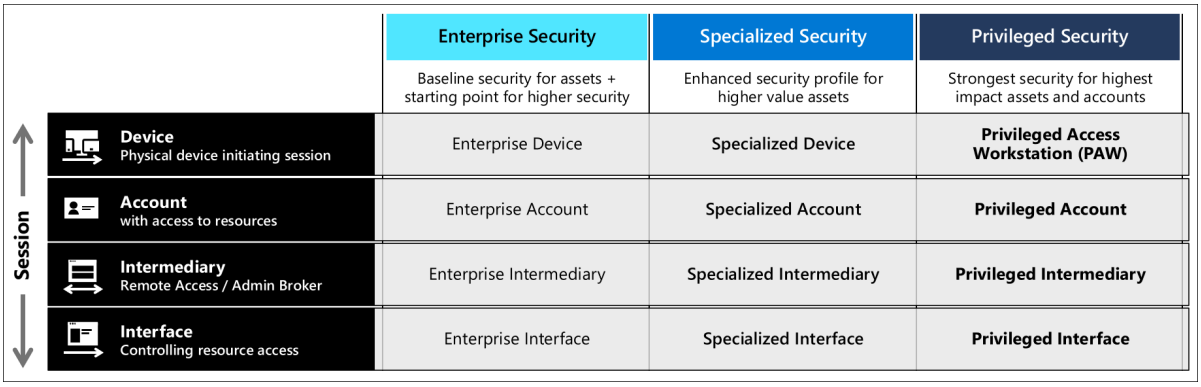
Deploying a privileged access solution - Privileged access

Privileged access deployment

- Article
- 06/20/2024

This document guides you through implementing the technical components of the privileged access strategy, including secure accounts, workstations and devices, and interface security (with conditional access policy).



This guidance sets up all of the profiles for all three security levels and should be assigned your organizations roles based on the Privileged access security levels guidance. Microsoft recommends configuring them in the order described in the rapid modernization plan (RAMP)

License requirements

The concepts covered in this guide assume you have Microsoft 365 Enterprise E5 or an equivalent product. Some of the recommendations in this guide can be implemented with other licenses. For more information, see Microsoft 365 Enterprise licensing.

To automate license provisioning, consider group-based licensing for your users.

Microsoft Entra configuration

Microsoft Entra ID manages users, groups, and devices for your administrator workstations. Enable identity services and features with an administrator account.

When you create the secured workstation administrator account, you expose the account to your current workstation. Make sure you use a known safe device to do this initial configuration and all global configuration. To reduce the attack exposure for the first-time experience, consider following the guidance to prevent malware infections.

Require multifactor authentication, at least for your administrators. See Conditional Access: Require MFA for administrators for implementation guidance.

Microsoft Entra users and groups

1. From the Azure portal, browse to **Microsoft Entra ID** > **Users** > **New user**.

2. Create your device user by following the steps in the create user tutorial.

3. Enter:
    - **Name** - Secure Workstation User
    - **User name** - `secure-ws-user@contoso.com`
    - **Directory role** - **Limited administrator** and select the **Intune Administrator** role.
    - **Usage Location** - For example **United Kingdom**, or your desired location from the list.
4. Select **Create**.

Create your device administrator user.

1. Enter:
    - **Name** - Secure Workstation Administrator
    - **User name** - `secure-ws-admin@contoso.com`
    - **Directory role** - **Limited administrator** and select the **Intune Administrator** role.
    - **Usage Location** - For example **United Kingdom**, or your desired location from the list.
2. Select **Create**.

Next, you create four groups: **Secure Workstation Users**, **Secure Workstation Admins**, **Emergency BreakGlass** and **Secure Workstation Devices**.

From the Azure portal, browse to **Microsoft Entra ID** > **Groups** > **New group**.

