Windows Analytics and Upgrade Readiness configuration

Ievgen Liashov
Microsoft MVP Enterprise Mobility
http://liashov.com/
http://en.liashov.com/

1. Introduction

This document identifies a process of configuring Upgrade Readiness in Windows Analytics.

2. Feature overview

Windows Analytics uses Azure Log Analytics (formerly known as Operations Management Suite or OMS), a collection of cloud-based servicing for monitoring and automating your on-premises and cloud environments. Windows Analytics is a set of solutions that provide you with extensive data about the state of devices in your deployment. There are currently three solutions which you can use singly or in any combination:

Device Health provides the following:

- Identification of devices that crash frequently, and therefore might need to be rebuilt or replaced
- Identification of device drivers that are causing device crashes, with suggestions of alternative versions of those drivers that might reduce the number of crashes
- Notification of Windows Information Protection misconfigurations that send prompts to end users

Update Compliance shows you the state of your devices with respect to the Windows updates so that you can ensure that they are on the most current updates as appropriate. In addition, Update Compliance provides the following:

- Dedicated drill-downs for devices that might need attention
- An inventory of devices, including the version of Windows they are running and their update status
- The ability to track protection and threat status for Windows Defender Antivirus-enabled devices
- An overview of Windows Update for Business deferral configurations (Windows 10, version 1607 and later)
- Powerful built-in log analytics to create useful custom queries
- Cloud-connected access utilizing Windows 10 diagnostic data means no need for new complex, customized infrastructure

Upgrade Readiness offers a set of tools to plan and manage the upgrade process end to end, allowing you to adopt new Windows releases more quickly. With new Windows versions being released multiple times a year, ensuring application and driver compatibility on an ongoing basis is key to adopting new Windows versions as they are released. Upgrade Readiness not only supports upgrade management from Windows 7 and Windows 8.1 to Windows 10, but also Windows 10 upgrades in the Windows as a Service model.

Use Upgrade Readiness to get:

- A visual workflow that guides you from pilot to production
- Detailed computer and application inventory
- Powerful computer-level search and drill-downs
- Guidance and insights into application and driver compatibility issues, with suggested fixes
- Data-driven application rationalization tools

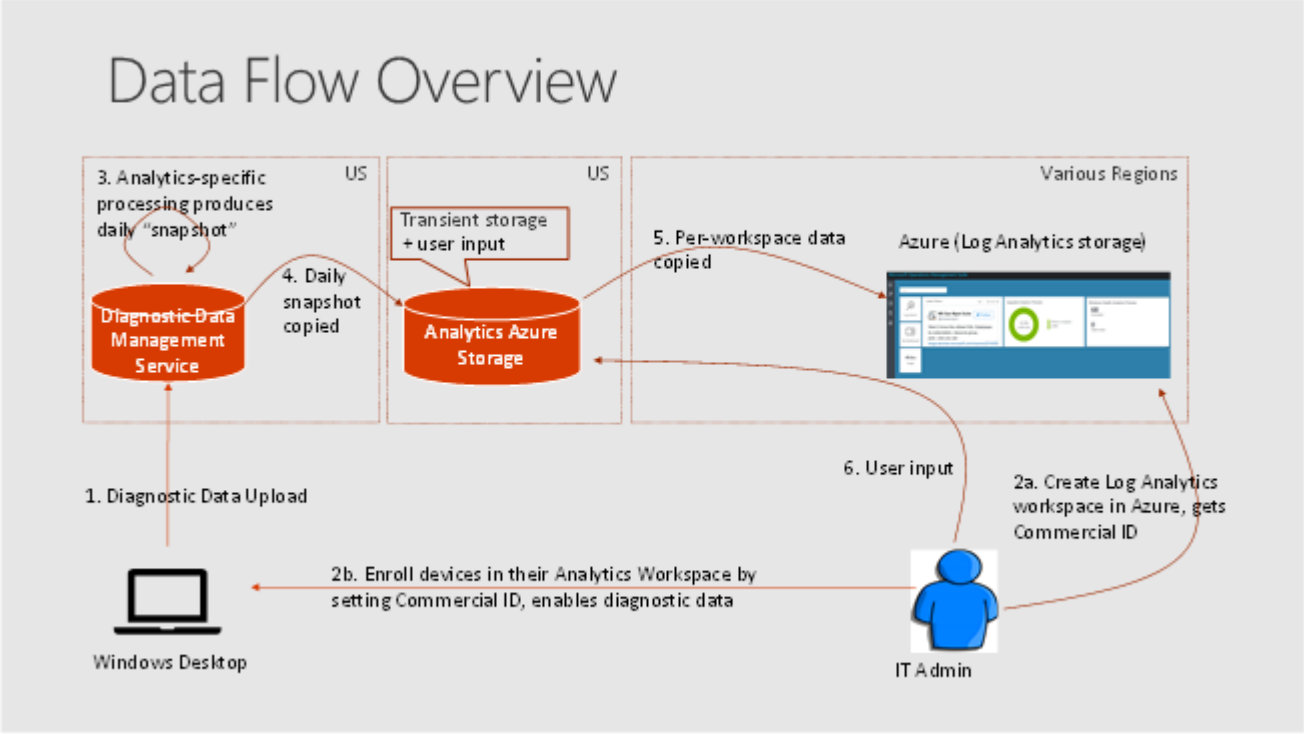
- Application usage information, allowing targeted validation; workflow to track validation progress and decisions
- Data export to commonly used software deployment tools, including System Center Configuration Manager

