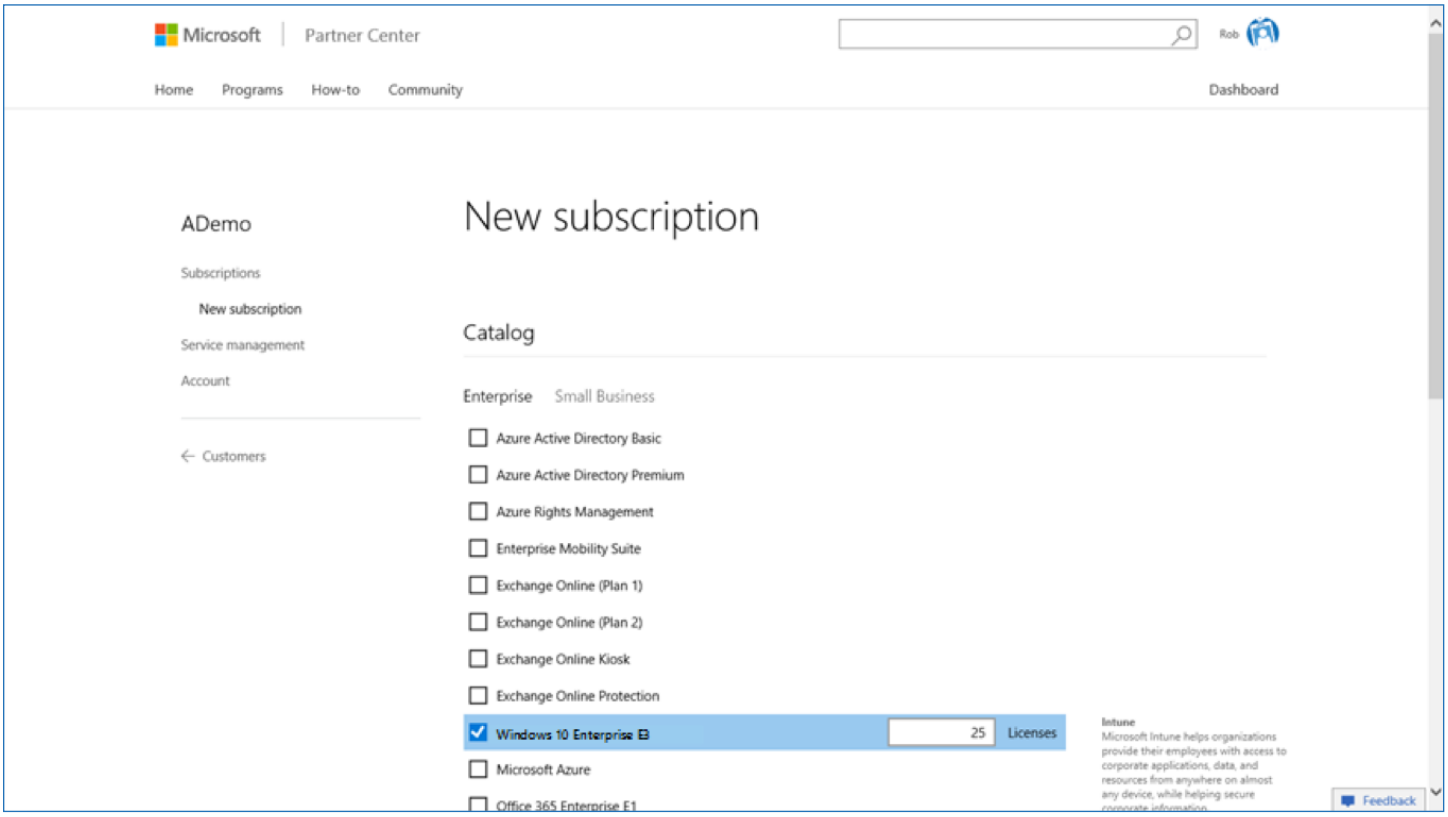

FIgure 5. New subscription for customer in Partner Center portal

3. Once you have added the Windows 10 Enterprise E3 subscription to the customer, the subscription is listed in the **Subscriptions** panel for the customer, as FIgure 6 shows.

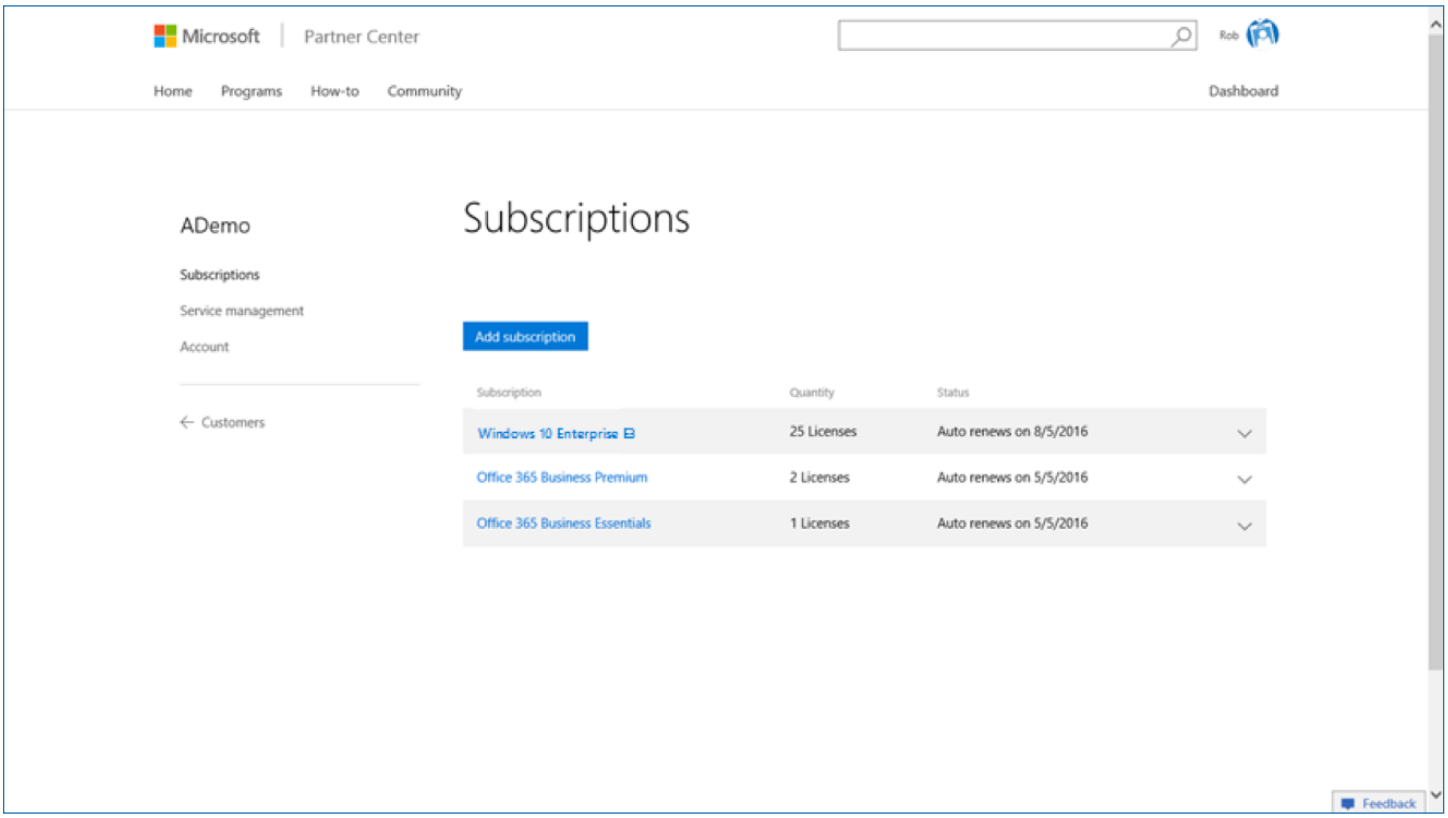

FIgure 6. List of customer subscriptions in the Partner Center portal

In addition, you can add the Windows 10 Enterprise E3 subscription as you create a new customer, as FIgure 7 shows.