1. For the workstation users group, you might want to configure group-based licensing to automate provisioning of licenses to users.
2. For the workstation users group, enter:
    - **Group type** - Security
    - **Group name** - Secure Workstation Users
    - **Membership type** - Assigned
3. Add your secure workstation user: `secure-ws-user@contoso.com`
4. You can add any other users that use secure workstations.
5. Select **Create**.
6. For the Privileged Workstation Admins group, enter:
    - **Group type** - Security
    - **Group name** - Secure Workstation Admins
    - **Membership type** - Assigned
7. Add your secure workstation user: `secure-ws-admin@contoso.com`
8. You can add any other users that manage secure workstations.
9. Select **Create**.
10. For the Emergency BreakGlass group, enter:
    - **Group type** - Security
    - **Group name** - Emergency BreakGlass
    - **Membership type** - Assigned
11. Select **Create**.
12. Add Emergency Access accounts to this group.

13. For the workstation devices group, enter:
    - **Group type** - Security
    - **Group name** - Secure Workstation Devices
    - **Membership type** - Dynamic Device
    - **Dynamic Membership rules** - `(device.devicePhysicalIds -any _ -contains "[OrderID]:PAW")`
14. Select **Create**.

Microsoft Entra device configuration

Specify who can join devices to Microsoft Entra ID

Configure your devices setting in Active Directory to allow your administrative security group to join devices to your domain. To configure this setting from the Azure portal:

1. Go to **Microsoft Entra ID** > **Devices** > **Device settings**.
2. Choose **Selected** under **Users may join devices to Microsoft Entra ID**, and then select the "Secure Workstation Users" group.

Remove local admin rights

This method requires that users of the VIP, DevOps, and Privileged workstations have no administrator rights on their machines. To configure this setting from the Azure portal:

1. Go to **Microsoft Entra ID** > **Devices** > **Device settings**.
2. Select **None** under **Additional local administrators on Microsoft Entra joined devices**.

Refer to How to manage the local administrators group on Microsoft Entra joined devices for details on how to manage members of the local administrators group.

Require multifactor authentication to join devices

To further strengthen the process of joining devices to Microsoft Entra ID:

1. Go to **Microsoft Entra ID** > **Devices** > **Device settings**.
2. Select **Yes** under **Require Multi-Factor Auth to join devices**.
3. Select **Save**.

Configure mobile device management

From the Azure portal:

1. Browse to **Microsoft Entra ID** > **Mobility (MDM and MAM)** > **Microsoft Intune**.
2. Change the **MDM user scope** setting to **All**.
3. Select **Save**.

These steps allow you to manage any device with Microsoft Endpoint Manager. For more information, see Intune Quickstart: Set up automatic enrollment for Windows 10 devices. You create Intune configuration and compliance policies in a future step.

Microsoft Entra Conditional Access

Microsoft Entra Conditional Access can help restrict privileged administrative tasks to compliant devices. Predefined members of the **Secure Workstation Users** group are required to perform multifactor authentication when signing in to cloud applications. A best practice is to exclude emergency access accounts from the policy. For more information, see Manage emergency access accounts in Microsoft Entra ID.

Conditional Access only allowing secured workstation ability to access Azure portal

Organizations should block Privileged Users from being able to connect to cloud management interfaces, portals, and PowerShell, from non-PAW devices.

To block unauthorized devices from being able to access cloud management interfaces, follow the guidance in the article Conditional Access: Filters for Devices (preview). It's essential that while deploying this feature you consider, emergency access account functionality. These accounts should be used only for extreme cases and the account managed through policy.

Note

You will need to create a user group, and include your emergency user that can bypass the Conditional Access policy. For our example we have a security group called **Emergency BreakGlass**

This policy set ensures that your Administrators must use a device that is able to present a specific device attribute value, that MFA is satisfied, and the device is marked as compliant by Microsoft Endpoint Manager and Microsoft Defender for Endpoint.

Organizations should also consider blocking legacy authentication protocols in their environments. For more information about blocking legacy authentication protocols, see the article, How to: Block legacy authentication to Microsoft Entra ID with Conditional Access.