3. Windows Analytics and privacy

Windows Analytics is fully committed to privacy, centering on these tenets:

- **Transparency:** We fully document the Windows Analytics diagnostic events (see the links for additional information) so you can review them with your company's security and compliance teams. The Diagnostic Data Viewer lets you see diagnostic data sent from a given device (see Diagnostic Data Viewer Overview for details).
- **Control:** You ultimately control the level of diagnostic data you wish to share. In Windows 10 1709 we added a new policy to Limit enhanced diagnostic data to the minimum required by Windows Analytics
- **Security:** Your data is protected with strong security and encryption
- **Trust:** Windows Analytics supports the Microsoft Online Service Terms

The following illustration shows how diagnostic data flows from individual devices through the Diagnostic Data Service, Azure Log Analytics storage, and to your Log Analytics workspace:



The data flow sequence is as follows:

1. Diagnostic data is sent from devices to the Microsoft Diagnostic Data Management service, which is hosted in the US.
2. An IT administrator creates an Azure Log Analytics workspace. The administrator chooses the location, copies the Commercial ID (which identifies that workspace), and then pushes Commercial ID to devices they want to monitor. This is the mechanism that specifies which devices appear in which workspaces.

3. Each day Microsoft produces a "snapshot" of IT-focused insights for each workspace in the Diagnostic Data Management service.
4. These snapshots are copied to transient storage which is used only by Windows Analytics (also hosted in US data centers) where they are segregated by Commercial ID.
5. The snapshots are then copied to the appropriate Azure Log Analytics workspace.
6. If the IT administrator is using the Upgrade Readiness solution, user input from the IT administrator (specifically, the target operating system release and the importance and upgrade readiness per app) is stored in the Windows Analytics Azure Storage. (Upgrade Readiness is the only Windows Analytics solution that takes such user input.)

4. Manage Windows upgrades with Upgrade Readiness

Upgrading to new operating systems has traditionally been a challenging, complex, and slow process for many enterprises. Discovering applications and drivers and then testing them for potential compatibility issues have been among the biggest pain points.

With the release of Upgrade Readiness, enterprises now have the tools to plan and manage the upgrade process end to end, allowing them to adopt new Windows releases more quickly. With new Windows versions being released multiple times a year, ensuring application and driver compatibility on an ongoing basis is key to adopting new Windows versions as they are released. Windows Upgrade Readiness not only supports upgrade management from Windows 7, Windows 8.1 to Windows 10, but also Windows 10 upgrades in the Windows as a service model.

Microsoft developed Upgrade Readiness in response to demand from enterprise customers looking for additional direction and details about upgrading to Windows 10. Upgrade Readiness was built taking into account multiple channels of customer feedback, testing, and Microsoft's experience upgrading millions of devices to Windows 10.

With Windows diagnostic data enabled, Upgrade Readiness collects system, application, and driver data for analysis. We then identify compatibility issues that can block an upgrade and suggest fixes when they are known to Microsoft.

Use Upgrade Readiness to get:

