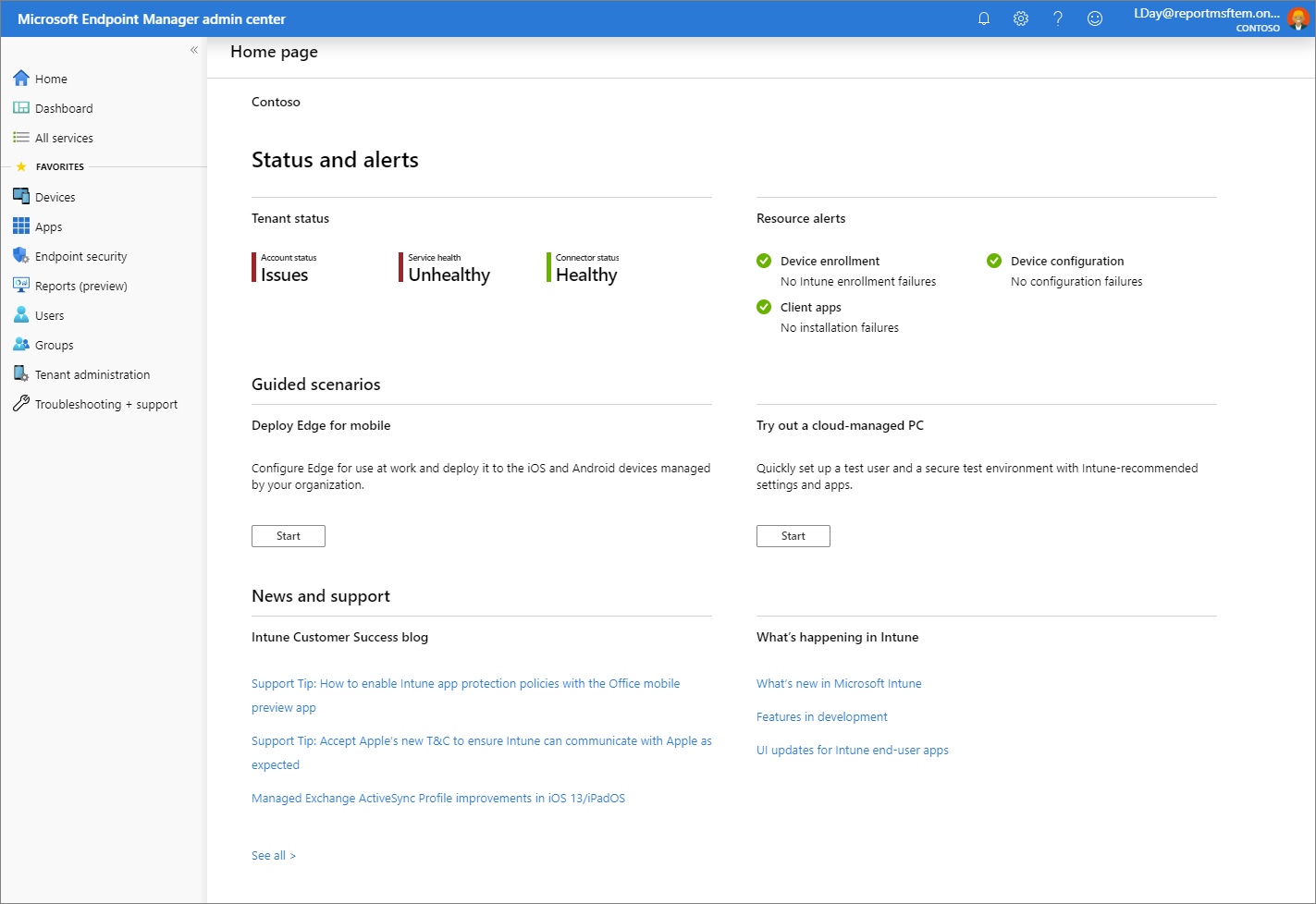
**Lab C - Microsoft Intune in the Microsoft Endpoint Manager admin center**

Follow the steps below to better understand Intune in the Microsoft Endpoint Manager admin center. Once you complete the tour, you'll have a better understanding of some of the major areas of Intune.

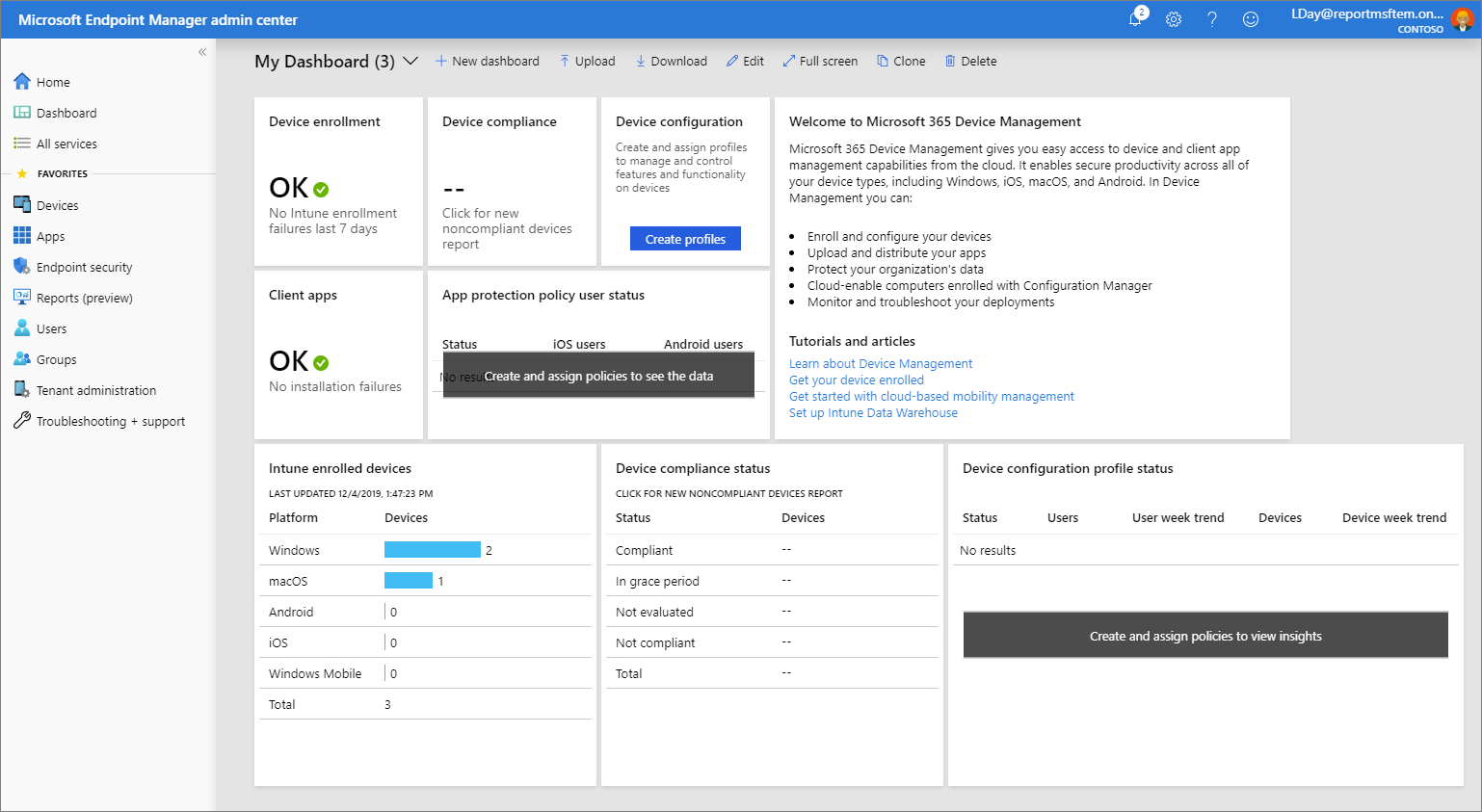
1. Open a browser and sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). If you are new to Intune, use your free trial subscription.