Microsoft Intune configuration

Device enrollment deny BYOD

In our sample, we recommend that BYOD devices not be permitted. Using Intune BYOD enrollment allows users to enroll devices that are less, or not trusted. However it's important to note that in organizations that have a limited budget to purchase new devices, looking to use existing hardware fleet, or considering non-windows devices, might consider the BYOD capability in Intune to deploy the Enterprise profile.

The following guidance configures enrollment for deployments that deny BYOD access.

Set enrollment restrictions preventing BYOD

1. In the Microsoft Intune admin center, choose > **Devices** > **Enrollment restrictions** > choose the default restriction **All Users**
2. Select **Properties** > Platform settings **Edit**
3. Select **Block** for All types, except Windows MDM.
4. Select **Block** for all Personally owned items.

Create an Autopilot deployment profile

After creating a device group, you must create a deployment profile to configure the Autopilot devices.

1. In the Microsoft Intune admin center, choose **Device enrollment** > **Windows enrollment** > **Deployment Profiles** > **Create Profile**.

2. Enter:

    - Name - **Secure workstation deployment profile**.
    - Description - **Deployment of secure workstations**.
    - Set **Convert all targeted devices to Autopilot** to **Yes**. This setting makes sure that all devices in the list get registered with the Autopilot deployment service. Allow 48 hours for the registration to be processed.

3. Select **Next**.
    - For **Deployment mode**, choose **Self-Deploying (Preview)**. Devices with this profile are associated with the user who enrolls the device. During the deployment, it's advisable to use the Self-Deployment mode features to include:
        - Enrolls the device in Intune Microsoft Entra automatic MDM enrollment, and only allow for a device to be accessed until all policies, applications, certificates, and networking profiles are provisioned on the device.
        - User credentials are required to enroll the device. It's essential to note that deploying a device in the **Self-Deploying** mode allows you to deploy laptops in a shared model. No user assignment happens until the device is assigned to a user for the first time. As a result, any user policies such as BitLocker won't be enabled until a user assignment is completed. For more information about how to sign in to a secured device, see selected profiles.
    - Select your Language (Region), User account type **standard**.
4. Select **Next**.

    Select a scope tag if you have preconfigured one.
5. Select **Next**.
6. Choose **Assignments** > **Assign to** > **Selected Groups**. In **Select groups to include**, choose **Secure Workstation Devices**.
7. Select **Next**.
8. Select **Create** to create the profile. The Autopilot deployment profile is now available to assign to devices.

Device enrollment in Autopilot provides a different user experience based on device type and role. In our deployment example, we illustrate a model where the secured devices are bulk deployed and can be shared, but when used for the first time, the device is assigned to a user. For more information, see Intune Autopilot device enrollment.

Enrollment Status Page

The Enrollment Status Page (ESP) displays provisioning progress after a new device is enrolled. To ensure that devices are fully configured before use, Intune provides a means to **Block device use until all apps and profiles are installed**.

Create and assign enrollment status page profile

1. In the Microsoft Intune admin center, choose **Devices** > **Windows** > **Windows enrollment** > **Enrollment Status Page** > **Create profile**.
2. Provide a **Name** and **Description**.
3. Choose **Create**.
4. Choose the new profile in the **Enrollment Status Page** list.
5. Set **Show app profile installation progress** to **Yes**.
6. Set **Block device use until all apps and profiles are installed** to **Yes**.
7. Choose **Assignments** > **Select groups** > choose `Secure Workstation` group > **Select** > **Save**.
8. Choose **Settings** > choose the settings you want to apply to this profile > **Save**.

Configure Windows Update

Keeping Windows 10 up to date is one of the most important things you can do. To maintain Windows in a secure state, you deploy an update ring to manage the pace that updates are applied to workstations.