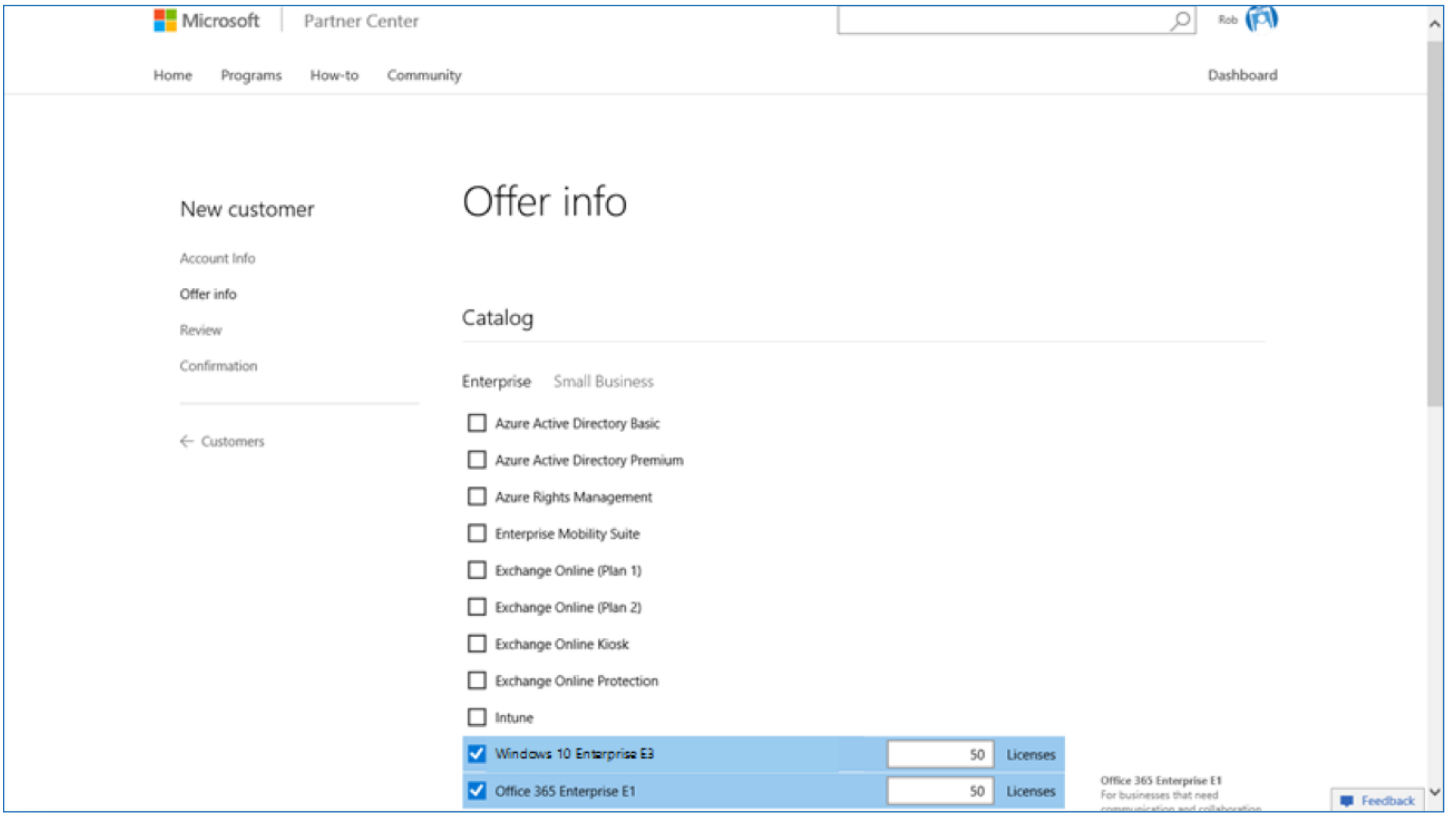

FIgure 7. Adding a Windows 10 Enterprise E3 subscription as you add a new customer in the Partner Center portal

STEP 3: ASSIGN WINDOWS 10 ENTERPRISE E3 LICENSES TO THE CUSTOMER'S USERS

After you have added Windows 10 Enterprise E3 subscriptions (with the appropriate number of licenses), you can then assign the Windows 10 Enterprise E3 licenses to the customer's users. You can assign up to the maximum number of licenses purchased by the customer. You can also dynamically reassign licenses from one user to another user.

Assign Windows 10 Enterprise E3 licenses to users in the Partner

Center portal by performing the following steps:

1. In the Partner Center portal, under the customer, in the **License management** panel, select the user, as illustrated in FIgure 8.

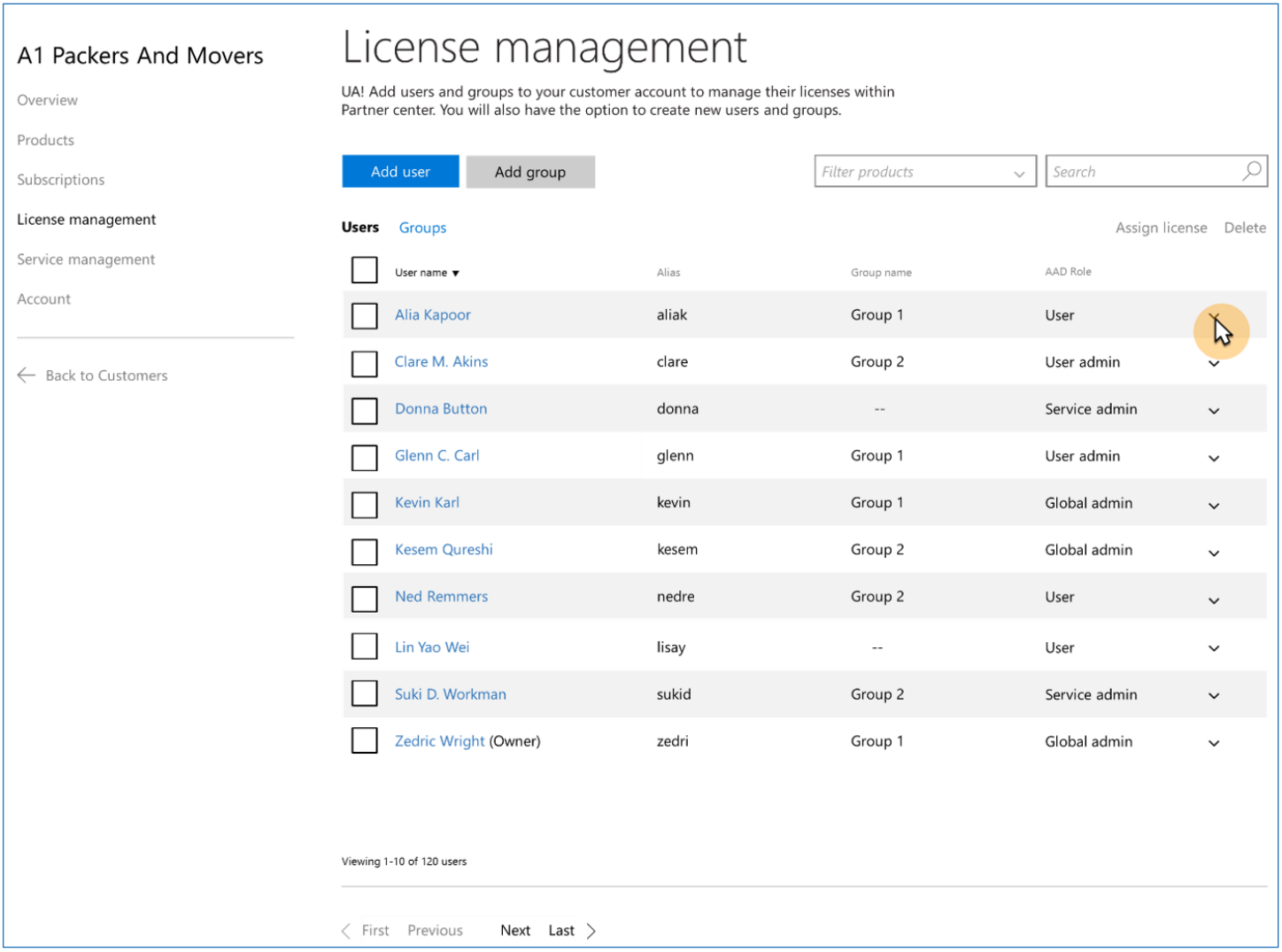

FIgure 8. Select a user to assign license management in Partner Center portal

2. Once you have selected the user, assign a Windows 10 Enterprise E3 license to the user.

You repeat these steps to assign Windows 10 Enterprise E3 licenses to as many users as identified by the customer.

STEP 4: VIEW BILLING INFORMATION

One of the most important tasks that you will want to perform is to view the current billing information for your customers in the Partner Center portal. In the Partner Center portal, in the **Dashboard**, in the **Billing** panel, view your current billing, billing history, and reconciliation files, as illustrated in FIgure 9.

