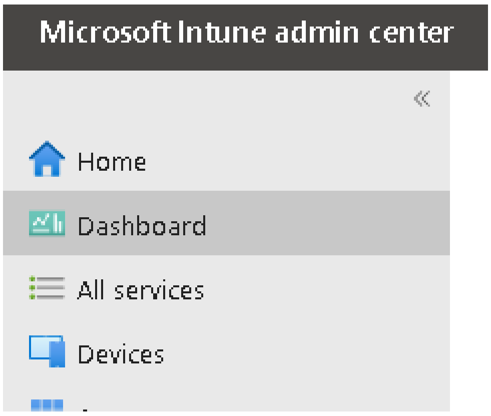
Intune Reporting and Monitoring

Contents

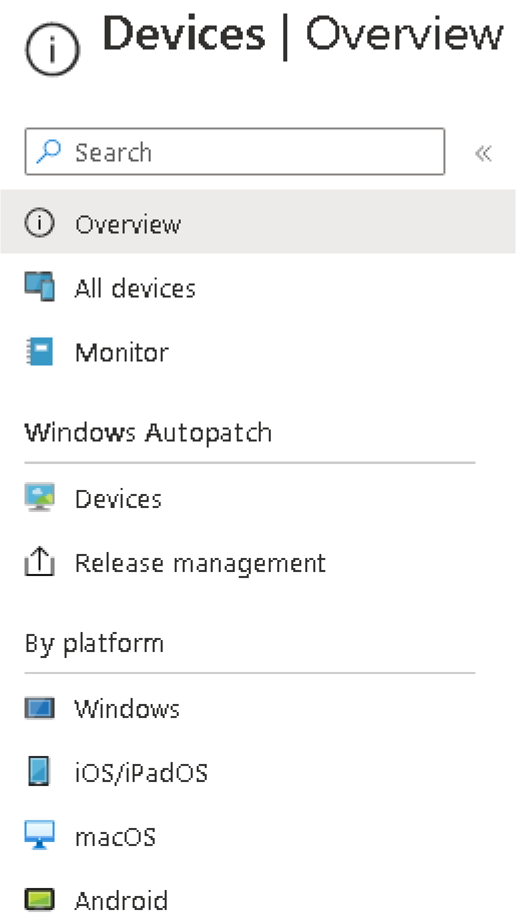
List all devices

Navigate to the Intune console (https://in.cmd.ms)

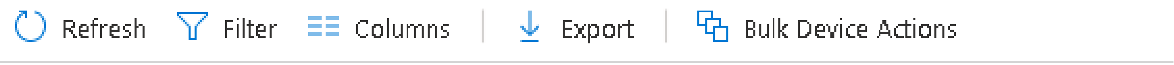
On the home screen click Devices on the left:



From here you can either select All Devices, or select a platform for a filtered view:

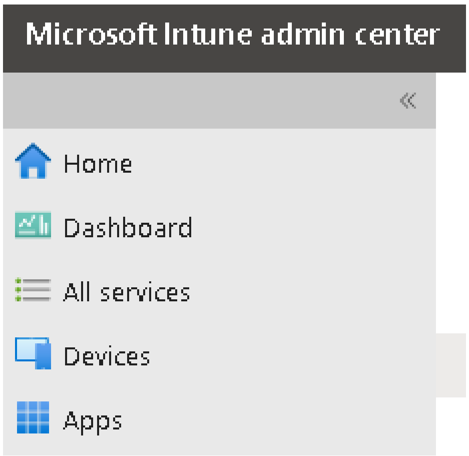


At the top of the next screen, you can search, export, or add/remove columns. There are a lot of extra options in the columns so it's worth investigating