When you open the Microsoft Endpoint Manager, the service is displayed in a pane of your browser. Some of the first workloads you may use in Intune include **Devices**, **Apps**, **Users**, and **Groups**. A workload is simply a sub-area of a service. When you select the workload, it opens that pane as a full page. Other panes slide out from the right side of the pane when they open, and close to reveal the previous pane.

By default, when you open the Microsoft Endpoint Manager you'll see the **Home page** pane. This pane provides an overall visual snapshot of tenant status and compliance status, as well as other helpful related links.

1. From the navigation pane, select **Dashboard** to display overall details about the devices and client apps in your Intune tenant. If you are starting with a new Intune tenant, you will not have any enrolled devices yet.



Intune lets you manage your workforce's devices and apps, including how they access your company data. To use this mobile device management (MDM) service, the devices must first be enrolled in Intune. When a device is enrolled, it is issued an MDM certificate. This certificate is used to communicate with the Intune service.

There are several methods to enroll your workforce's devices into Intune. Each method depends on the device's ownership (personal or corporate), device type (iOS/iPadOS, Windows, Android), and management requirements (resets, affinity, locking). However, before you can enable device enrollment, you must set up your Intune infrastructure. In particular, device enrollment requires that you [set your MDM authority](https://docs.microsoft.com/en-us/mem/intune/fundamentals/mdm-authority-set). For more information about getting your Intune environment (tenant) ready, see [Set up Intune](https://docs.microsoft.com/en-us/mem/intune/fundamentals/setup-steps). Once you have your Intune tenant ready, you can enroll devices. For more information about device enrollment, see [What is device enrollment?](https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment)

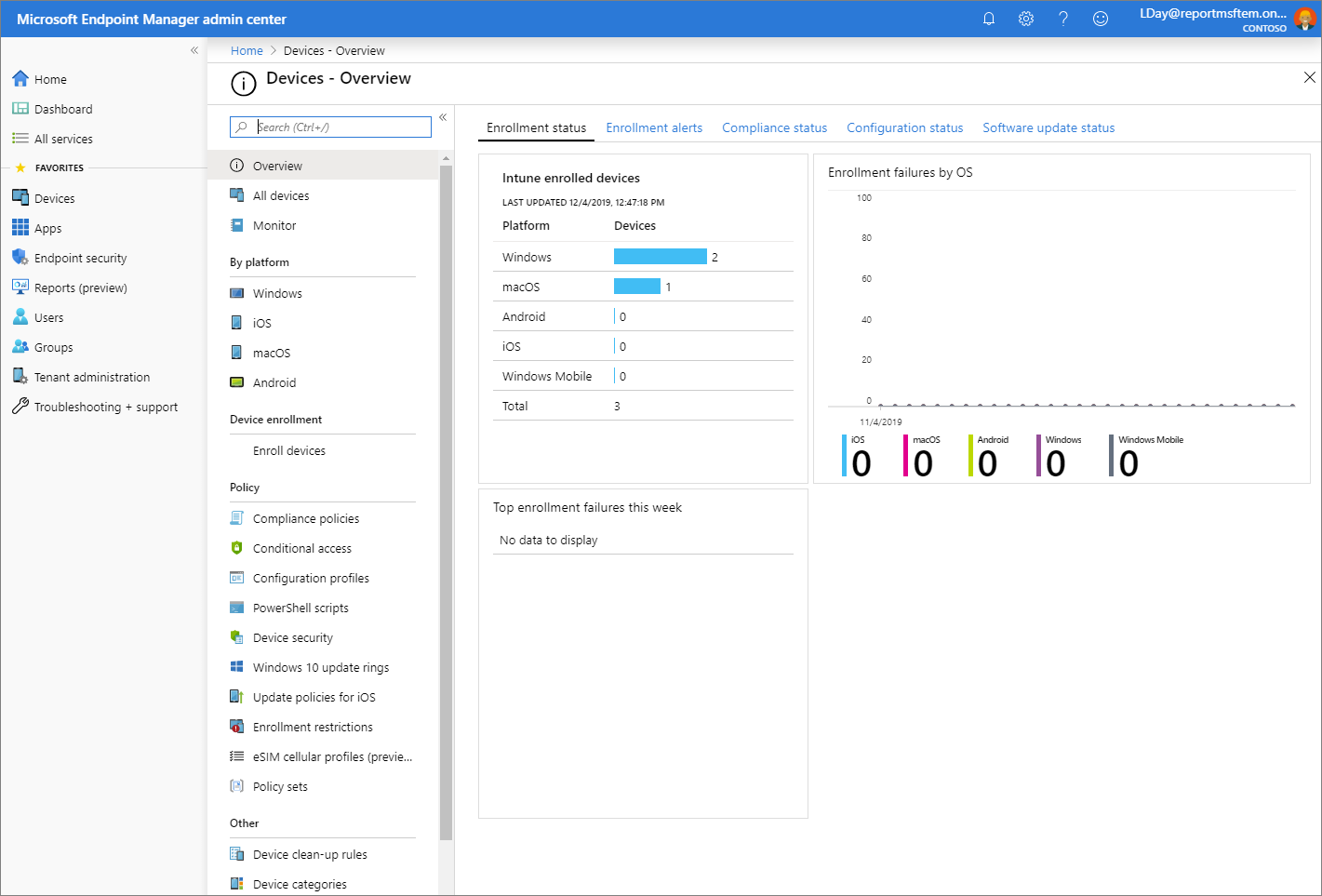
1. From the navigation pane, select **Devices** to display details about the enrolled devices in your Intune tenant.

**Tip**

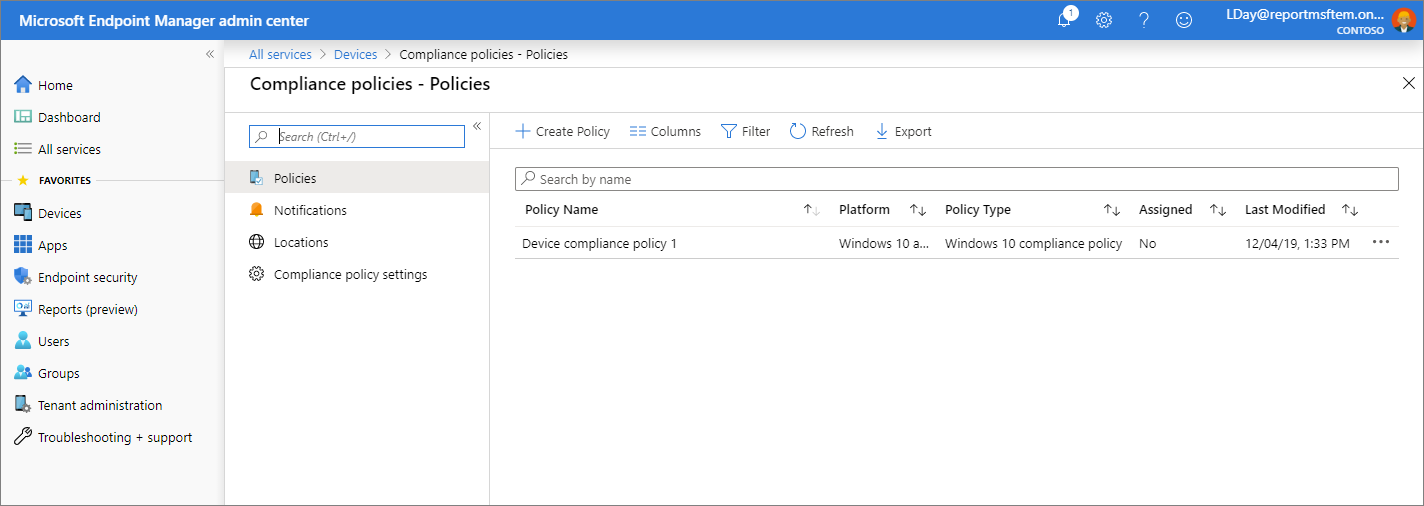
If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Devices**.