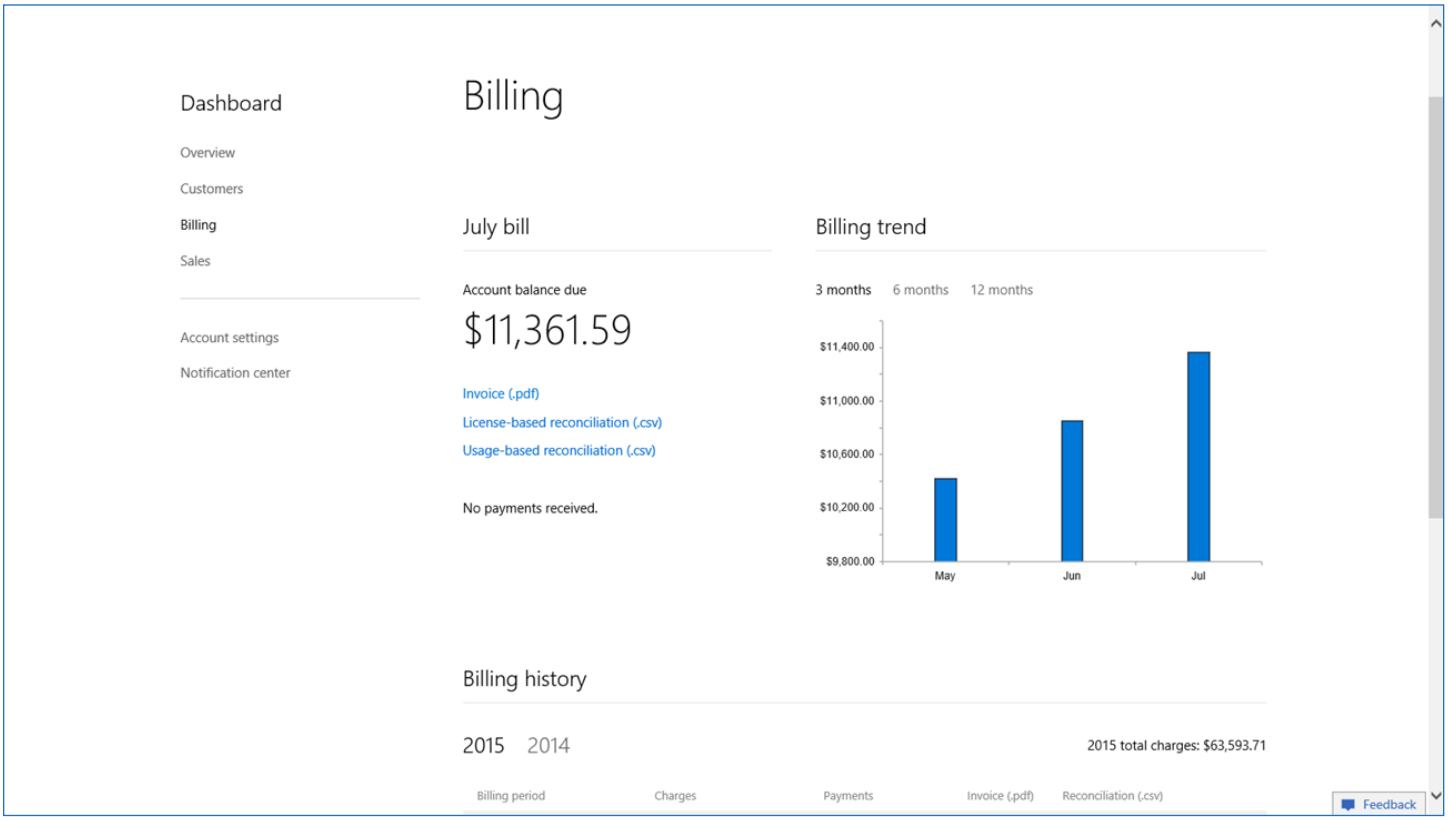

FIgure 9. Billing panel in the Partner Center Dashboard

EXPLORE THE UPGRADE EXPERIENCE

Now that you have managed the customer subscription and assigned Windows 10 Enterprise E3 licenses to users, the users are ready to upgrade their devices running Windows 10 Pro Anniversary Update edition to Windows 10 Enterprise edition. So what will the users experience? How will they upgrade their devices?

STEP 1: JOIN USERS' DEVICES TO AZURE AD

Users can join a device to Azure AD the first time they start the device (during setup), or they can join a Windows 10 Pro Anniversary Update edition device that they already use.

To join a device to Azure AD the first time the device is started, perform the following steps:

1. During the initial setup, on the **Who owns this PC?** page, select **My organization**, and then click **Next**, as illustrated in FIgure 10.

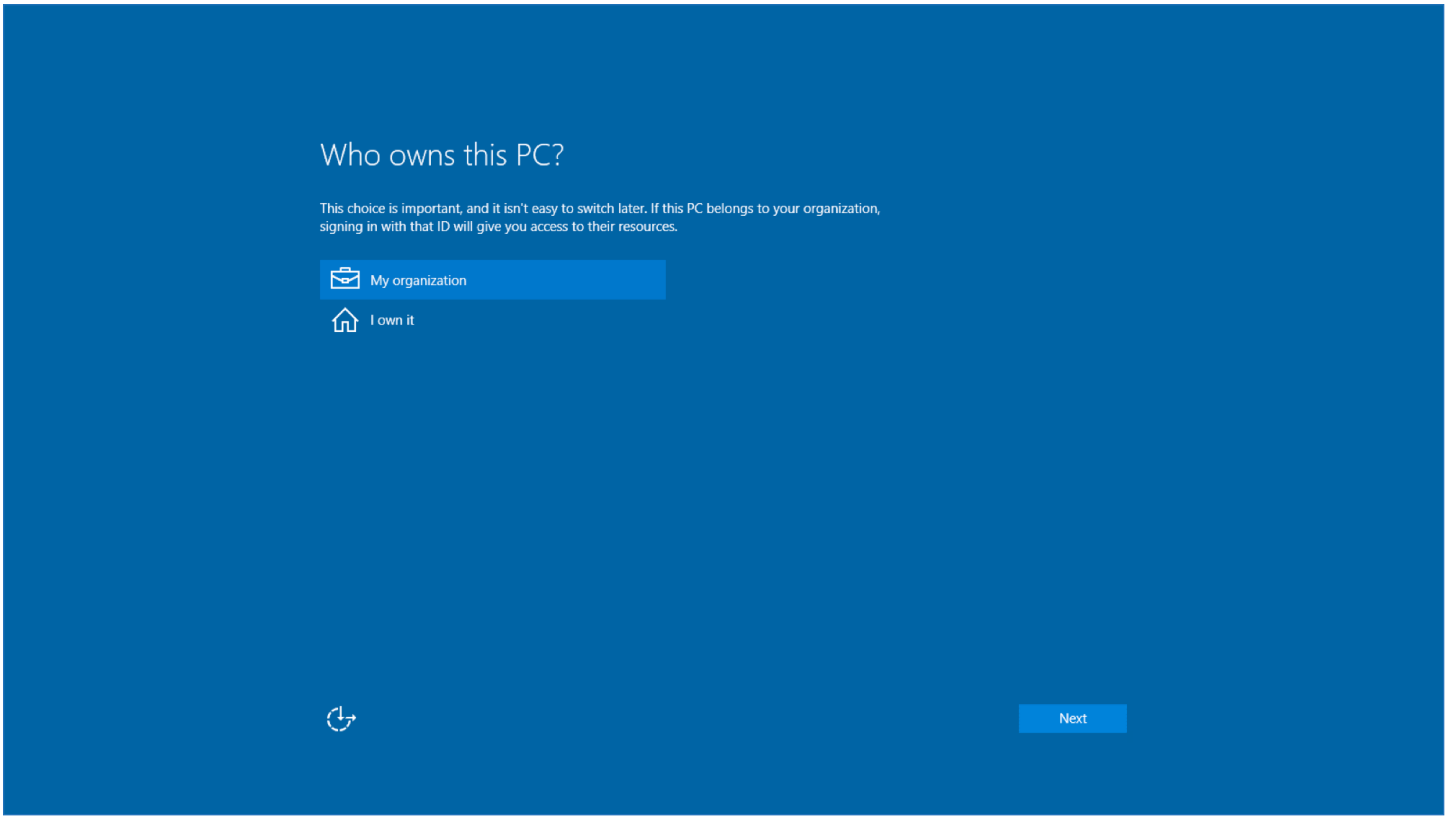

FIgure 10. The "Who owns this PC?" page in initial Windows 10 setup

2. On the **Choose how you'll connect** page, select **Join Azure AD**, and then click **Next**, as illustrated in FIgure 11.

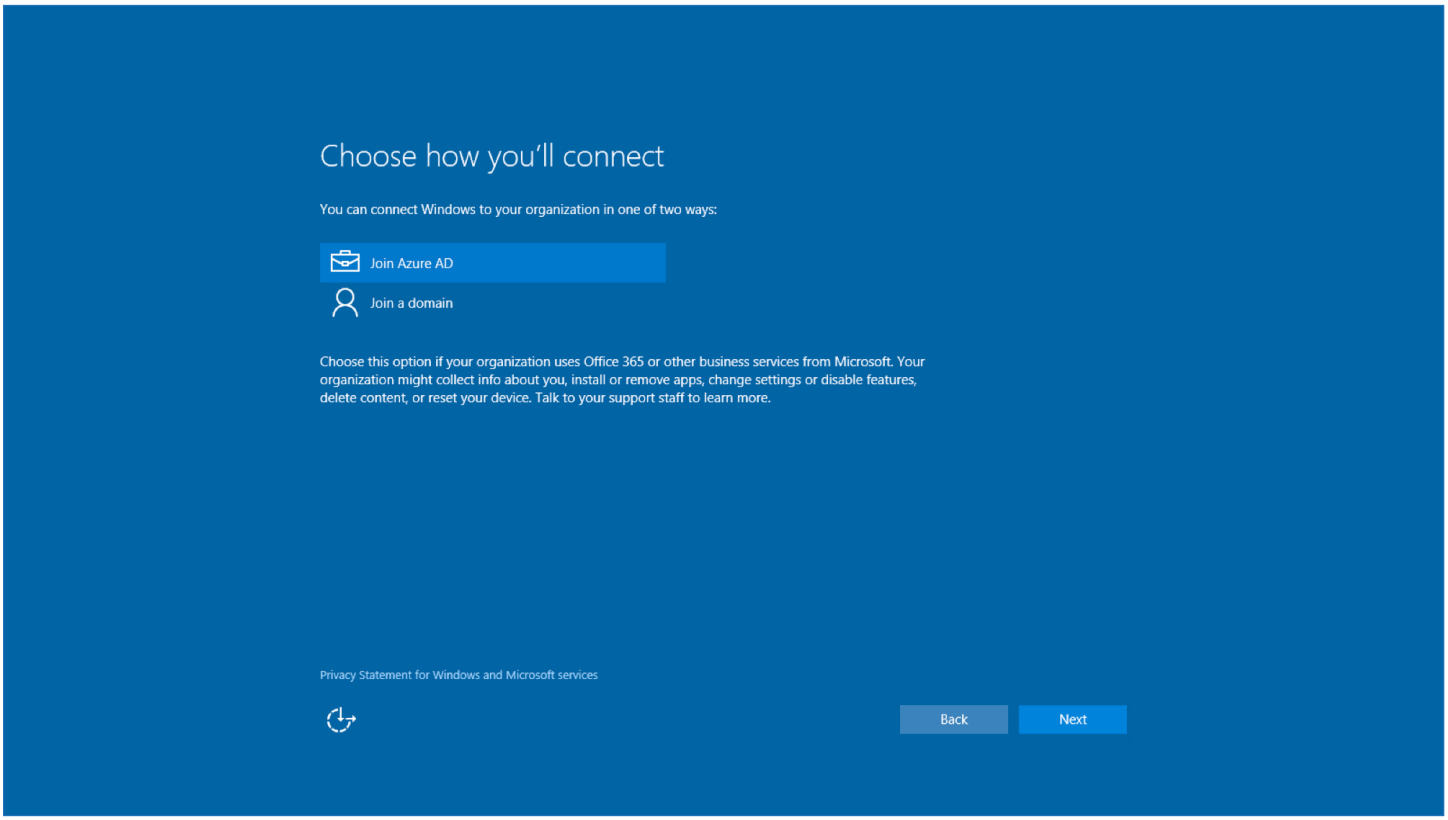

FIgure 11. The "Choose how you'll connect" page in initial Windows 10 setup

3. On the **Let's get you signed in** page, enter the Azure AD credentials, and then click **Sign in**, as illustrated in FIgure 12.