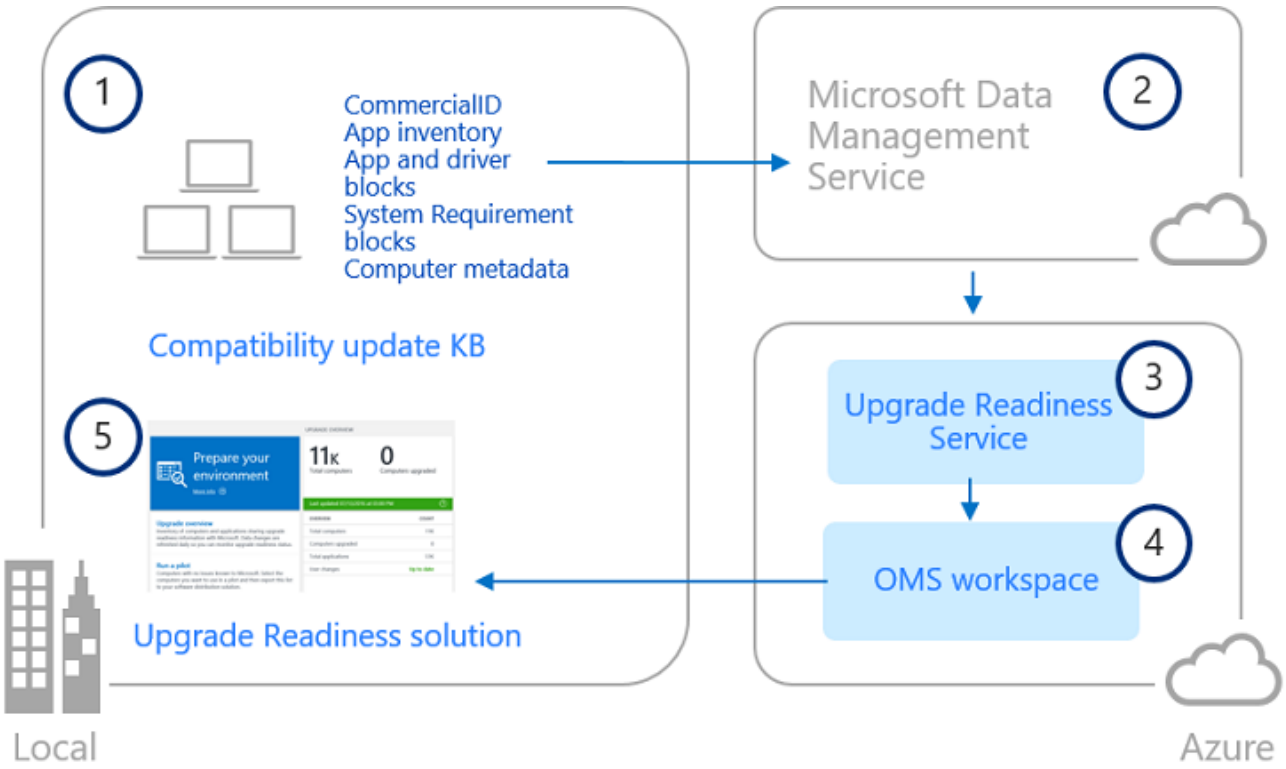
- A visual workflow that guides you from pilot to production
- Detailed computer and application inventory
- Powerful computer level search and drill-downs
- Guidance and insights into application and driver compatibility issues, with suggested fixes
- Data driven application rationalization tools
- Application usage information, allowing targeted validation; workflow to track validation progress and decisions
- Data export to commonly used software deployment tools, including System Center Configuration Manager

The Upgrade Readiness workflow steps you through the discovery and rationalization process until you have a list of computers that are ready to be upgraded.

Important For system, application, and driver data to be shared with Microsoft, you must configure user computers to send data.

4. Upgrade Readiness architecture

Microsoft analyzes system, application, and driver diagnostic data to help you determine when computers are upgrade-ready, allowing you to simplify and accelerate Windows upgrades in your organization. The diagram below illustrates how Upgrade Readiness components work together in a typical installation.



After you enable Windows diagnostic data on user computers and install the compatibility update KB (1), user computers send computer, application and driver diagnostic data to a secure Microsoft data center through the Microsoft Data Management Service (2). After you configure Upgrade Readiness, diagnostic data is analyzed by the Upgrade Readiness Service (3) and pushed to your OMS workspace (4). You can then use the Upgrade Readiness solution (5) to plan and manage Windows upgrades.

5. Upgrade Readiness requirements and costs

5.1 Windows 7 and Windows 8.1

To perform an in-place upgrade, user computers must be running the latest version of either Windows 7 SP1 or Windows 8.1. After you enable Windows diagnostic data, Upgrade Readiness performs a full inventory of computers so that you can see which version of Windows is installed on each computer.

The compatibility update that sends diagnostic data from user computers to Microsoft data centers works with Windows 7 SP1 and Windows 8.1 only. Upgrade Readiness cannot evaluate Windows XP or Windows Vista for upgrade eligibility.

If you need to update user computers to Windows 7 SP1 or Windows 8.1, use Windows Update or download and deploy the applicable package from the Microsoft Download Center.

Note: Upgrade Readiness is designed to best support in-place upgrades. In-place upgrades do not support migrations from BIOS to UEFI or from 32-bit to 64-bit architecture. If you need to migrate computers in these scenarios, use the wipe-and-reload method. Upgrade Readiness insights are still valuable in this scenario; however, you can ignore in-place upgrade specific guidance.

5.2 Windows 10

Keeping Windows 10 up to date involves deploying a feature update, and Upgrade Readiness tools help you prepare and plan for these Windows updates. The latest cumulative updates must be installed on Windows 10 computers to make sure that the required compatibility updates are installed. You can find the latest cumulative update on the Microsoft Update Catalog.