The **Devices - Overview** pane has several tabs that allow you to view a summary of the following statuses and alerts:

* + **Enrollment status** - Review details about Intune enrolled devices by platform and enrollment failures.
  + **Enrollment alerts** - Find more details about unassigned devices by platform.
  + **Compliance status** - Review compliance status based on device, policy, setting, threats, and protection. Additionally, this pane provides a list of devices without a compliance policy.
  + **Configuration status** - Review configuration status of device profiles, as well as profile deployment., and
  + **Software update status** - See a visual of the deployment status for all devices and for all users.



1. From the **Devices - Overview** pane, select **Compliance policies** to display details about compliance for devices managed by Intune. You will see details similar to the following image.



**Tip**

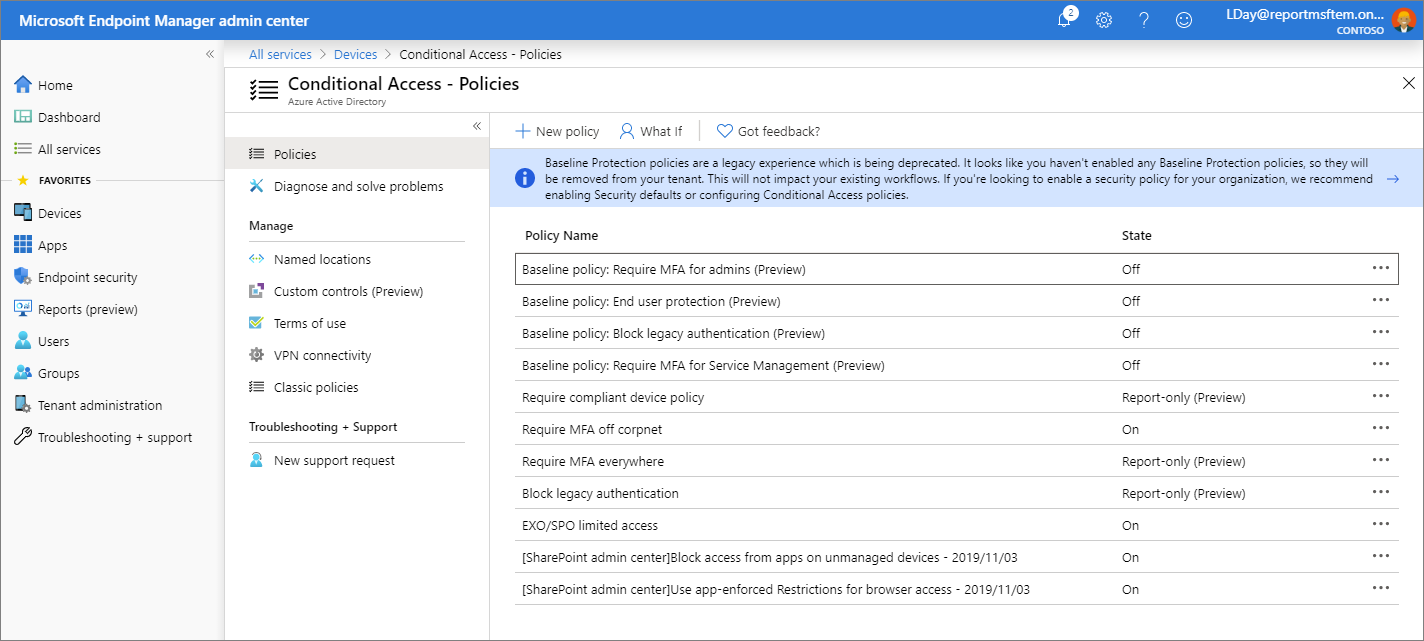
If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Device Compliance**.

Compliance requirements are essentially rules, such as requiring a device PIN, or requiring device encryption. Device compliance policies define the rules and settings that a device must follow to be considered compliant. To use device compliance, you must have:

* + An Intune and an Azure Active Directory (Azure AD) Premium subscription
  + Devices running a supported platform
  + Devices must be enrolled in Intune
  + Devices that are enrolled to either one user or no primary user.

For more information, see [Get started with device compliance policies in Intune](https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started).

1. From the **Devices - Overview** pane, select **Conditional Access** to display details about access policies.

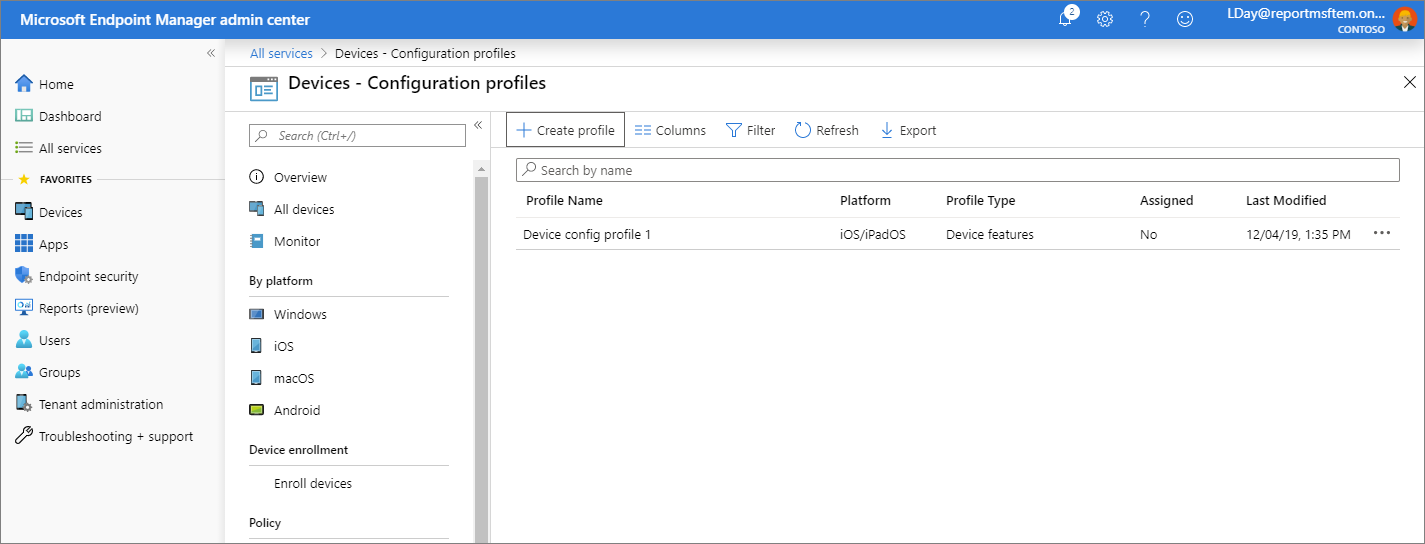


**Tip**

If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Conditional Access**.