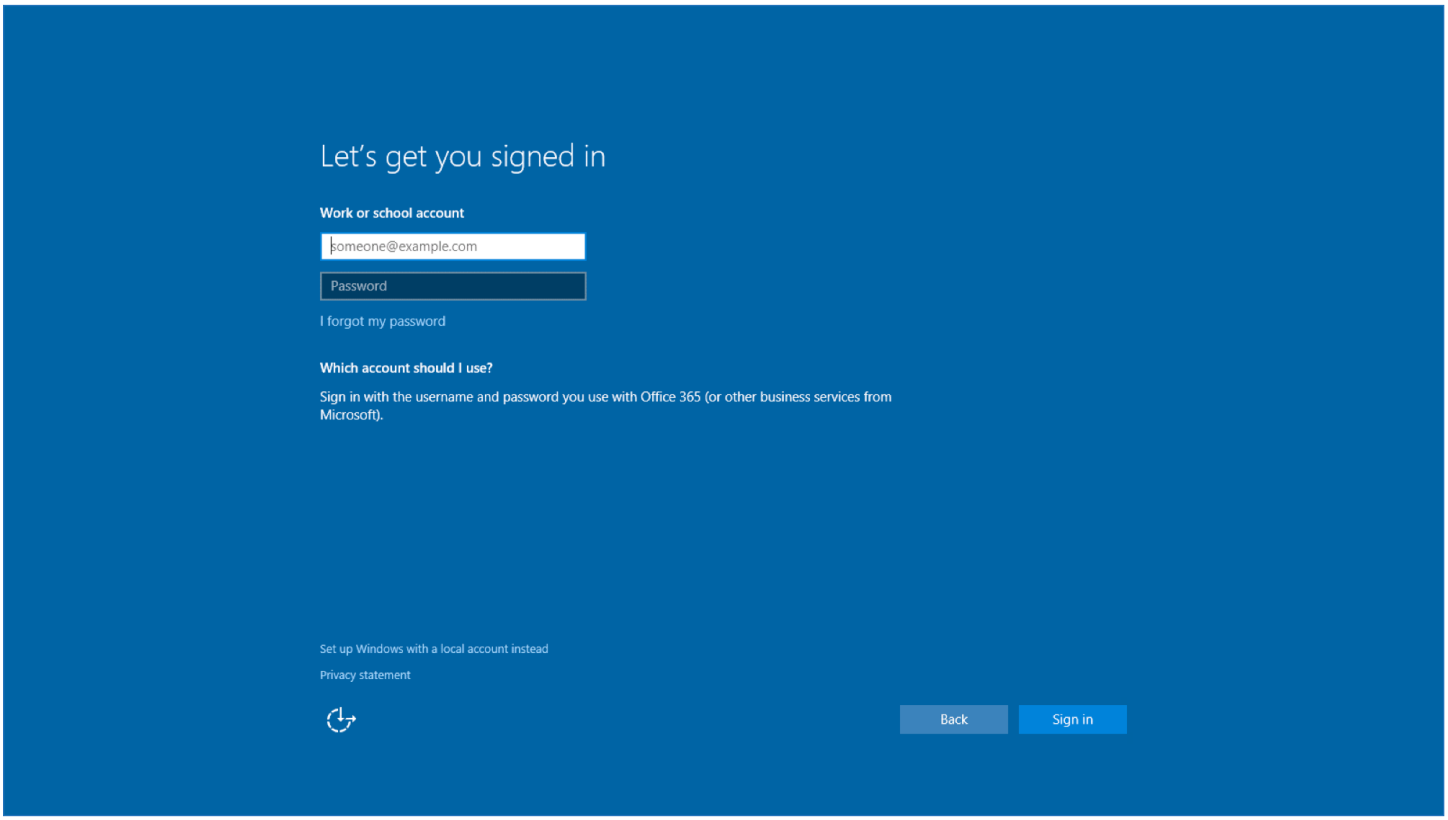

FIgure 12. The "Let's get you signed in" page in initial Windows 10 setup

Now the device is Azure AD joined to the company's subscription.

To join a device to Azure AD when the device already has Windows 10 Pro Anniversary Update edition installed and set up, perform the following steps:

1. Go to **Settings** > **Accounts** > **Access work or school**, as illustrated in FIgure 13.

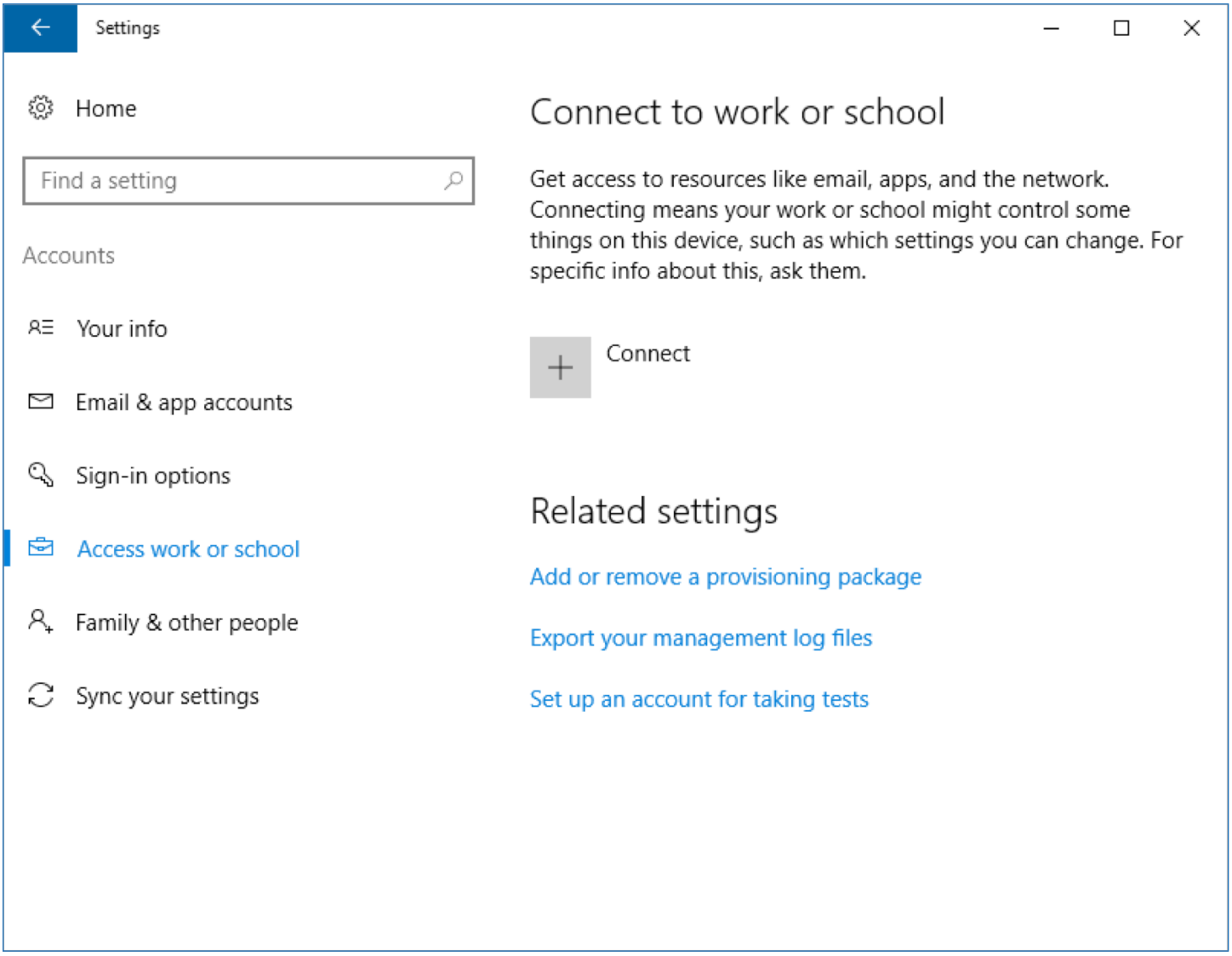

FIgure 13. Connect to work or school configuration in Settings

2. In **Set up a work or school account**, click **Join this device to Azure Active Directory**, as illustrated in FIgure 14.