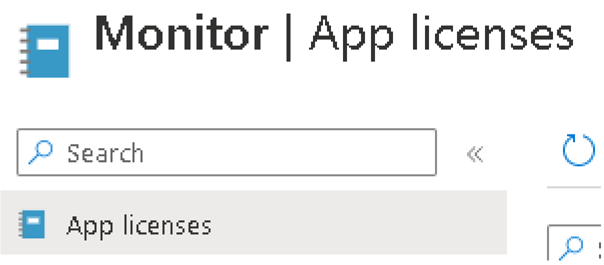
List all applications configured

In the menu, select Apps



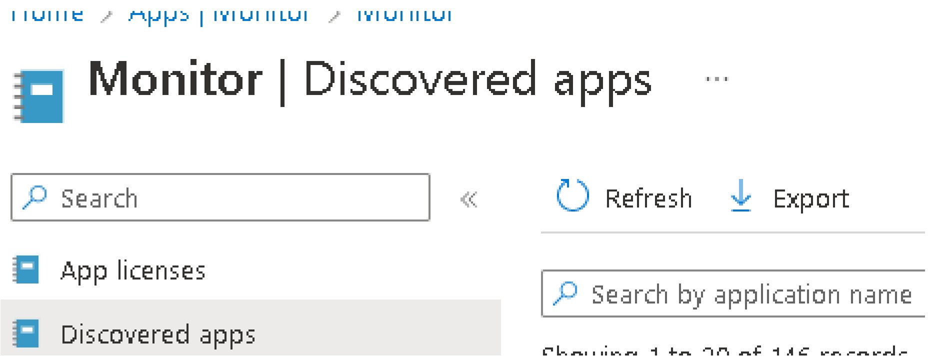
Again, you can select All Apps or filter by device

To review your licenses for Apple purchased applications, navigate to Apps – Monitor – App Licenses



List Applications Discovered

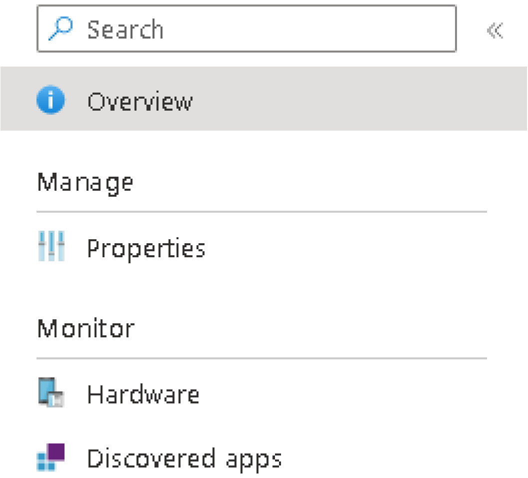
To view all applications discovered by Intune, including those manually installed, navigate to Apps – Monitor – Discovered Apps. Here you can also search and export as it can contain numerous listings


Home > Apps | Monitor > Monitor
Monitor | Discovered apps ...
Search
«
Refresh
Export
App licenses
Discovered apps
Search by application name
Showing 1 to 20 of 146 records

List applications on a device

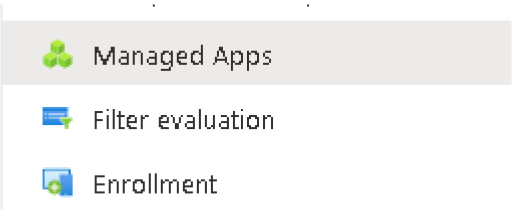
If you want to check if a particular application is installed on a device, navigate to Devices – All Devices and find your device

Click on the device and click Discovered Apps:



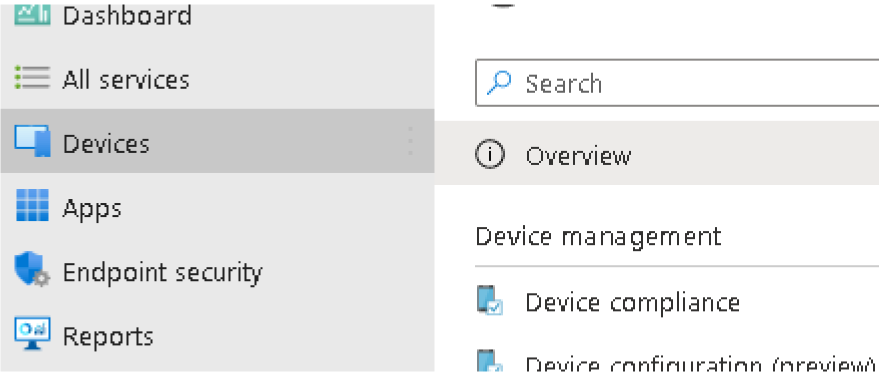
This will show everything installed on this device.