Conditional Access refers to ways you can control the devices and apps that are allowed to connect to your email and company resources. To learn about device-based and app-based Conditional Access, and find common scenarios for using Conditional Access with Intune, see [What's Conditional Access?](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access)

1. From the navigation pane, select **Devices** > **Configuration profiles** to display details about device profiles in Intune.



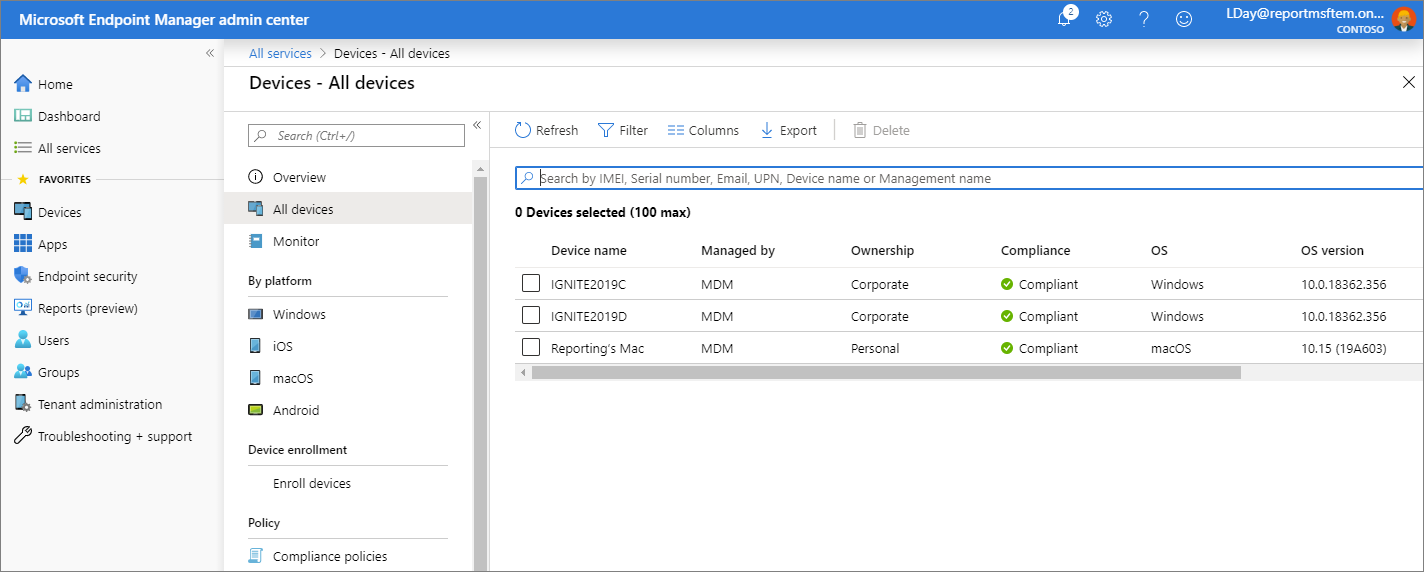
**Tip**

If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Device configuration**.

Intune includes settings and features that you can enable or disable on different devices within your organization. These settings and features are added to "configuration profiles". You can create profiles for different devices and different platforms, including iOS/iPadOS, Android, macOS, and Windows. Then, you can use Intune to apply the profile to devices in your organization.

For more information about device configuration, see [Apply features settings on your devices using device profiles in Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/configuration/device-profiles).

1. From the navigation pane, select **Devices** > **All devices** to display details about your Intune tenant's enrolled devices. If you are starting with a new Intune enlistment, you will not have any enrolled devices yet.



This list of devices show key details about compliance, OS version, and last check-in date.

**Tip**

If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Devices** > **All devices**.

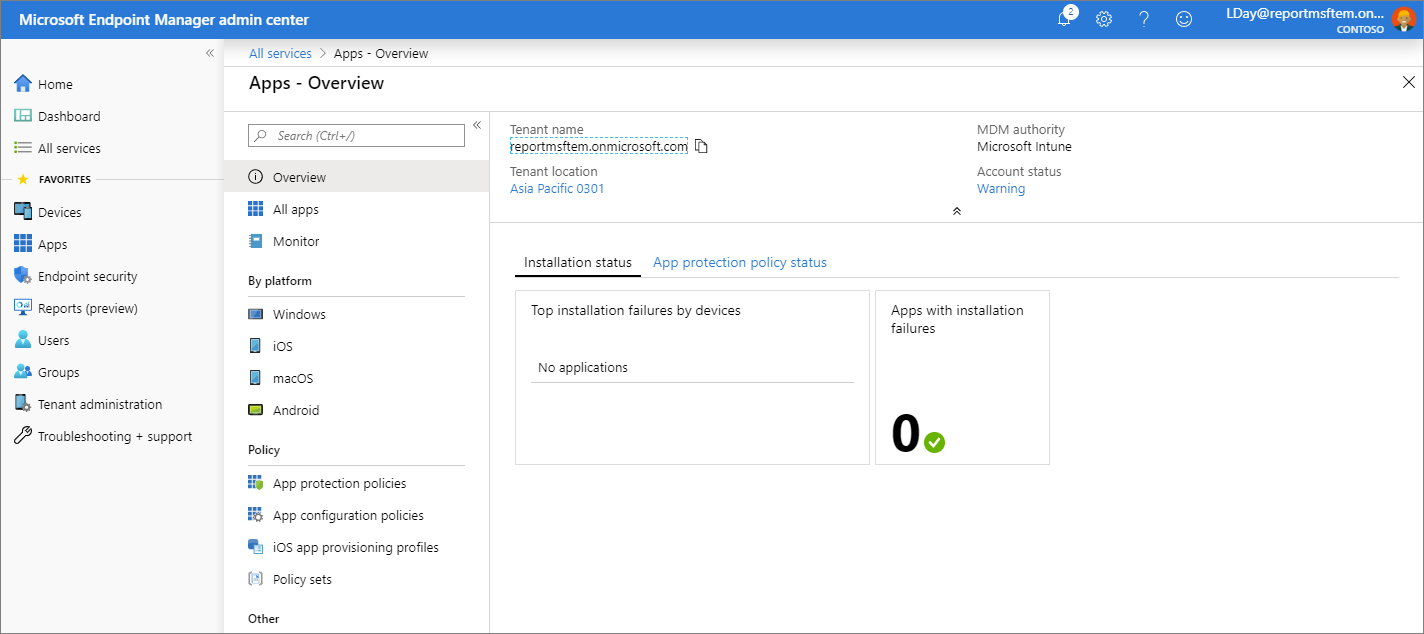
1. From the navigation pane, select **Apps** to display an overview of app status. This pane provides app installation status based on the following tabs:

**Tip**

If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Client apps**.

The **Apps - Overview** pane has two tabs that allow you to view a summary of the following statuses:

* + **Installation status** - View the top installation failures by device, as well as the apps with installation failures.
  + **App protection policy status** - Find details about assigned users to app protection policies, as well as flagged users.



As an IT admin, you can use Microsoft Intune to manage the client apps that your company's workforce uses. This functionality is in addition to managing devices and protecting data. One of an admin's priorities is to ensure that end users have access to the apps they need to do their work. Additionally, you might want to assign and manage apps on devices that are not enrolled with Intune. Intune offers a range of capabilities to help you get the apps you need on the devices you want.