This guidance recommends that you create a new update ring and change the following default settings:

1. In the Microsoft Intune admin center, choose **Devices** > **Software updates** > **Windows 10 Update Rings**.

2. Enter:

    - Name - **Azure-managed workstation updates**
    - Servicing channel - **Semi-annual channel**
    - Quality update deferral (days) - **3**
    - Feature update deferral period (days) - **3**
    - Automatic update behavior - **Auto install and reboot without end-user control**
    - Block user from pausing Windows updates - **Block**
    - Require user's approval to restart outside of work hours - **Required**
    - Allow user to restart (engaged restart) - **Required**
    - Transition users to engaged restart after an auto-restart (days) - **3**
    - Snooze engaged restart reminder (days) - **3**
    - Set deadline for pending restarts (days) - **3**
3. Select **Create**.

4. On the **Assignments** tab, add the **Secure Workstations** group.

For more information about Windows Update policies, see Policy CSP - Update.

Microsoft Defender for Endpoint Intune integration

Microsoft Defender for Endpoint and Microsoft Intune work together to help prevent security breaches. They can also limit the impact of breaches. These capabilities provide real-time threat detection and enable extensive auditing and logging of the end-point devices.

To configure integration of Windows Defender for Endpoint and Microsoft Endpoint Manager:

1. In the Microsoft Intune admin center, choose **Endpoint Security** > **Microsoft Defender ATP**.

2. In step 1 under **Configuring Windows Defender ATP**, select **Connect Windows Defender ATP to Microsoft Intune in the Windows Defender Security Center**.

3. In the Windows Defender Security Center:

    1. Select **Settings** > **Advanced features**.
    2. For **Microsoft Intune connection**, choose **On**.
    3. Select **Save preferences**.
4. After a connection is established, return to Microsoft Endpoint Manager and select **Refresh** at the top.

5. Set **Connect Windows devices version(20H2) 19042.450 and above to Windows Defender ATP** to **On**.

6. Select **Save**.

Create the device configuration profile to onboard Windows devices

1. Sign in to the Microsoft Intune admin center, choose **Endpoint security** > **Endpoint detection and response** > **Create profile**.

2. For **Platform**, select **Windows 10 and Later**.

3. For **Profile type**, select **Endpoint detection and response**, and then select **Create**.

4. On the **Basics** page, enter a *PAW - Defender for Endpoint* in the Name field and *Description* (optional) for the profile, then choose **Next**.

5. On the **Configuration settings** page, configure the following option in **Endpoint Detection and Response**:

   Sample sharing for all files: Returns or sets the Microsoft Defender Advanced Threat Protection Sample Sharing configuration parameter.

   Onboard Windows 10 machines using Microsoft Endpoint Configuration Manager has more details on these Microsoft Defender ATP settings.

6. Select **Next** to open the **Scope tags** page. Scope tags are optional. Select **Next** to continue.

7. On the **Assignments** page, select *Secure Workstation* group. For more information on assigning profiles, see Assign user and device profiles.

   Select **Next**.

8. On the **Review + create** page, when you're done, choose **Create**. The new profile is displayed in the list when you select the policy type for the profile you created. **OK**, and then **Create** to save your changes, which creates the profile.

For more information, see Windows Defender Advanced Threat Protection.

Finish workstation profile hardening

To successfully complete the hardening of the solution, download and execute the appropriate script. Find the download links for your desired **profile level**:

Profile	Download location	Filename
Enterprise	https://aka.ms/securedworkstationgit	`Enterprise-Workstation-Windows10-(20H2).ps1`
Specialized	https://aka.ms/securedworkstationgit	`Specialized-Windows10-(20H2).ps1`
Privileged	https://aka.ms/securedworkstationgit	`Privileged-Windows10-(20H2).ps1`

Note

The removal of of admin rights and access, as well as, Application execution control (AppLocker) are managed by the policy profiles that are deployed.

After the script successfully executes, you can make updates to profiles and policies in Intune. The scripts create policies and profiles for you, but you must assign the policies to your **Secure Workstations** device group.