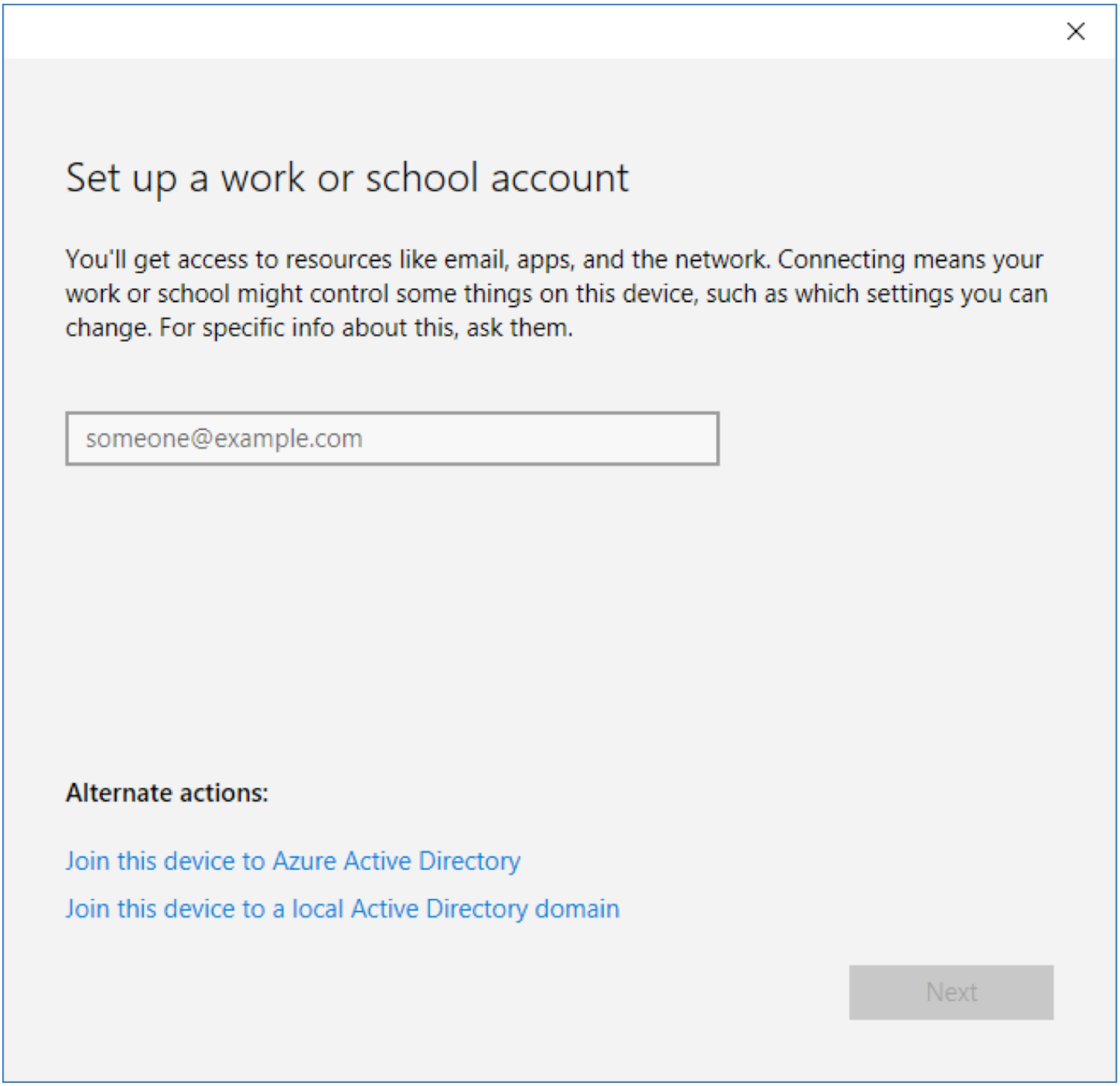

FIgure 14. Set up a work or school account

3. On the **Let's get you signed in** page, enter the Azure AD credentials, and then click **Sign in**, as illustrated in FIgure 15.

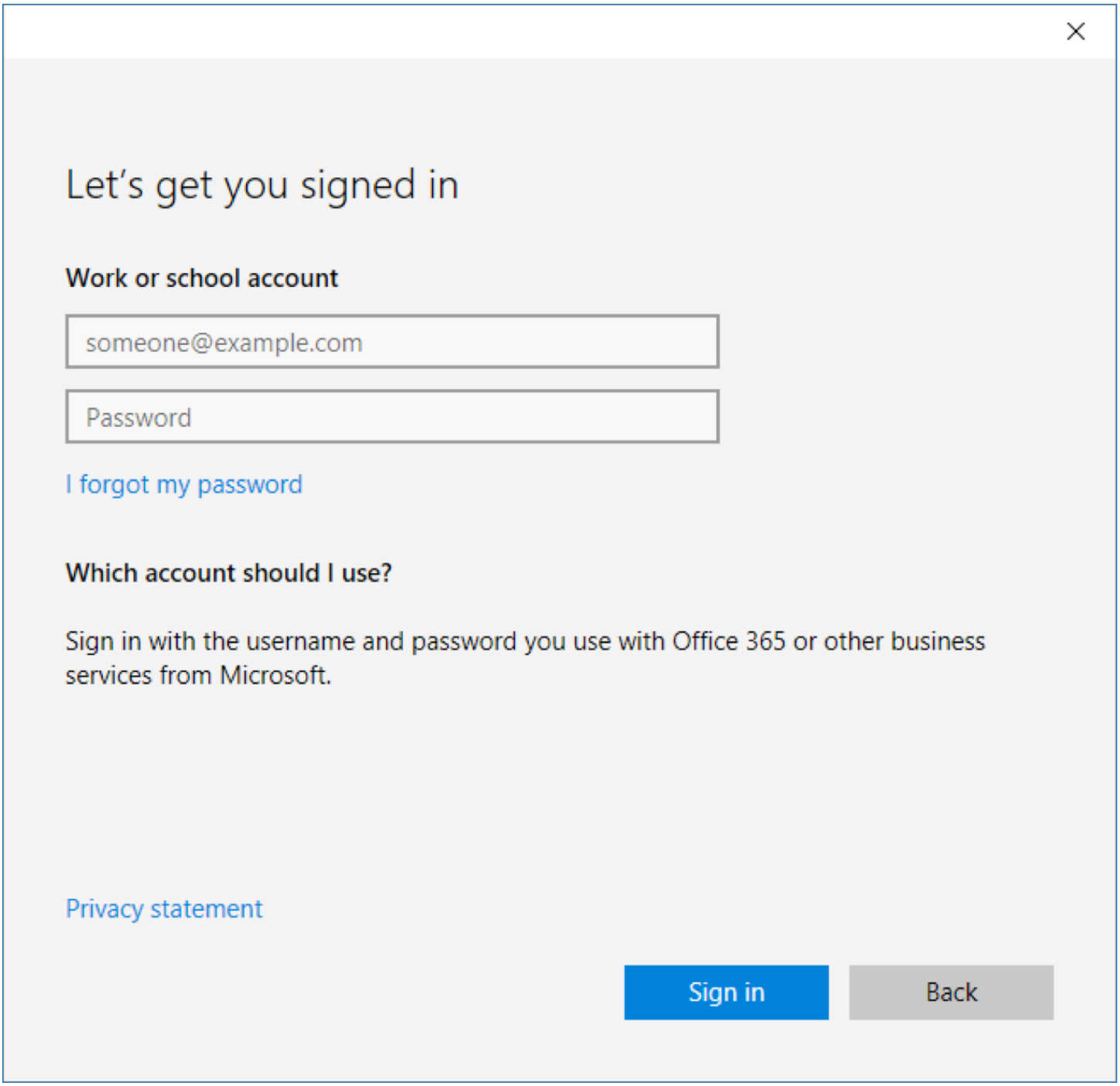

FIgure 15. The "Let's get you signed in" dialog box

Now the device is Azure AD joined to the company's subscription.

STEP 2: SIGN IN USING AZURE AD ACCOUNT

Once the device is joined to the customer's Azure AD subscription, the user will sign in by using his or her Azure AD account, as illustrated in FIgure 16. The Windows 10 Enterprise E3 license associated with the user will enable Windows 10 Enterprise edition capabilities on the device.