**Note**

The **Apps - Overview** pane also provides tenant status and account details.

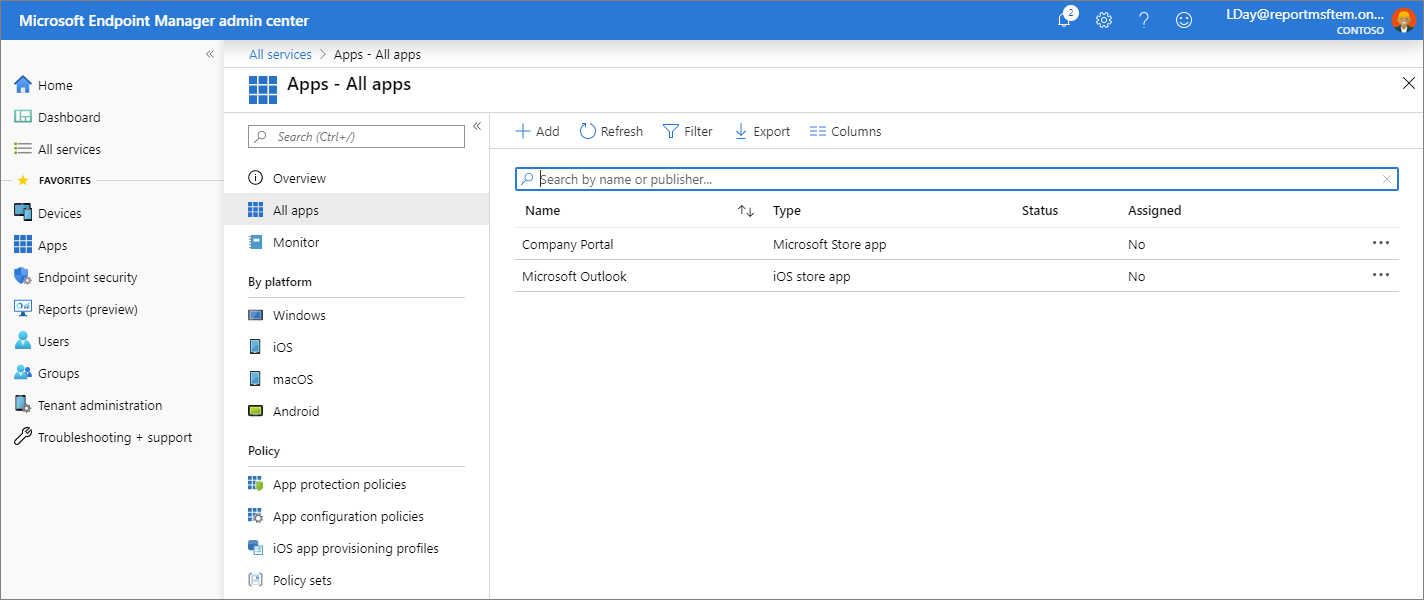
For more information about adding and assigning apps, see [Add apps to Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/apps/apps-add) and [Assign apps to groups with Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy).

1. From the **Apps - Overview** pane, select **All apps** to see a list of apps that have been added to Intune.

**Tip**

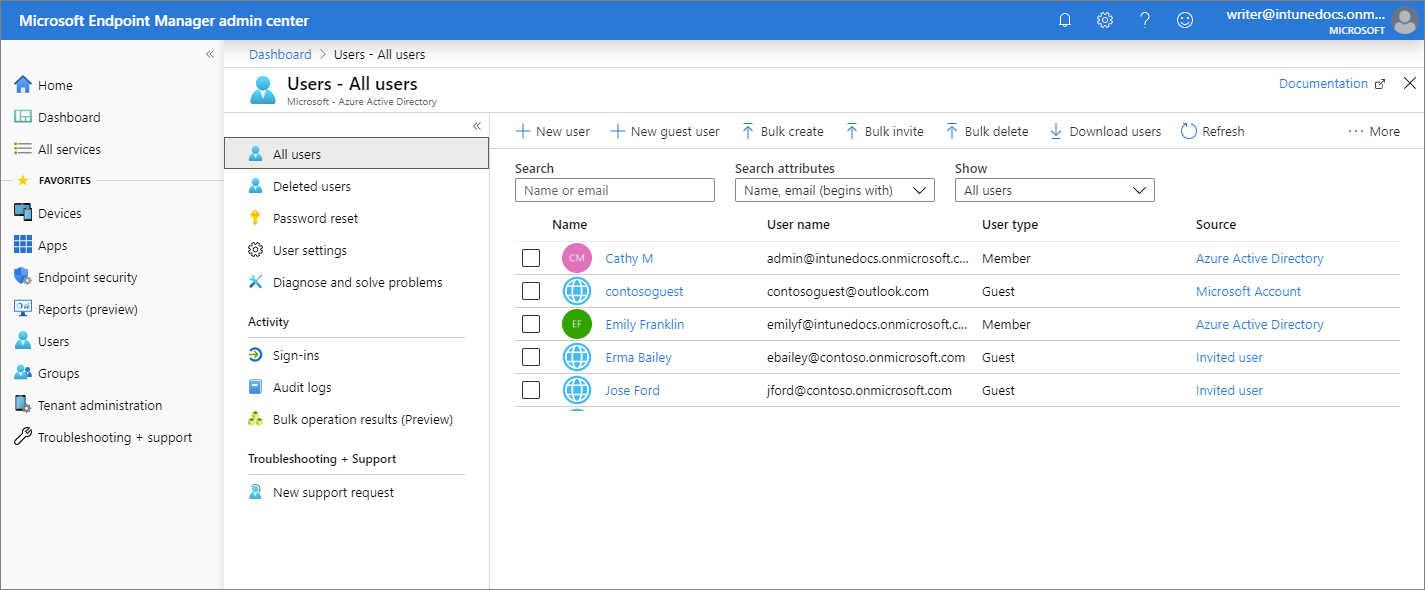
If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Client apps** > **Apps**.

You can add a variety of different app type based on platform to Intune. Once an app has been added, you can assign it to groups of users.



For more information, see [Add apps to Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/apps/apps-add).

1. From the navigation pane, select **Users** to display details about the users that you have included in Intune. These users are your company's workforce.