While Upgrade Readiness can be used to assist with updating devices from Windows 10 Long-Term Servicing Channel (LTSC) to Windows 10 Semi-Annual Channel, Upgrade Readiness does not support updates to Windows 10 LTSC. The Long-Term Servicing Channel of Windows 10 is not intended for general deployment, and does not receive feature updates, therefore it is not a supported target with Upgrade Readiness.

5.3 Operations Management Suite or Azure Log Analytics

Upgrade Readiness is offered as a solution in Microsoft Operations Management Suite (OMS) and Azure Log Analytics, a collection of cloud-based services for managing on premises and cloud computing environments.

If you're already using OMS or Azure Log Analytics, you'll find Upgrade Readiness in the Solutions Gallery.

Important

You can use either a Microsoft Account or a Work or School account to create a workspace. If your company is already using Azure Active Directory, use a Work or School account when you sign in to OMS. Using a Work or School account allows you to use identities from your Azure AD to manage permissions in OMS. You also need an Azure subscription to link to your OMS workspace. The account you used to create the workspace must have administrator permissions on the Azure subscription in order to link the workspace to the Azure account. Once the link has been established, you can revoke the administrator permissions.

5.4 System Center Configuration Manager integration

Upgrade Readiness can be integrated with your installation of Configuration Manager.

5.5 Windows Analytics costs

Windows Analytics solution	**Windows license requirements**	**Windows version requirements**	**Minimum diagnostic data requirements**
Upgrade Readiness	No additional requirements	Windows 7 with Service Pack 1, Windows 8.1, Windows 10	Basic level in most cases; Enhanced level to support Windows 10 app

Windows Analytics solution	Windows license requirements	Windows version requirements	Minimum diagnostic data requirements
			usage data and IE site discovery
Update Compliance	No additional requirements	Windows 10	Basic level
Device Health	**Any** of the following licenses: - Windows 10 Enterprise or Windows 10 Education per-device with active Software Assurance - Windows 10 Enterprise E3 or E5 per-device or per-user subscription (including Microsoft 365 F1, E3, or E5) - Windows 10 Education A3 or A5 (including Microsoft 365 Education A3 or A5) - Windows VDA E3 or E5 per-device or per-user subscription - Windows Server 2016 or later	Windows 10	- For Windows 10 version 1709 or later: Enhanced (Limited) - For earlier versions: Enhanced

Note

Regarding licensing requirements for Device Health, you do not need per-seat licensing, but only enough licenses to cover your total device usage. For example, if you have 100 E3 licenses, you can monitor 100 devices with Device Health.

Beyond the cost of Windows operating system licenses, there is no additional cost for using Windows Analytics. Within Azure Log Analytics, Windows Analytics is "zero-rated;" this means it is excluded from data limits and costs regardless of the Azure Log Analytics pricing tier you have chosen. To be more specific, Azure Log Analytics is available in different pricing tiers as described in Pricing - Log Analytics.

- If you are using the free tier, which has a cap on the amount of data collected per day, the Windows Analytics data will not count towards this cap. You will be able to collect all the Windows Analytics data from your devices and still have the full cap available for collecting additional data from other sources.
- If you are using a paid tier that charges per GB of data collected, the Windows Analytics data will not be charged. You will be able to collect all the Windows Analytics data from your devices and not incur any costs.

Note that different Azure Log Analytics plans have different data retention periods, and the Windows Analytics solutions inherit the workspace's data retention policy. So, for example, if your workspace is on the free plan then Windows Analytics will retain the last weeks' worth of "daily snapshots" that are collected in the workspace.

5.6 Important information about this release

Before you get started configuring Upgrade Analytics, review the following tips and limitations about this release.

Upgrade Readiness does not support on-premises Windows deployments. Upgrade Readiness is built as a cloud service, which allows Upgrade Readiness to provide you with insights based on the data from user computers and other Microsoft compatibility services. Cloud services are easy to get up and running and are cost-effective because there is no requirement to physically implement and maintain services on-premises.

In-region data storage requirements. Windows diagnostic data from user computers is encrypted, sent to, and processed at Microsoft-managed secure data centers located in the US. Our analysis of the upgrade readiness-related data is then provided to you through the Upgrade Readiness solution in the Microsoft Operations Management Suite (OMS) portal. Upgrade Readiness is supported in all OMS regions; however, selecting an international OMS region does not prevent diagnostic data from being sent to and processed in Microsoft's secure data centers in the US.

