Windows 10 Enterprise E3 in CSP

08/23/2017 • 16 minutes to read • +5

In this article

Windows 10 Enterprise E3 launched in the Cloud Solution Provider (CSP) channel on September 1, 2016. Windows 10 Enterprise E3 in CSP is a new offering that delivers, by subscription, exclusive features reserved for Windows 10 Enterprise edition. This offering is available through the Cloud Solution Provider (CSP) channel via the Partner Center as an online service. Windows 10 Enterprise E3 in CSP provides a flexible, per-user subscription for small- and medium-sized organizations (from one to hundreds of users). To take advantage of this offering, you must have the following:

- Windows 10 Pro, version 1607 (Windows 10 Anniversary Update) or later, installed and activated, on the devices to be upgraded
- Azure Active Directory (Azure AD) available for identity management

Starting with Windows 10, version 1607 (Windows 10 Anniversary Update), you can move from Windows 10 Pro to Windows 10 Enterprise more easily than ever before—no keys and no reboots. After one of your users enters the Azure AD credentials associated with a Windows 10 Enterprise E3 license, the operating system turns from Windows 10 Pro to Windows 10 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.

Previously, only organizations with a Microsoft Volume Licensing Agreement 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.

When you purchase Windows 10 Enterprise E3 via a partner, you get the following benefits:

- **Windows 10 Enterprise edition**. Devices currently running Windows 10 Pro, version 1607 can get 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**. 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.
- **Deploy on up to five devices**. For each user covered by the license, you can deploy 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**. 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 you to optimize your licensing investment against changing needs.

How does the Windows 10 Enterprise E3 in CSP program compare with Microsoft Volume Licensing Agreements 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 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.

> In addition, in Windows 10 Enterprise E3 in CSP, a partner can manage your licenses for you. With Software Assurance, you, the customer, manage your 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 access to Windows 10 Enterprise edition.

Compare Windows 10 Pro and Enterprise editions

Windows 10 Enterprise edition has a number of features that are unavailable in Windows 10 Pro. Table 1 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.

Table 1. Windows 10 Enterprise features not found in Windows 10 Pro

Feature	Description

Feature	Description
Credential Guard	This feature uses virtualization-based security to help protect security secrets (for example, 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. • **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. For more information, see Protect derived domain credentials with Credential Guard. *Credential Guard 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)*
Device Guard	This feature is a combination of hardware and software security features that allows only trusted applications to run on a device. Even if an attacker manages to get control of the Windows kernel, he or she will be much less likely to run executable code. Device Guard can use virtualization-based security (VBS) in Windows 10 Enterprise edition to isolate the Code Integrity service from the Windows kernel itself. With VBS, even if malware gains access to the kernel, the effects can be severely limited, because the hypervisor can prevent the malware from executing code. Device Guard does the following: • Helps protect against malware • Helps protect the Windows system core from vulnerability and zero-day exploits • Allows only trusted apps to run For more information, see Introduction to Device Guard.

Feature	Description
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. For more information, see AppLocker.
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. For more information, see Getting Started with App-V for Windows 10.
User Experience Virtualization (UE-V)	With this feature, you can capture user-customized Windows and application settings and store them on a centrally managed network file share. When users log on, their personalized settings are applied to their work session, regardless of which device or virtual desktop infrastructure (VDI) sessions they log on to. UE-V provides the ability to do the following: • Specify which application and Windows settings synchronize across user devices • Deliver the settings anytime and anywhere users work throughout the enterprise • Create custom templates for your third-party or line-of-business applications • Recover settings after hardware replacement or upgrade, or after re-imaging a virtual machine to its initial state For more information, see User Experience Virtualization (UE-V) for Windows 10 overview.

Feature	Description
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

Deployment of Windows 10 Enterprise E3 licenses

See Deploy Windows 10 Enterprise licenses.

Deploy Windows 10 Enterprise features

Now that you have Windows 10 Enterprise edition running on devices, how do you take advantage of the Enterprise edition features and capabilities? What are the next steps that need to be taken for each of the features discussed in Table 1?

The following sections provide you with the high-level tasks that need to be performed in your 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 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:
    - Add the virtualization-based security features by using Programs and Features or Deployment Image Servicing and Management (DISM).
    - 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.

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)*

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 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.

For more information about implementing Device Guard, see:

- Planning and getting started on the Device Guard deployment process
- Device Guard deployment guide

AppLocker management

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

For more information about AppLocker management by using Group Policy, see AppLocker deployment guide.

App-V

App-V requires an App-V server infrastructure to support App-V clients. The primary App-V components that the you 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 run 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 hosting 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 must be enabled on any client device on which apps will be run from the App-V server. These will be the Windows 10 Enterprise E3 devices.

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

- Getting Started with App-V for Windows 10
- Deploying the App-V server
- Deploying the App-V Sequencer and Configuring the Client

UE-V

UE-V requires server- and client-side components that you you'll need to download, activate, and install. These components include:

- **UE-V service**. The UE-V service (when enabled on devices) monitors registered applications and Windows for any settings changes, then synchronizes those settings between devices.

- **Settings packages**. Settings packages created by the UE-V service store application settings and Windows settings. Settings packages are built, locally stored, and copied to the settings storage location.
- **Settings storage location**. This location is a standard network share that your users can access. The UE-V service verifies the location and creates a hidden system folder in which to store and retrieve user settings.
- **Settings location templates**. Settings location templates are XML files that UE-V uses to monitor and synchronize desktop application settings and Windows desktop settings between user computers. By default, some settings location templates are included in UE-V. You can also create, edit, or validate custom settings location templates by using the UE-V template generator. Settings location templates are not required for Windows applications.
- **Universal Windows applications list**. UE-V determines which Windows applications are enabled for settings synchronization using a managed list of applications. By default, this list includes most Windows applications.

For more information about deploying UE-V, see the following resources:

- User Experience Virtualization (UE-V) for Windows 10 overview
- Get Started with UE-V
- Prepare a UE-V Deployment

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 2 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, you must have AD DS with the Windows 10 Enterprise devices joined to your AD DS domain.

Table 2. Managed User Experience features

Feature	Description

Feature	Description
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. For more information on these settings, see Customize Windows 10 Start and taskbar with Group Policy.
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. For more information on these settings, see Unbranded Boot.
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. For more information on these settings, see Custom Logon.
Shell launcher	Enables Assigned Access to run only a classic Windows app via Shell Launcher to replace the shell. For more information on these settings, see Shell Launcher.
Keyboard filter	You can use Keyboard Filter to suppress undesirable key presses or key combinations. Normally, users 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. For more information on these settings, see Keyboard 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. For more information on these settings, see Unified Write Filter.

Related topics

Windows 10 Enterprise Subscription Activation

Connect domain-joined devices to Azure AD for Windows 10 experiences

Compare Windows 10 editions

Windows for business

Is this page helpful?

👍 Yes 👎 No