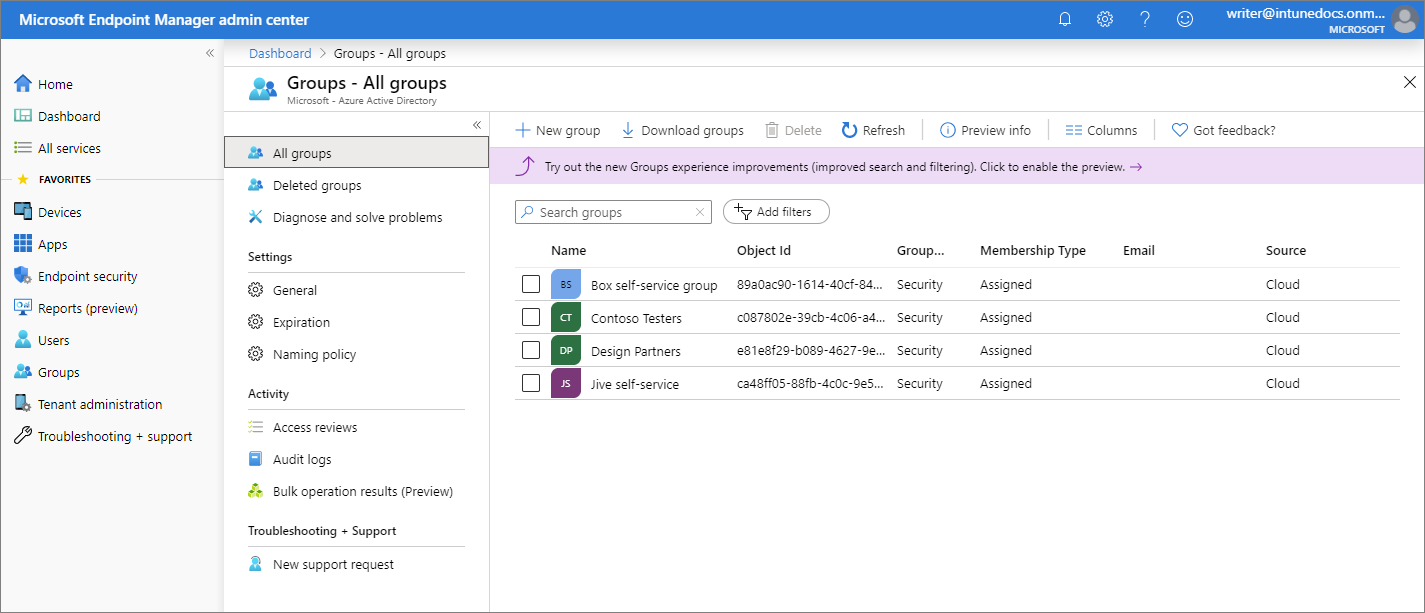


**Tip**

If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Users**.

You can add users directly to Intune or synchronize users from your on-premises Active Directory. Once added, users can enroll devices and access company resources. You can also give users additional permissions to access Intune. For more information, see [Add users and grant administrative permission to Intune](https://docs.microsoft.com/en-us/mem/intune/fundamentals/users-add).

1. From the navigation pane, select **Groups** to display details about the Azure Active Directory (Azure AD) groups included in Intune. As an Intune admin, you use groups to manage devices and users.



**Tip**

If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Groups**.

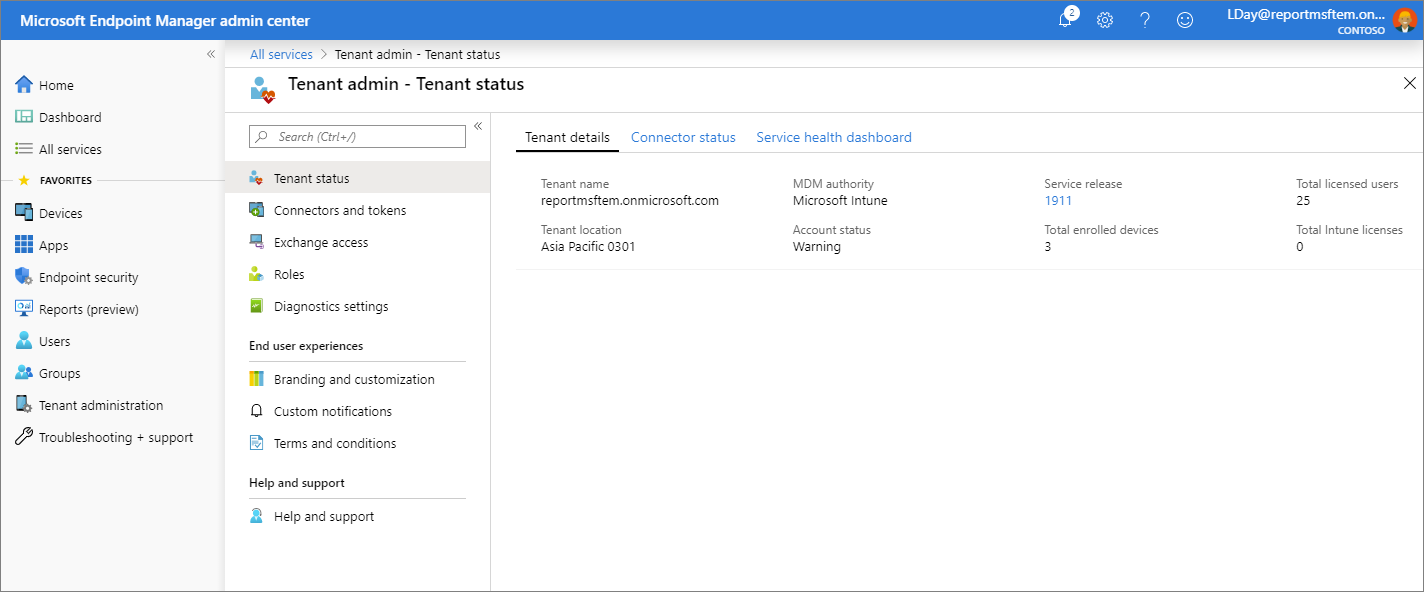
You can set up groups to suit your organizational needs. Create groups to organize users or devices by geographic location, department, or hardware characteristics. Use groups to manage tasks at scale. For example, you can set policies for many users or deploy apps to a set of devices. For more information about groups, see [Add groups to organize users and devices](https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add).

1. From the navigation pane, select **Tenant administration** to display details about your Intune tenant.

**Tip**

If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Tenant status**.

The **Tenant admin - Tenant status** pane provides tabs for **Tenant details**, **Connector status**, and **Service health dashboard**. If there are any issues with your tenant or Intune itself, you will find details available from this pane.



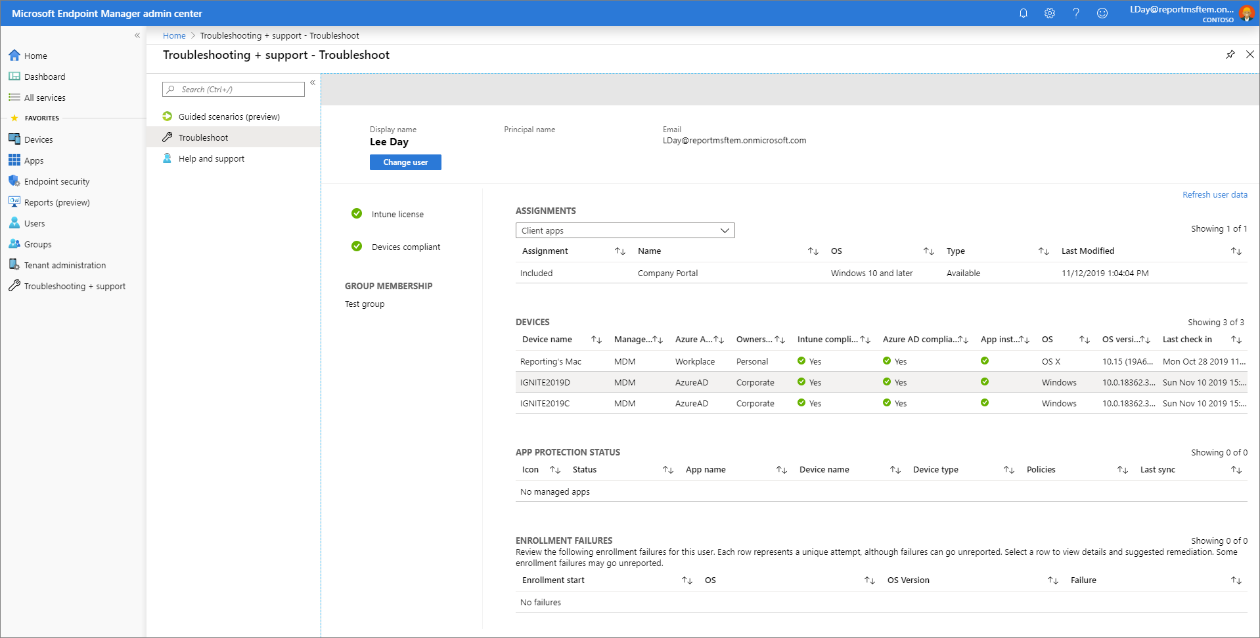
For more information, see [Intune Tenant Status](https://docs.microsoft.com/en-us/mem/intune/fundamentals/tenant-status).