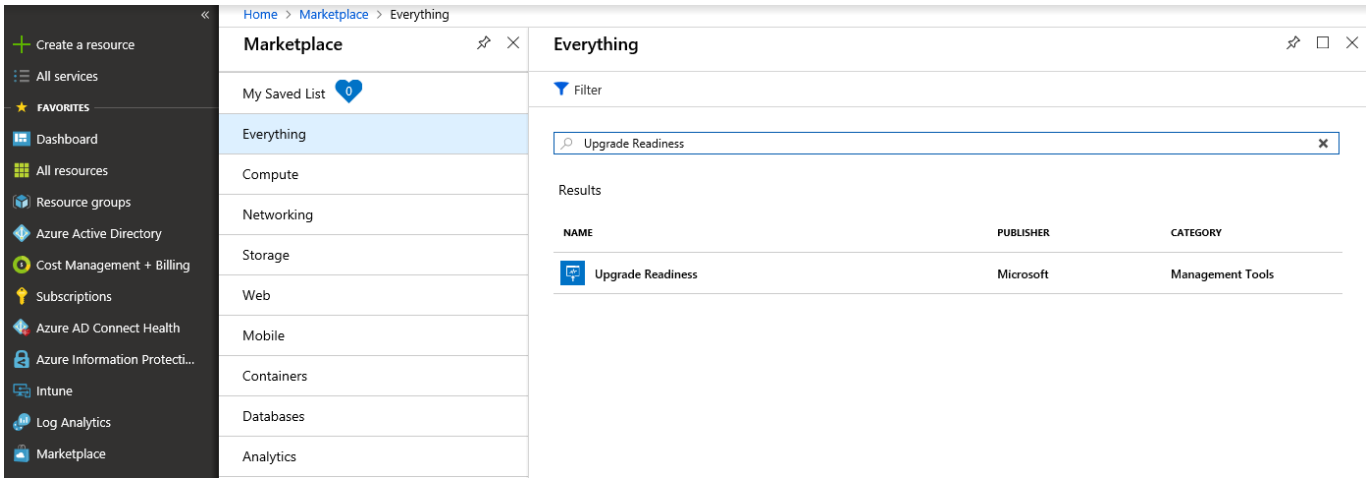
6. Get started with Upgrade Readiness

This topic explains how to obtain and configure Upgrade Readiness for your organization.

You can use Upgrade Readiness to plan and manage your upgrade project end-to-end. Upgrade Readiness works by establishing communications between computers in your organization and Microsoft. Upgrade Readiness collects computer, application, and driver data for analysis. This data is used to identify compatibility issues that can block your upgrade and to suggest fixes that are known to Microsoft.

6.1 Add the Upgrade Readiness solution to your Azure subscription

Sign in to the Azure Portal with your work or school account or a Microsoft account. If you don't already have an Azure subscription you can create one (including free trial options) through the portal. In the Azure portal go to **Marketplace**, search for "Upgrade Readiness", and then select **Create** on the **Upgrade Readiness** solution.



Upgrade Readiness

Microsoft

The Upgrade Readiness solution gives enterprises the tools to plan and manage the upgrade process end to end. Using information known to Microsoft, we provide recommendations for resolving blocking issues, allowing you to streamline and accelerate Windows upgrades.

With Windows telemetry enabled, Upgrade Readiness collects and analyzes your data to identify device, application, and driver compatibility issues that can block your upgrade.

The Upgrade Readiness visual workflow steps you through the discovery and rationalization process until you have a list of devices that are ready to be upgraded.

With Upgrade Readiness you can:

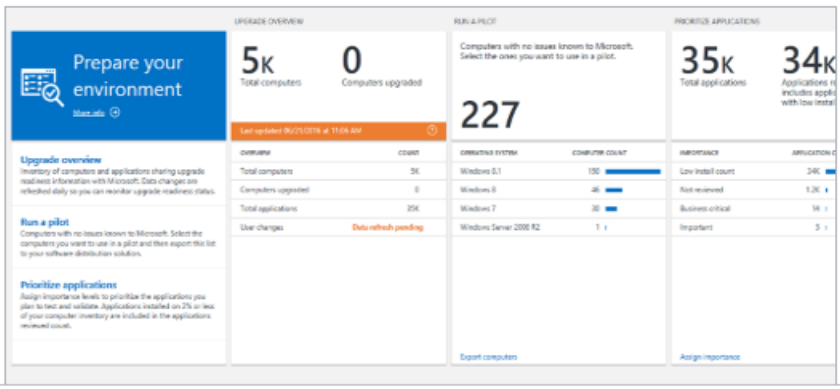
• Decide which computers you want to use in a pilot and then export this list to your software deployment tool

• See which applications are used the most, grouped by the computers they're installed on

• Decide which computers are ready to be upgraded and then export this list to your software deployment tool