If the application is being managed and deployed by Intune, click on Managed Apps for a more thorough output



Review non-compliant devices

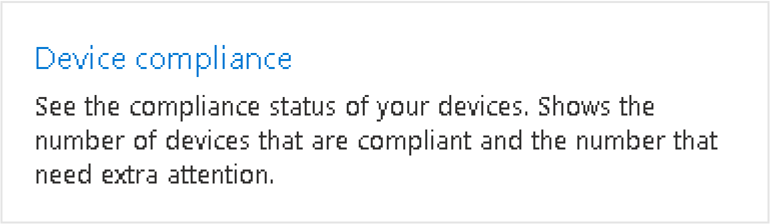
To check your device compliance, navigate to Reports – Device Compliance



You will need to click Refresh initially for the report to generate data

Next to Summary is a Reports button, clicking this will give more detailed reports

In this case, click Device Compliance



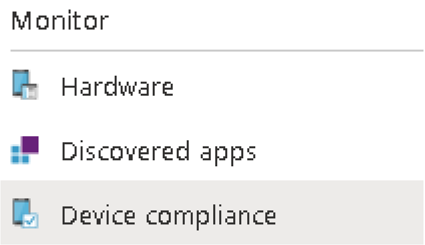
Device compliance

See the compliance status of your devices. Shows the number of devices that are compliant and the number that need extra attention.

Then click Generate Report

Once you have a list of your non-compliant devices, navigate to them in Devices – All Devices

Click on the device and click Device Compliance

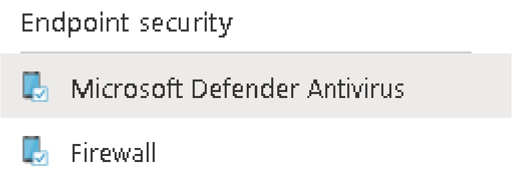


Here you can see which policy is non-compliant

Clicking the policy name will tell you which policy setting the device is not meeting the criteria for.

Review security alerts

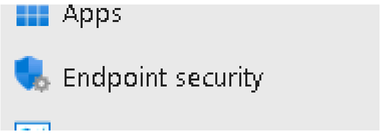
Navigate to Reports and under Endpoint Security you can report on Antivirus and Firewall



Again, clicking Refresh will generate an overview and in the event of anything unwanted, the Reports tab will drill down to the device level

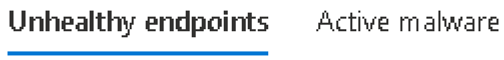
Resolving Security Alerts

Should you notice an issue in here, click on the Endpoint Security menu option

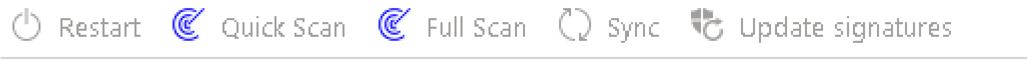


Click Security Tasks and review/accept any changes in there

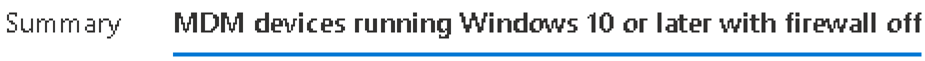
Next, click on Antivirus and click on Unhealthy endpoints and Active Malware



Here you have a selection of commands to run against devices



Click on Firewall and select MDM devices running Windows 10 or later with firewall off

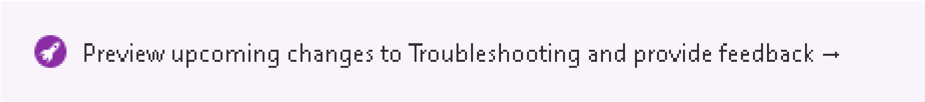


Here you can sync or restart a device to re-enable the firewall

Device Troubleshooting

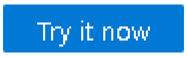
Should a user report an issue, the first step is to use the built in Troubleshooting tool.

First, if this banner is active, click it to enable the new features



Preview upcoming changes to Troubleshooting and provide feedback →

Then click Try it Now



Try it now

Now, type in the users email address or name

It will now present a full overview of the user including a policy, compliance and app summary.

You can quickly check the account is enabled and licensed ok, check group membership as well as which policies and apps are applying to the user