1. From the navigation pane, select **Troubleshooting + support** > **Troubleshoot** to check status details on a specific user.

**Tip**

If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Troubleshoot**.

From the **Assignments** dropdown list, you can choose to view the targeted assignments of client apps, policies, update rings, and enrollment restrictions. Additionally, this pane provides device details, app protection status, and enrollment failures for a specific user.



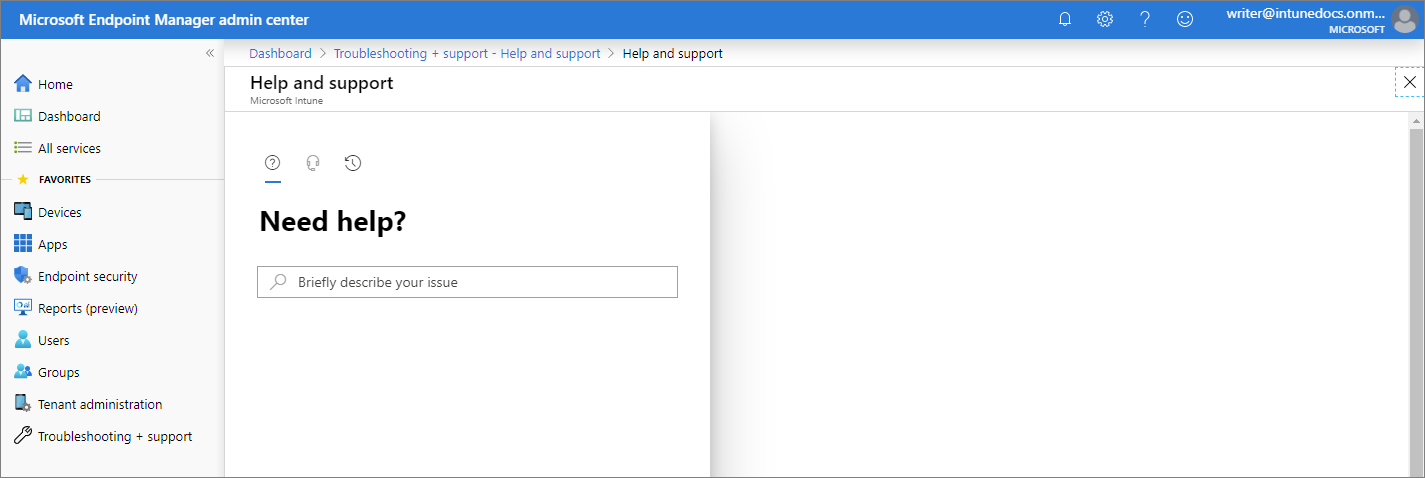
For more information about troubleshooting within Intune, see [Use the troubleshooting portal to help users at your company](https://docs.microsoft.com/en-us/mem/intune/fundamentals/help-desk-operators).

1. From the navigation pane, select **Troubleshooting + support** > **Help and support** to request help.

**Tip**

If you have previously used Intune in the Azure portal, you found the above details in the Azure portal by signing in to [**Intune**](https://go.microsoft.com/fwlink/?linkid=2090973) and selecting **Help and support**.

As an IT admin, you can use the **Help and Support** option to search and view solutions, as well as file an on-line support ticket for Intune.



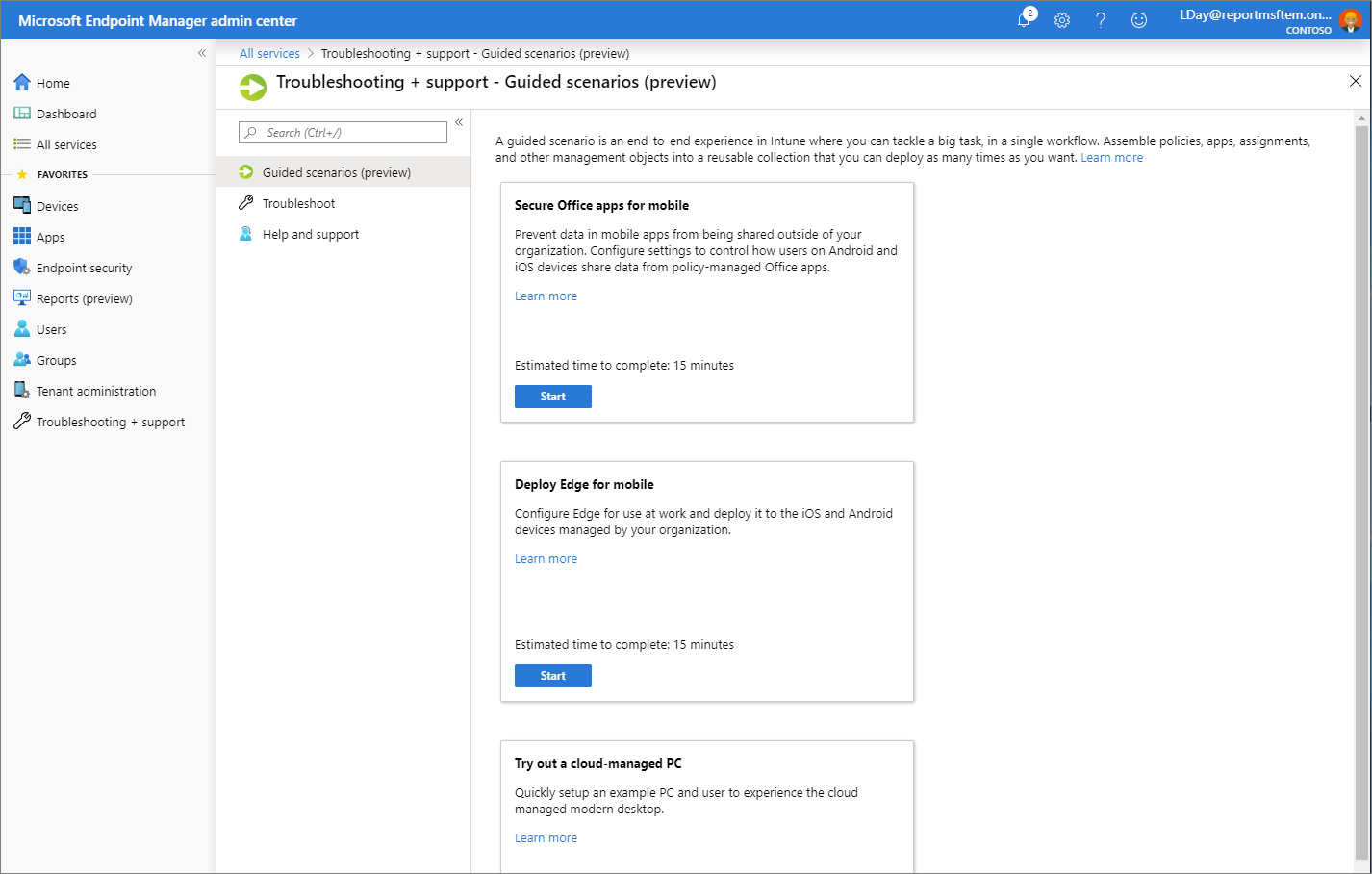
To create a support ticket, your account must be assigned as an administrator role in Azure Active Directory. Administrator roles include, **Intune administrator**, **Global administrator**, and **Service administrator**.