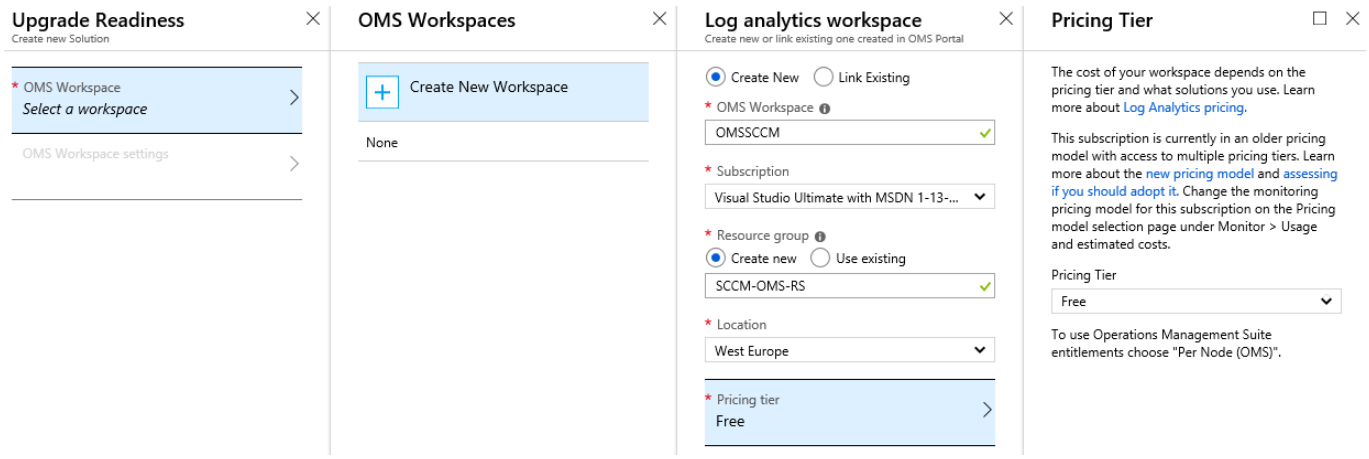
IMPORTANT: For upgrade readiness information to be shared with and analyzed by Upgrade Readiness, you must enable and configure Windows telemetry on user computers. After you've added this solution to your workspace, go to Connected Sources in Settings for information about how to enable telemetry. Learn more.