- Here's where you can find the Intune device configuration profiles created by the scripts: **Azure portal** > **Microsoft Intune** > **Device configuration** > **Profiles**.
- Here's where you can find the Intune device compliance policies created by the scripts: **Azure portal** > **Microsoft Intune** > **Device Compliance** > **Policies**.

Run the Intune data export script `DeviceConfiguration_Export.ps1` from the DeviceConfiguration GitHub repository to export all current Intune profiles for comparison, and evaluation of the profiles.

Set rules in the Endpoint Protection Configuration Profile for Microsoft Defender Firewall

Windows Firewall policy settings are included in the Endpoint Protection Configuration Profile. The behavior of the policy applied in described in the following table.

Profile	Inbound Rules	Outbound Rules	Merge behavior
Enterprise	Block	Allow	Allow
Specialized	Block	Allow	Block
Privileged	Block	Block	Block

Enterprise: This configuration is the most permissive as it mirrors the default behavior of a Windows Install. All inbound traffic is blocked except for rules that are explicitly defined in the local policy rules as merging of local rules is set to allowed. All outbound traffic is allowed.

Specialized: This configuration is more restrictive as it ignores all locally defined rules on the device. All inbound traffic is blocked including locally defined rules the policy includes two rules to allow Delivery Optimization to function as designed. All outbound traffic is allowed.

Privileged: All inbound traffic is blocked including locally defined rules the policy includes two rules to allow Delivery Optimization to function as designed. Outbound traffic is also blocked apart from explicit rules that allow DNS, DHCP, NTP, NSCI, HTTP, and HTTPS traffic. This configuration not only reduces the attack surface presented by the device to the network it limits the outbound connections that the device can establish to only those connections required to administer cloud services.

Rule	Direction	Action	Application / Service	Protocol	Local Ports	Remote Ports
World Wide Web Services (HTTP Traffic-out)	Outbound	Allow	All	TCP	All ports	80
World Wide Web Services (HTTPS Traffic-out)	Outbound	Allow	All	TCP	All ports	443
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	546	547
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)	Outbound	Allow	Dhcp	TCP	546	547
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCP-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	68	67

Rule	Direction	Action	Application / Service	Protocol	Local Ports	Remote Ports
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCP-Out)	Outbound	Allow	Dhcp	TCP	68	67
Core Networking - DNS (UDP-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	UDP	All Ports	53
Core Networking - DNS (UDP-Out)	Outbound	Allow	Dnscache	UDP	All Ports	53
Core Networking - DNS (TCP-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	All Ports	53
Core Networking - DNS (TCP-Out)	Outbound	Allow	Dnscache	TCP	All Ports	53
NSCI Probe (TCP-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	All ports	80
NSCI Probe - DNS (TCP-Out)	Outbound	Allow	NlaSvc	TCP	All ports	80
Windows Time (UDP-Out)	Outbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	All ports	80
Windows Time Probe - DNS (UDP-Out)	Outbound	Allow	W32Time	UDP	All ports	123
Delivery Optimization (TCP-In)	Inbound	Allow	%SystemRoot%\system32\svchost.exe	TCP	7680	All ports
Delivery Optimization (TCP-In)	Inbound	Allow	DoSvc	TCP	7680	All ports
Delivery Optimization (UDP-In)	Inbound	Allow	%SystemRoot%\system32\svchost.exe	UDP	7680	All ports
Delivery Optimization (UDP-In)	Inbound	Allow	DoSvc	UDP	7680	All ports

Note

There are two rules defined for each rule in the Microsoft Defender Firewall configuration. To restrict the inbound and outbound rules to Windows Services, e.g. DNS Client, both the service name, DNSCache, and the executable path, C:\Windows\System32\svchost.exe, need to be defined as separate rule rather than a single rule that is possible using Group Policy.

You can make additional changes to the management of both inbound and outbound rules as needed for your permitted and blocked services. For more information, see Firewall configuration service.