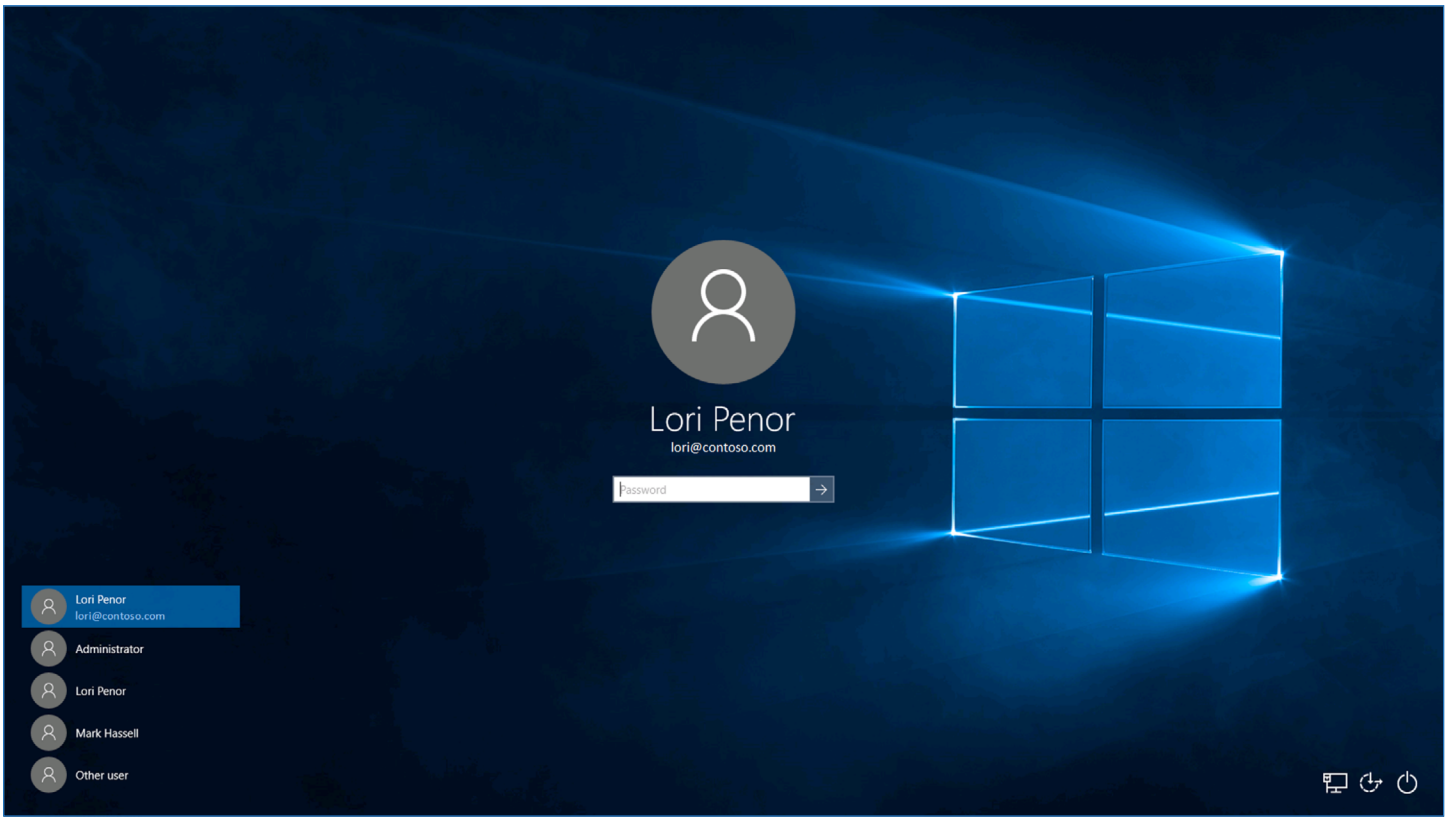

FIgure 16. Sign in by using Azure AD account

STEP 3: VERIFY THAT ENTERPRISE EDITION IS ENABLED

You can verify the Windows 10 Enterprise E3 subscription in **Settings** > **Update & Security** > **Activation**, as FIgure 17 shows.

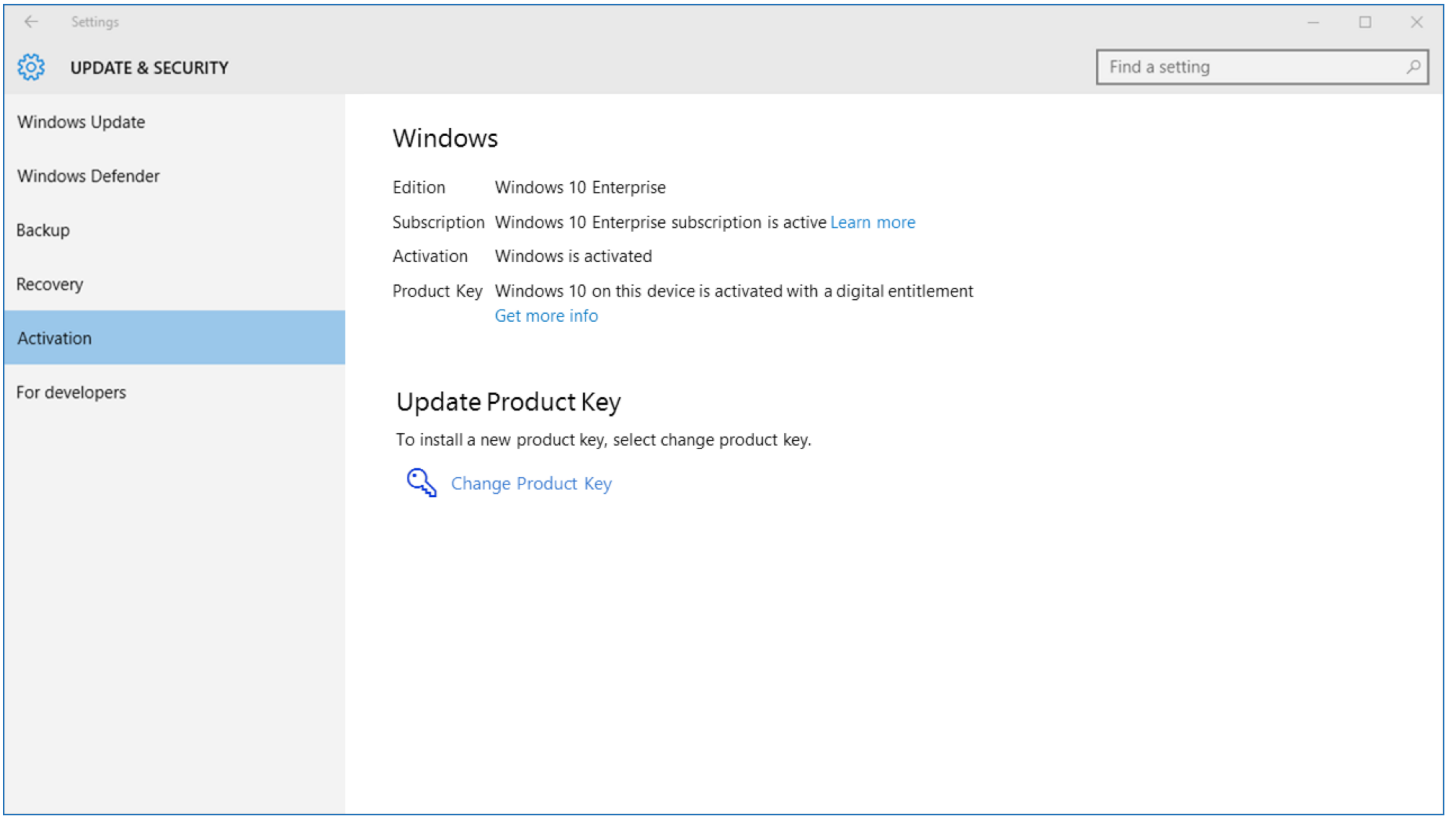

FIgure 17. Windows 10 Enterprise E3 subscription in Settings

If there are any problems with the Windows 10 Enterprise E3 license or the activation of the license, the **Activation** panel will display the appropriate error message or status. You can use this information to help you diagnose the licensing and activation process.

TROUBLESHOOT THE USER EXPERIENCE

In some instances, users may experience problems with the Windows 10 Enterprise E3 subscription. The most common problems that users may experience are as follows:

- The existing Windows 10 Pro Anniversary Update edition license is not activated.
- The Windows 10 Enterprise E3 license has lapsed or has been removed.

Use the following figures to help you troubleshoot when users experience these common problems:

- FIgure 17 on page 29 illustrates a device in a healthy state, where the Windows 10 Pro Anniversary Update edition license is activated and the Windows 10 Enterprise E3 subscription is active.

- FIgure 18 illustrates a device on which the Windows 10 Pro Anniversary Update edition license is not activated, but the Windows 10 Enterprise E3 subscription is active.