Save for later

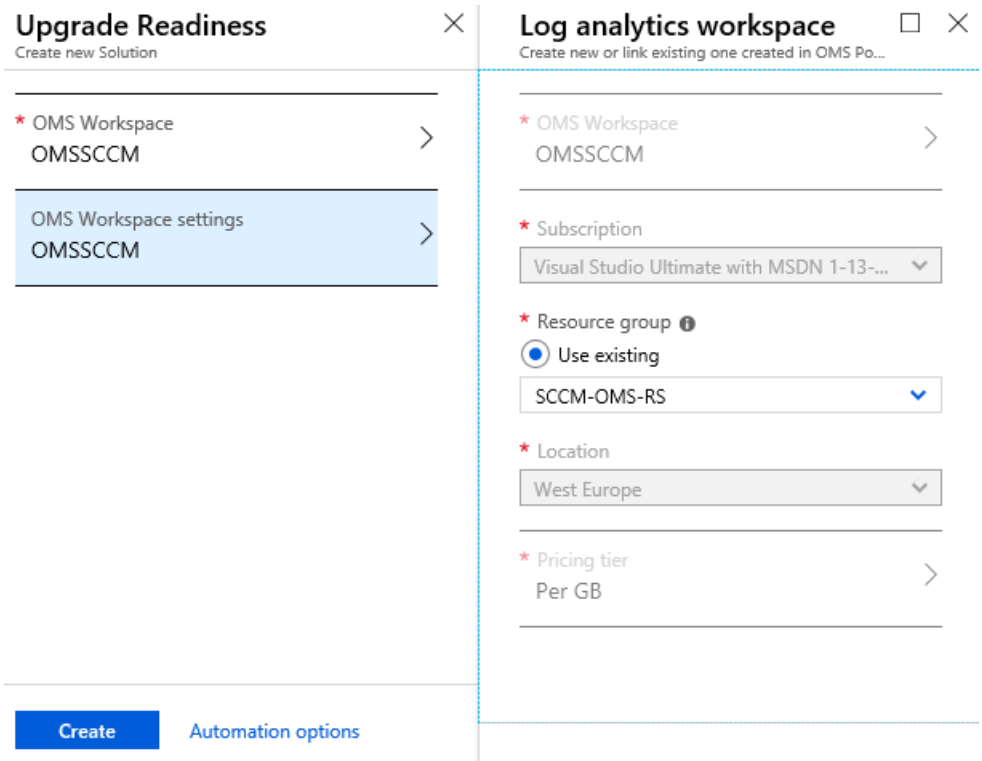


Create

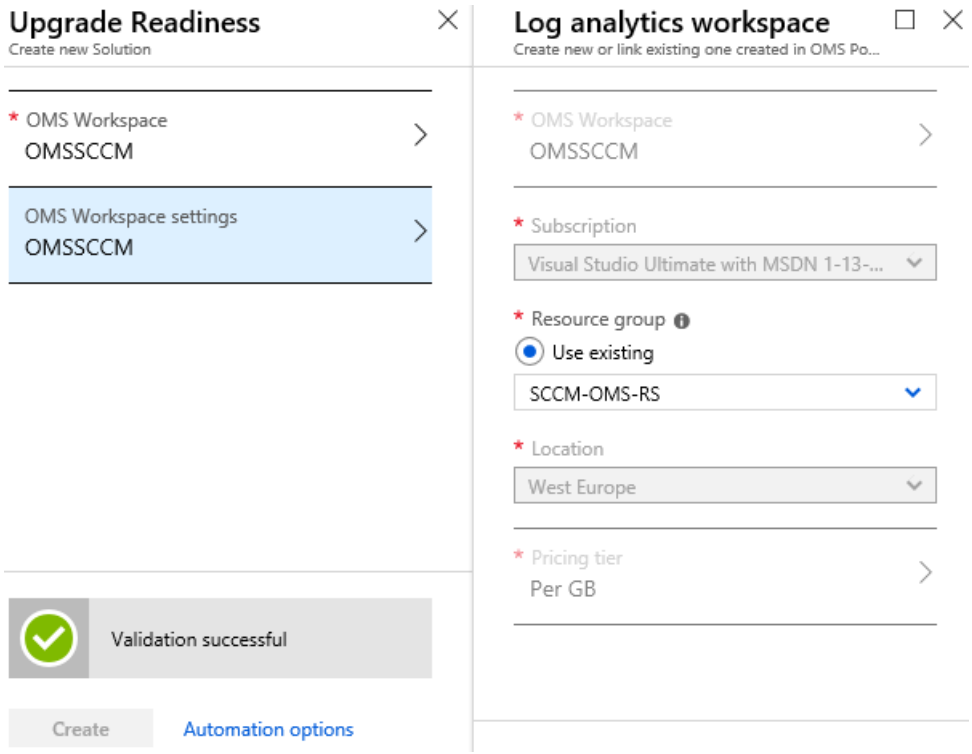
Choose an existing workspace or create a new workspace to host the Upgrade Readiness solution.



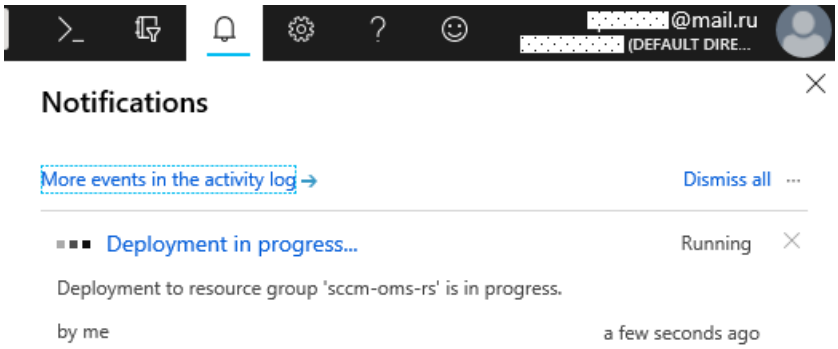
If you create a new workplace, provide an **OMS Workplace name**, **Resource group name**, choose **Azure subscription**, **Location** and **Pricing tier**. After creating the resource group click on **OMS Workplace settings** and choose created resource group, then click **Create**:



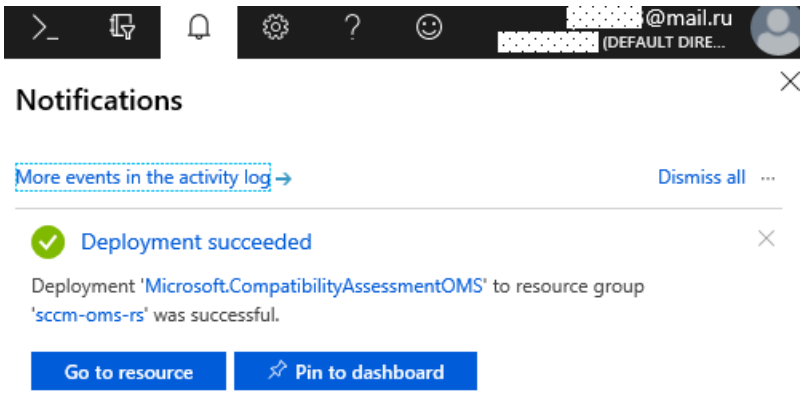
Wait for a successful validation:



And click **Create** again. Then go to **Notifications** and wait until service is created.