For more information, see [How to get support in Microsoft Endpoint Manager](https://docs.microsoft.com/en-us/mem/get-support).

1. From the navigation pane, select **Troubleshooting + support** > **Guided scenarios** to display available Intune guided scenarios.

A guided scenario is a customized series of steps centered around one end-to-end use-case. Common scenarios are based on the role an admin, user, or device plays in your organization. These roles typically require a collection of carefully orchestrated profiles, settings, applications, and security controls to provide the best user experience and security.

If you are not familiar with all the steps and resources needed to implement a particular Intune scenario, guided scenarios may be used as your starting point.



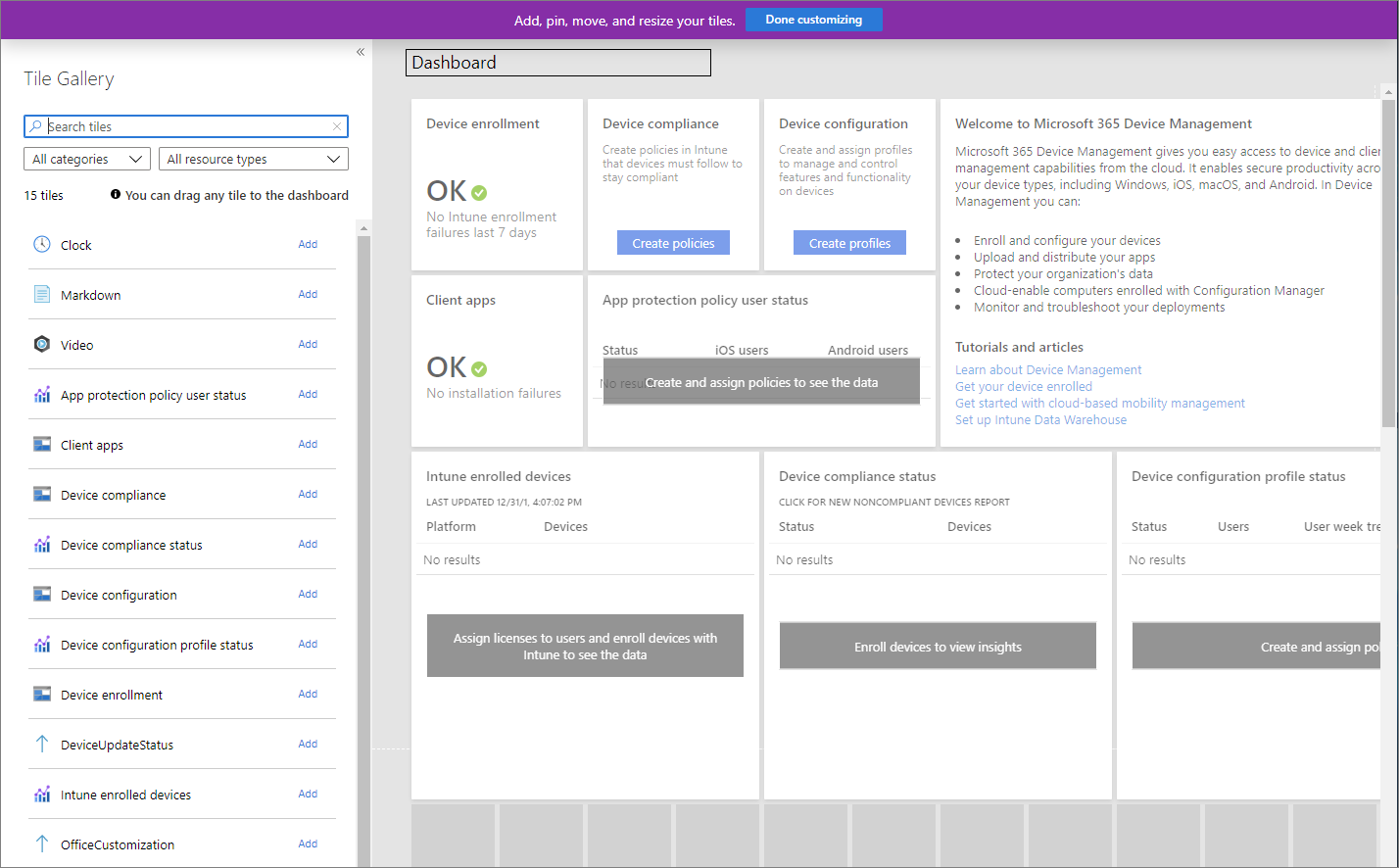
For more information about guided scenarios, see [Guided scenarios overview](https://docs.microsoft.com/en-us/mem/intune/fundamentals/guided-scenarios-overview).

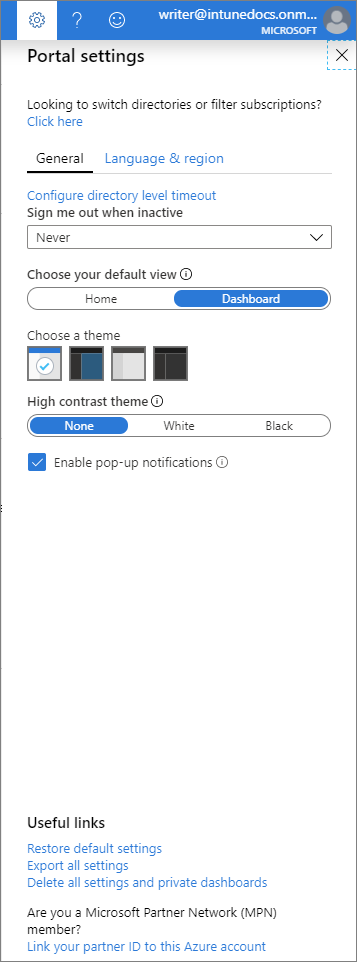
**Configure the Microsoft Endpoint Manager admin center**

Microsoft Endpoint Manager admin center allows you to customize and configure the view of the portal.

**Change the Dashboard**

The **Dashboard** to display overall details about the devices and client apps in your Intune tenant. Dashboards provide a way for you to create a focused and organized view in the Microsoft Endpoint Manager admin center. Use dashboards as a workspace where you can quickly launch tasks for day-to-day operations and monitor resources. Build custom dashboards based on projects, tasks, or user roles, for example. The Microsoft Endpoint Manager admin center provides a default dashboard as a starting point. You can edit the default dashboard, create and customize additional dashboards, and publish and share dashboards to make them available to other users.



To modify your current dashboard, select **Edit**. If you don't want to change your default dashboard, you can also create a **New dashboard**. Creating a new dashboard gives you an empty, private dashboard with the **Tile Gallery**, which lets you add or rearrange tiles. You can find tiles by category or resource type. You can also search for particular tiles. Select **My Dashboard** to select any of your existing custom dashboards.

**Change the Portal settings**

You can customize the Microsoft Endpoint Manager admin center by choosing the default view, the theme, the credentials timeout period, as well as language and region settings.