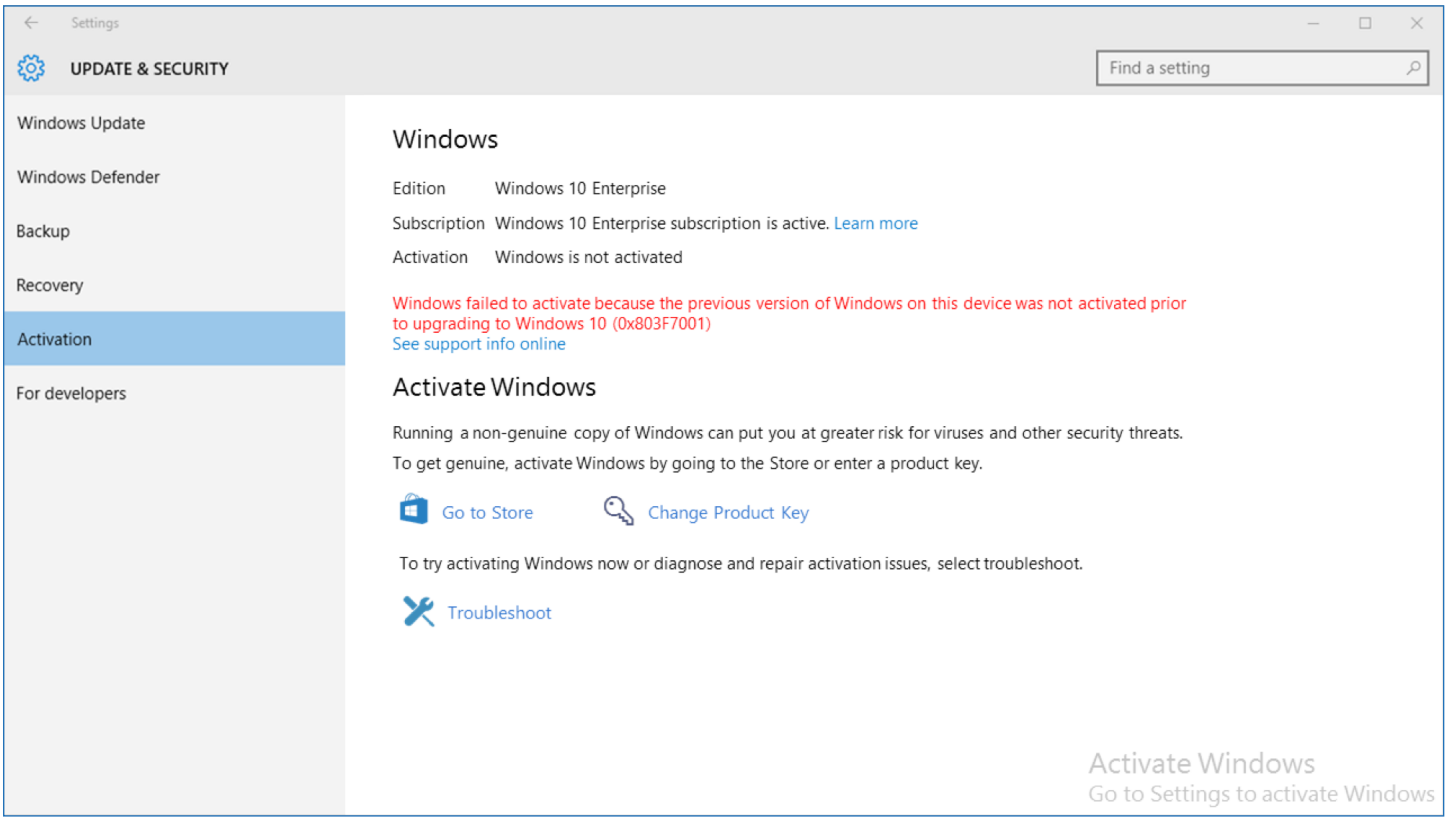

FIgure 18. Windows 10 Pro Anniversary Update edition not activated in Settings

- FIgure 19 illustrates a device on which the Windows 10 Pro Anniversary Update edition license is activated, but the Windows 10 Enterprise E3 subscription is lapsed or removed.

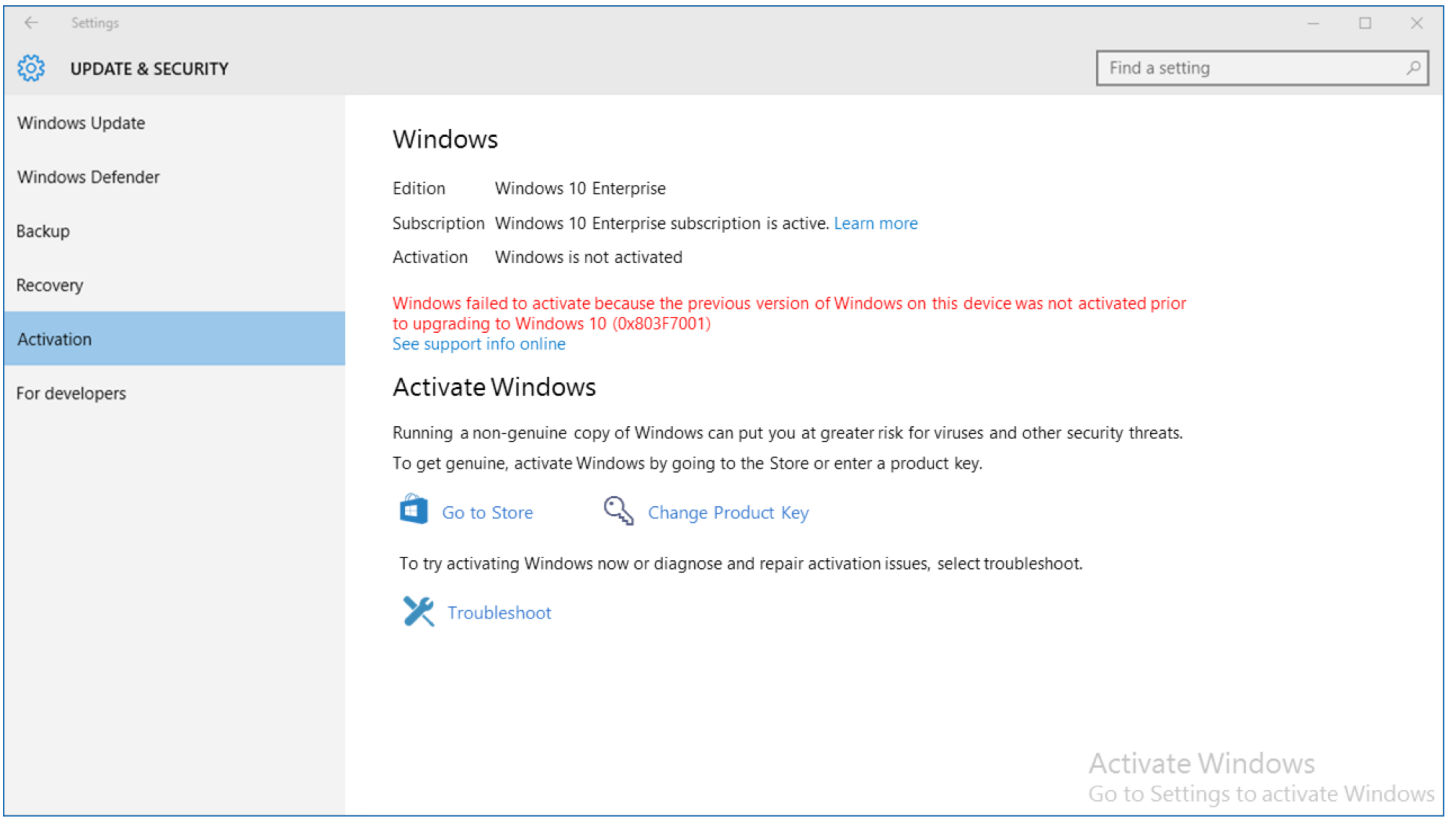

FIgure 19. Windows 10 Enterprise E3 subscription lapsed or removed in Settings

- FIgure 20 illustrates a device on which the Windows 10 Pro Anniversary Update edition license is not activated and the Windows 10 Enterprise E3 subscription is lapsed or removed.

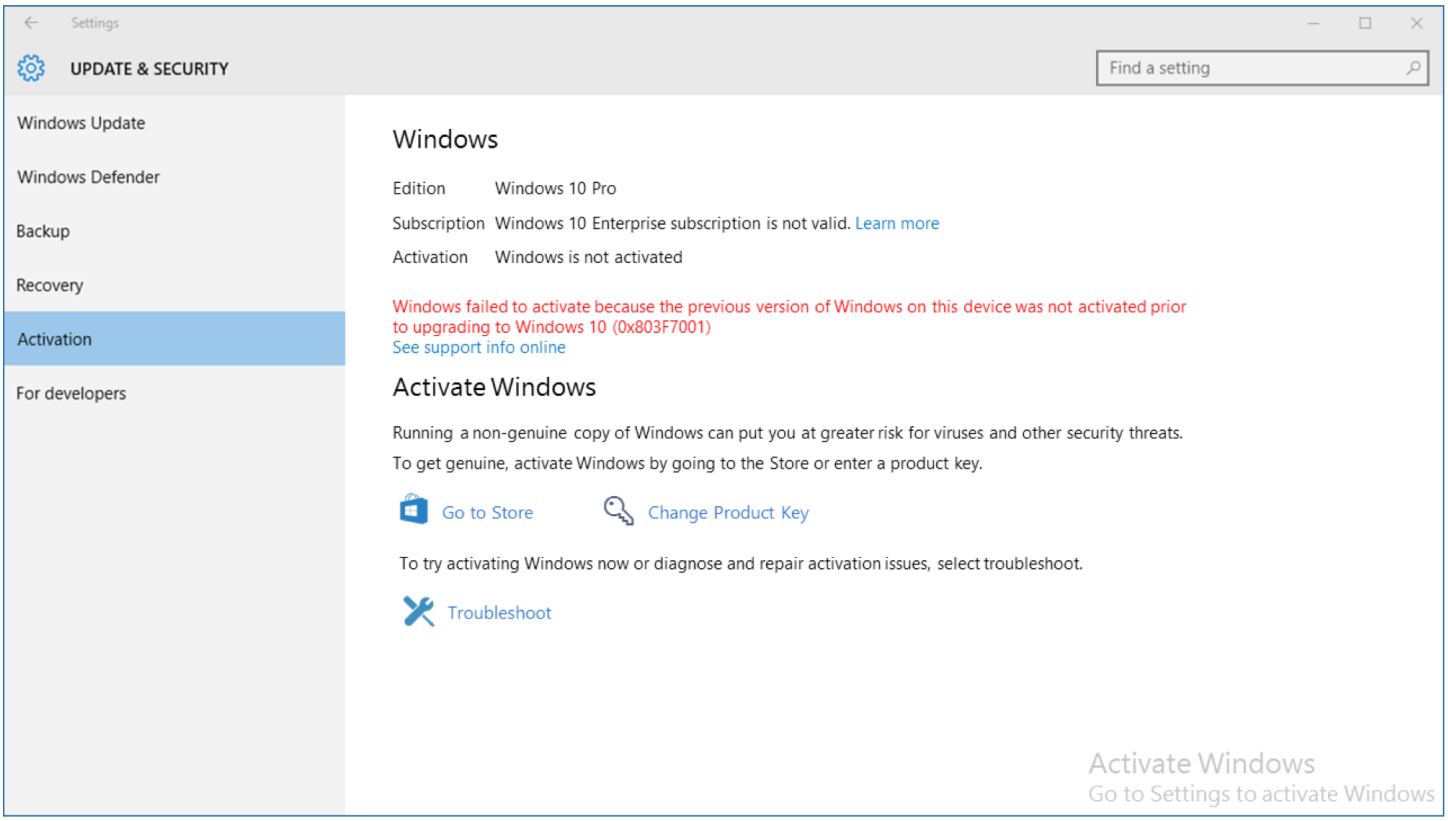

FIgure 20. Windows 10 Pro Anniversary Update edition not activated and Windows 10 Enterprise E3 subscription lapsed or removed in Settings

DEPLOY WINDOWS 10 ENTERPRISE E3 FEATURES

Now that the customer has Windows 10 Enterprise edition running on devices, how does it take full advantage of the Windows 10 Enterprise edition features? What are the next steps that need to be taken for each of the features discussed in the section "Determine which users need Windows 10 Enterprise E3" on page 8?