URL lock proxy

Restrictive URL traffic management includes:

- Deny All outbound traffic except selected Azure and Microsoft services including Azure Cloud Shell and the ability to allow self-service password reset.
- The Privileged profile restricts the endpoints on the internet that the device can connect to using the following URL Lock Proxy configuration.

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
"ProxyEnable"=dword:00000001
"ProxyServer"="127.0.0.2:8080"
"ProxyOverride"="*.azure.com;*.azure.net;*.microsoft.com;*.windowsupdate.com;*.microsoftonline.com;
*.microsoftonline.cn;*.windows.net;*.windowsazure.com;*.windowsazure.cn;*.azure.cn;*.loganalytics.i
o;*.applicationinsights.io;*.vsassets.io;*.azure-
automation.net;*.visualstudio.com,portal.office.com;*.aspnetcdn.com;*.sharepointonline.com;*.msecnd
.net;*.msocdn.com;*.webtrends.com"
"AutoDetect"=dword:00000000
```

The endpoints listed in the ProxyOverride list are limited to those endpoints needed to authenticate to Microsoft Entra ID and access Azure or Office 365 management interfaces. To extend to other cloud services, add their administration URL to the list. This approach is designed to limit access to the wider internet to protect privileged users from internet-based attacks. If this approach is deemed too restrictive, then consider using the following approach for the privileged role.

Enable Microsoft Defender for Cloud Apps, URLs restricted list to approved URLs (Allow most)

In our roles deployment it's recommended that for Enterprise, and Specialized deployments, where a strict *deny all* web browsing isn't desirable, that using the capabilities of a cloud access security broker (CASB) such as Microsoft Defender for Cloud Apps be utilized to block access to risky, and questionable web sites. The solution addresses a simple way to block applications and websites that have been curated. This solution is similar to getting access to the blocklist from sites such as the Spamhaus Project who maintains the Domain Blocklist (DBL): a good resource to use as an advanced set of rules to implement for blocking sites.

The solution provides you:

- Visibility: detect all cloud services; assign each a risk ranking; identify all users and non-Microsoft apps able to sign in
- Data security: identify and control sensitive information (DLP); respond to classification labels on content
- Threat protection: offer adaptive access control (AAC); provide user and entity behavior analysis (UEBA); mitigate malware
- Compliance: supply reports and dashboards to demonstrate cloud governance; assist efforts to conform to data residency and regulatory compliance requirements

Enable Defender for Cloud Apps and connect to Defender ATP to block access the risky URLs:

- In Microsoft Defender Security Center > Settings > Advanced features, set Microsoft Defender for Cloud Apps integration > **ON**
- In Microsoft Defender Security Center > Settings > Advanced features, set Custom network indicators > **ON**
- In Microsoft Defender for Cloud Apps portal > Settings > Microsoft Defender for Endpoint > Select **Enforce app access**

Manage local applications

The secure workstation moves to a truly hardened state when local applications are removed, including productivity applications. Here, you add Visual Studio Code to allow connection to Azure DevOps for GitHub to manage code repositories.

Configuring the Company Portal your for custom apps

An Intune-managed copy of the Company Portal gives you on-demand access to additional tools that you can push down to users of the secured workstations.

In a secured mode, application installation is restricted to managed applications delivered by Company Portal. However, installing the Company Portal requires access to Microsoft Store. In your secured solution, you add and assign the Windows 10 Company Portal app for Autopilot provisioned devices.

Note

Make sure you assign the Company Portal app to the **Secure Workstation Device Tag** group used to assign the Autopilot profile.

Deploy applications using Intune

In some situations, applications like the Microsoft Visual Studio Code are required on the secured workstation. The following example provides instructions to install Microsoft Visual Studio Code to users in the security group **Secure Workstation Users**.