The following sections provide you with the high-level tasks that need to be performed in the customer's environment to help users take advantage of the Windows 10 Enterprise edition features.

CREDENTIAL GUARD*

You can implement Credential Guard on Windows 10 Enterprise devices by turning on Credential Guard on these devices. Credential Guard uses Windows 10 virtualization-based security features (Hyper-V features) that must be enabled on each device before you

INFORMATION

For more information about implementing Credential Guard, see the following resources:

- Protect derived domain credentials with Credential Guard
- PC OEM requirements for Device Guard and Credential Guard
- Device Guard and Credential Guard hardware readiness tool

* Requires UEFI 2.3.1 or greater with Trusted Boot; Virtualization Extensions such as Intel VT-x, AMD-V, and SLAT must be enabled; x64 version of Windows; IOMMU, such as Intel VT-d, AMD-Vi; BIOS Lockdown; TPM 2.0 recommended for device health attestation (will use software if TPM 2.0 not present)

can turn on Credential Guard. You can turn on Credential Guard by using one of the following methods:

- **Automated.** You can automatically turn on Credential Guard for one or more devices by using Group Policy. The Group Policy settings automatically add the virtualization-based security features and configure the Credential Guard registry settings on managed devices.
- **Manual.** You can manually turn on Credential Guard by doing the following:

    1. Add the virtualization-based security features by using Programs and Features or Deployment Image Servicing and Management (DISM).

    2. Configure Credential Guard registry settings by using the Registry Editor or the Device Guard and Credential Guard hardware readiness tool.

You can automate these manual steps by using a management tool such as System Center Configuration Manager.

DEVICE GUARD

Now that the devices have Windows 10 Enterprise, you can implement Device Guard on the Windows 10 Enterprise devices by performing the following steps:

1. Optionally, create a signing certificate for code integrity policies.

    As you deploy code integrity policies, you might need to sign catalog files or code integrity policies internally. To do this, you will either need a publicly issued code signing certificate (that you purchase) or an internal certificate authority (CA). If you choose to use an internal CA, you will need to create a code signing certificate.

2. Create code integrity policies from "golden" computers.

    When you have identified departments or roles that use distinctive or partly distinctive sets of hardware and software, you can set up "golden" computers containing that software and hardware. In this respect, creating and managing code integrity policies to align with the needs of roles or departments can be similar to managing corporate

INFORMATION

Device Guard deployment guide

images. From each "golden" computer, you can create a code integrity policy and decide how to manage that policy. You can merge code integrity policies to create a broader policy or a master policy, or you can manage and deploy each policy individually.

3. Audit the code integrity policy and capture information about applications that are outside the policy.

   We recommend that you use "audit mode" to carefully test each code integrity policy before you enforce it. With audit mode, no application is blocked—the policy just logs an event whenever an application outside the policy is started. Later, you can expand the policy to allow these applications, as needed.

4. Create a "catalog file" for unsigned line-of-business (LOB) applications.

   Use the Package Inspector tool to create and sign a catalog file for your unsigned LOB applications. In later steps, you can merge the catalog file's signature into your code integrity policy so that applications in the catalog will be allowed by the policy.

5. Capture needed policy information from the event log, and merge information into the existing policy as needed.

   After a code integrity policy has been running for a time in audit mode, the event log will contain information about applications that are outside the policy. To expand the policy so that it allows for these applications, use Windows PowerShell commands to capture the needed policy information from the event log, and then merge that information into the existing policy. You can merge code integrity policies from other sources also, for flexibility in how you create your final code integrity policies.

6. Deploy code integrity policies and catalog files.

   After you confirm that you have completed all the preceding steps, you can begin deploying catalog files and taking code integrity policies out of audit mode. We strongly recommend that you begin this process with a test group of users. This provides a final quality-control validation before you deploy the catalog files and code integrity policies more broadly.

7. Enable desired hardware security features.

Hardware-based security features—also called virtualization-based security (VBS) features—strengthen the protections offered by code integrity policies.

APPLOCKER MANAGEMENT

You can manage AppLocker in Windows 10 Enterprise by using Group Policy. Group Policy requires that the customer have AD DS and that the Windows 10 Enterprise devices are joined to the customer's AD DS domain. You can create AppLocker rules by using Group Policy, and then target those rules to the appropriate devices.

INFORMATION

AppLocker Policies Deployment Guide

APP-V

App-V requires that the customer have an App-V server infrastructure. The primary App-V components that the customer must have are as follows:

- **App-V server.** The App-V server provides App-V management, virtualized app publishing, app streaming, and reporting services. Each of these services can be run on one server or can be run individually on multiple servers. For example, you could have multiple streaming servers. App-V clients contact App-V servers to determine which apps are published to the user or device, and then stream the virtualized app from the server.
- **App-V sequencer.** The App-V sequencer is a typical client device that is used to sequence (capture) apps and prepare them for streaming from the App-V server. You install apps on the App-V sequencer, and the App-V sequencer software determines the files and registry settings that are changed during app installation. Then the sequencer captures these settings to create a virtualized app.
- **App-V client.** The App-V client is installed on any client device that wants to stream apps from the App-V server. These will be the Windows 10 Enterprise E3 devices.

INFORMATION

For more information about implementing the App-V server, App-V sequencer, and App-V client, see the following resources:

- How to Deploy the App-V 5.0 Server
- How to Deploy the App-V Client
- How to Install the Sequencer
- Deploying App-V 5.0

MANAGED USER EXPERIENCE

The Managed User Experience feature is a set of Windows 10 Enterprise edition features and corresponding settings that you can use to manage user experience. Table 4 describes the Managed User Experience settings (by category) which are only available in Windows 10 Enterprise edition. The management methods used to configure each feature depend on the feature. Some features are configured by using Group Policy, while others are configured by using Windows PowerShell, Deployment Image Servicing and Management (DISM), or other command-line tools. For the Group Policy settings, the customer must have AD DS with the Windows 10 Enterprise devices joined to the customer's AD DS domain.

- **Start layout customization.** You can deploy a customized Start layout to users in a domain. No reimaging is required, and the Start layout can be updated simply by overwriting the .xml file that contains the layout. This enables you to customize Start layouts for different departments or organizations, with minimal management overhead.
- **Unbranded boot.** You can suppress Windows elements that appear when Windows starts or resumes and can suppress the crash screen when Windows encounters an error from which it cannot recover.
- **Custom logon.** You can use the Custom Logon feature to suppress Windows 10 UI elements that relate to the Welcome screen and shutdown screen. For example, you can suppress all elements of the Welcome screen UI and provide a custom logon UI. You can also suppress the Blocked Shutdown Resolver (BSDR) screen and automatically end applications while the OS waits for applications to close before a shutdown.
- **Shell launcher.** Enables Assigned Access to run only a classic Windows app via Shell Launcher to replace the shell.
- **Keyboard filter.** You can use Keyboard Filter to suppress undesirable key presses or key combinations. Normally, a customer can use certain Windows key combinations like Ctrl+Alt+Delete or Ctrl+Shift+Tab to control a device by locking the screen or using Task Manager to close a running application. This is not desirable on devices intended for a dedicated purpose.

INFORMATION

For more information about the Managed User Experience features in Windows 10 Enterprise, see:

- Customize Windows 10 Start and taskbar with Group Policy
- Unbranded Boot
- Custom Logon
- Shell Launcher
- Keyboard Filter
- Unified Write Filter

- **Unified write filter.** You can use Unified Write Filter (UWF) on your device to help protect your physical storage media, including most standard writable storage types that are supported by Windows, such as physical hard disks, solid-state drives, internal USB devices, external SATA devices, and so on. You can also use UWF to make read-only media appear to the OS as a writable volume.

CONCLUSION

The Windows 10 Enterprise E3 in CSP program helps you to provide your customers with Windows 10 Enterprise edition so they can take advantage of all the enterprise-level features. You can license from one to hundreds of users, and each user can install Windows 10 Enterprise edition on up to five devices. Also, organizations can roll back to Windows 10 Pro at any time, because of the monthly, per-user subscription model, and they can move licenses between users at any time.

Get involved with the program by taking the following actions:

- **Review technical documentation and other resources.** You can find a full library of resources on the Microsoft Partner Network Portal.
- **Attend a Windows 10 Tech Series event.** Windows 10 Tech Series events provide deeper, in-person technical training on the features, deployment, and management of Windows 10 Enterprise edition. Contact your Microsoft Partner Sales Executive for further information regarding events scheduled in your area.
- **Complete Windows 10 Enterprise sales training.** You can find Windows 10 Enterprise sales training on Windows Drumbeat.

Take advantage of the Windows 10 Enterprise E3 in CSP program to help improve your revenue and increase your customer satisfaction.