Visual Studio Code is provided as an EXE package so it needs to be packaged as an `.intunewin` format file for deployment using Microsoft Endpoint Manager using the Microsoft Win32 Content Prep Tool.

Download the Microsoft Win32 Content Prep Tool locally to a workstation and copy it to a directory for packaging, for example, C:\Packages. Then create a Source and Output directory under C:\Packages.

Package Microsoft Visual Studio Code

1. Download the offline installer Visual Studio Code for Windows 64-bit.
2. Copy the downloaded Visual Studio Code exe file to `C:\Packages\Source`
3. Open a PowerShell console and navigate to `C:\Packages`
4. Type `.\IntuneWinAppUtil.exe -c C:\Packages\Source\ -s C:\Packages\Source\VSCodeUserSetup-x64-1.51.1.exe -o C:\Packages\Output\VSCodeUserSetup-x64-1.51.1`
5. Type `Y` to create the new output folder. The intunewin file for Visual Studio Code is created in this folder.

Upload VS Code to Microsoft Endpoint Manager

1. In the **Microsoft Endpoint Manager admin center**, browse to **Apps** > **Windows** > **Add**
2. Under **Select app type**, choose **Windows app (Win32)**
3. Click **Select app package file**, click **Select a file**, then select the `VSCodeUserSetup-x64-1.51.1.intunewin` from `C:\Packages\Output\VSCodeUserSetup-x64-1.51.1`. Click **OK**
4. Enter `Visual Studio Code 1.51.1` in the Name field

5. Enter a description for Visual Studio Code in the **Description** field
6. Enter `Microsoft Corporation` in the **Publisher** Field
7. Download `https://jsarray.com/images/page-icons/visual-studio-code.png` and select image for the logo. Select **Next**
8. Enter `VSCodeSetup-x64-1.51.1.exe /SILENT` in the **Install command** field
9. Enter `C:\Program Files\Microsoft VS Code\unins000.exe` in the **Uninstall command** field
10. Select **Determine behavior based on return codes** from the **Device Restart behavior** dropdown list. Select **Next**
11. Select **64-bit** from the **Operating system architecture** checkbox dropdown
12. Select **Windows 10 1903** from the **Minimum operating system** checkbox dropdown. Select **Next**
13. Select **Manually configure** detection rules from the **Rules format** dropdown list
14. Click **Add** and then select **File** from the **Rule type** dropdown
15. Enter `C:\Program Files\Microsoft VS Code` in the **Path** field
16. Enter `unins000.exe` in the **File or folder** field
17. Select **File or folder exists** from the dropdown list, Select **OK** and then select **Next**
18. Select **Next** as there are no dependencies on this package
19. Select **Add Group** under **Available for enrolled devices**, add **Privileged Users group**. Click **Select** to confirm group. Select **Next**
20. Click **Create**

Use PowerShell to create custom apps and settings

There are some configuration settings that we recommend, including two Defender for Endpoint recommendations that must be set using PowerShell. These configuration changes can't be set via policies in Intune.

You can also use PowerShell to extend host management capabilities. The PAW-DeviceConfig.ps1 script from GitHub is an example script that configures the following settings:

- Removes Internet Explorer
- Removes PowerShell 2.0
- Removes Windows Media Player
- Removes Work Folders Client
- Removes XPS Printing
- Enables and configures Hibernate
- Implements registry fix to enable AppLocker DLL rule processing
- Implements registry settings for two Microsoft Defender for Endpoint recommendations that can't be set using Endpoint Manager.
    - Require users to elevate when setting a network's location
    - Prevent saving of network credentials
- Disable Network Location Wizard - prevents users from setting network location as Private and therefore increasing the attack surface exposed in Windows Firewall
- Configures Windows Time to use NTP and sets the Auto Time service to Automatic
- Downloads and sets the desktop background to a specific image to easily identify the device as a ready-to-use, privileged workstation.

The PAW-DeviceConfig.ps1 script from GitHub.

1. Download the script [PAW-DeviceConfig.ps1] to a local device.
2. Browse to the **Azure portal** > **Microsoft Intune** > **Device configuration** > **PowerShell scripts** > **Add**. vProvide a **Name** for the script and specify the **Script location**.
3. Select **Configure**.
    1. Set **Run this script using the logged on credentials** to **No**.
    2. Select **OK**.
4. Select **Create**.

5. Select **Assignments** > **Select groups**.
    1. Add the security group **Secure Workstations**.
    2. Select **Save**.

Validate and test your deployment with your first device

This enrollment assumes that you use a physical computing device. It's recommended that as part of the procurement process that the OEM, Reseller, distributor, or partner register devices in Windows Autopilot.

However for testing it's possible to stand up Virtual Machines as a test scenario. However note enrollment of personally joined devices need to be revised to allow this method of joining a client.

This method works for Virtual Machines or physical devices that haven't been previously registered.

1. Start the device and wait for the username dialog to be presented
2. Press `SHIFT + F10` to display command prompt
3. Type `PowerShell` press Enter
4. Type `Set-ExecutionPolicy RemoteSigned` press Enter
5. Type `Install-Script Get-WindowsAutopilotInfo` press Enter
6. Type `Y` and click Enter to accept PATH environment change
7. Type `Y` and click Enter to install NuGet provider
8. Type `Y` to trust the repository
9. Type Run `Get-WindowsAutoPilotInfo -GroupTag PAW –outputfile C:\device1.csv`
10. Copy the CSV from the Virtual Machine or Physical device

Import devices into Autopilot

1. In the **Microsoft Endpoint Manager admin center**, go to **Devices** > **Windows Devices** > **Windows enrollment** > **Devices**

2. Select **Import** and choose your CSV file.

3. Wait for the `Group Tag` to be updated to `PAW` and the `Profile Status` to change to `Assigned`.

    Note

    The Group Tag is used by the Secure Workstation dynamic group to make the device a member of its group,

4. Add the device to the **Secure Workstations** security group.

5. On the Windows 10 device you wish to configure, go to **Windows Settings** > **Update & Security** > **Recovery**.

    1. Choose **Get started** under **Reset this PC**.
    2. Follow the prompts to reset and reconfigure the device with the profile and compliance policies configured.

After you configure the device, complete a review and check the configuration. Confirm that the first device is configured correctly before continuing your deployment.

Assign devices

To assign devices and users, you need to map the selected profiles to your security group. All new users who require permissions to the service must be added to the security group as well.

Using Microsoft Defender for Endpoint to monitor and respond to security incidents

- Continuously observe and monitor vulnerabilities and misconfigurations
- Utilize Microsoft Defender for Endpoint to prioritize dynamic threats in the wild
- Drive correlation of vulnerabilities with endpoint detection and response (EDR) alerts
- Use the dashboard to identify machine-level vulnerability during investigations
- Push out remediations to Intune

Configure your Microsoft Defender Security Center. Using guidance at Threat & Vulnerability Management dashboard overview.

Monitoring application activity using Advanced Threat Hunting

Starting at the specialized workstation, AppLocker is enabled for monitoring of application activity on a workstation. By default Defender for Endpoint captures AppLocker events and Advanced Hunting Queries can be used to determine what applications, scripts, DLL files are being blocked by AppLocker.

Note

The Specialized and Privileged workstation profiles contain the AppLocker policies. Deployment of the policies is required for monitoring of application activity on a client.

From the Microsoft Defender Security Center Advanced Hunting pane, use the following query to return AppLocker events

Kusto

```
DeviceEvents
| where Timestamp > ago(7d) and
ActionType startswith "AppControl"
| summarize Machines=dcount(DeviceName) by ActionType
| order by Machines desc
```

Monitoring

- Understand how to review your Exposure Score
- Review Security recommendation
- Manage security remediations
- Manage endpoint detection and response
- Monitor profiles with Intune profile monitoring.

Next steps