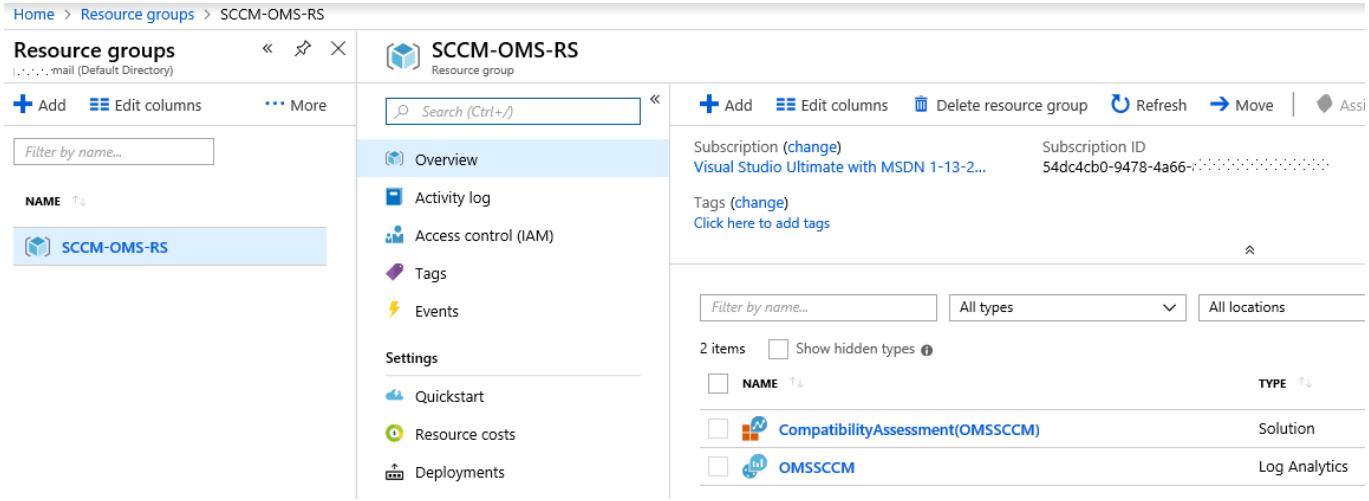


When creating the resource group is finished **Go to resource**:

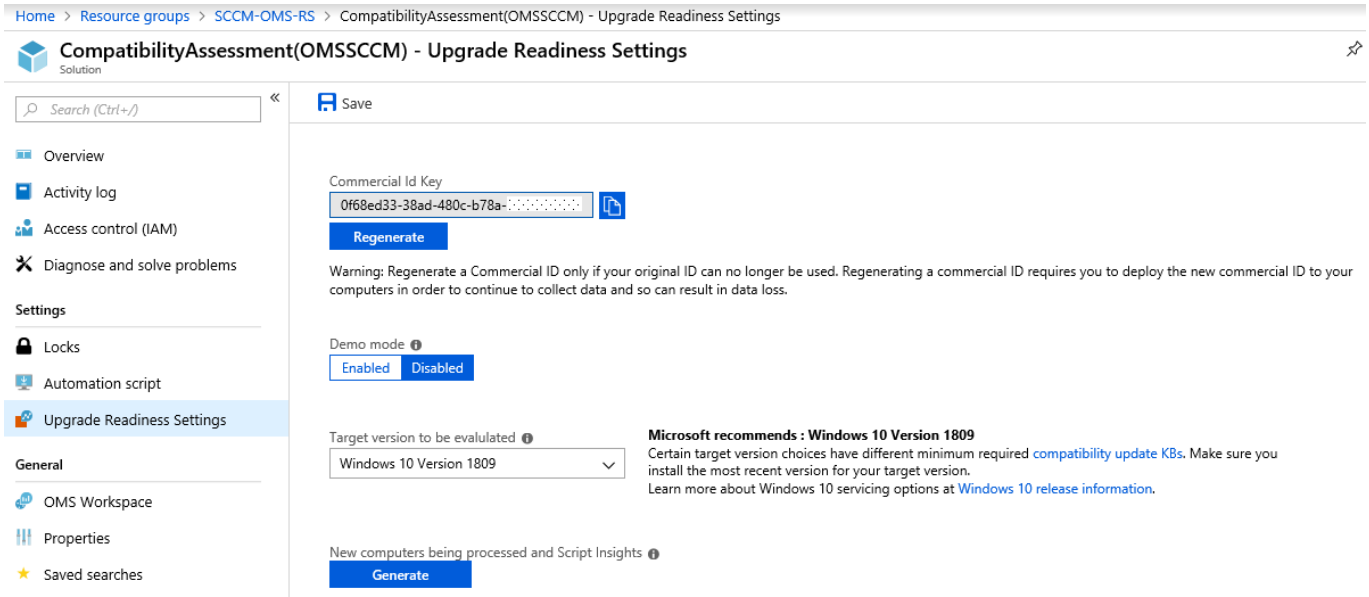


6.2 The Upgrade Readiness configuration settings

Navigate to **Overview** of your resource group and click on **CompatibilityAssessment** solution:



On the **Upgrade Readiness settings** page copy your **Commercial ID** and specify **Windows 10 target version to be evaluated**:



Then click **Save**.

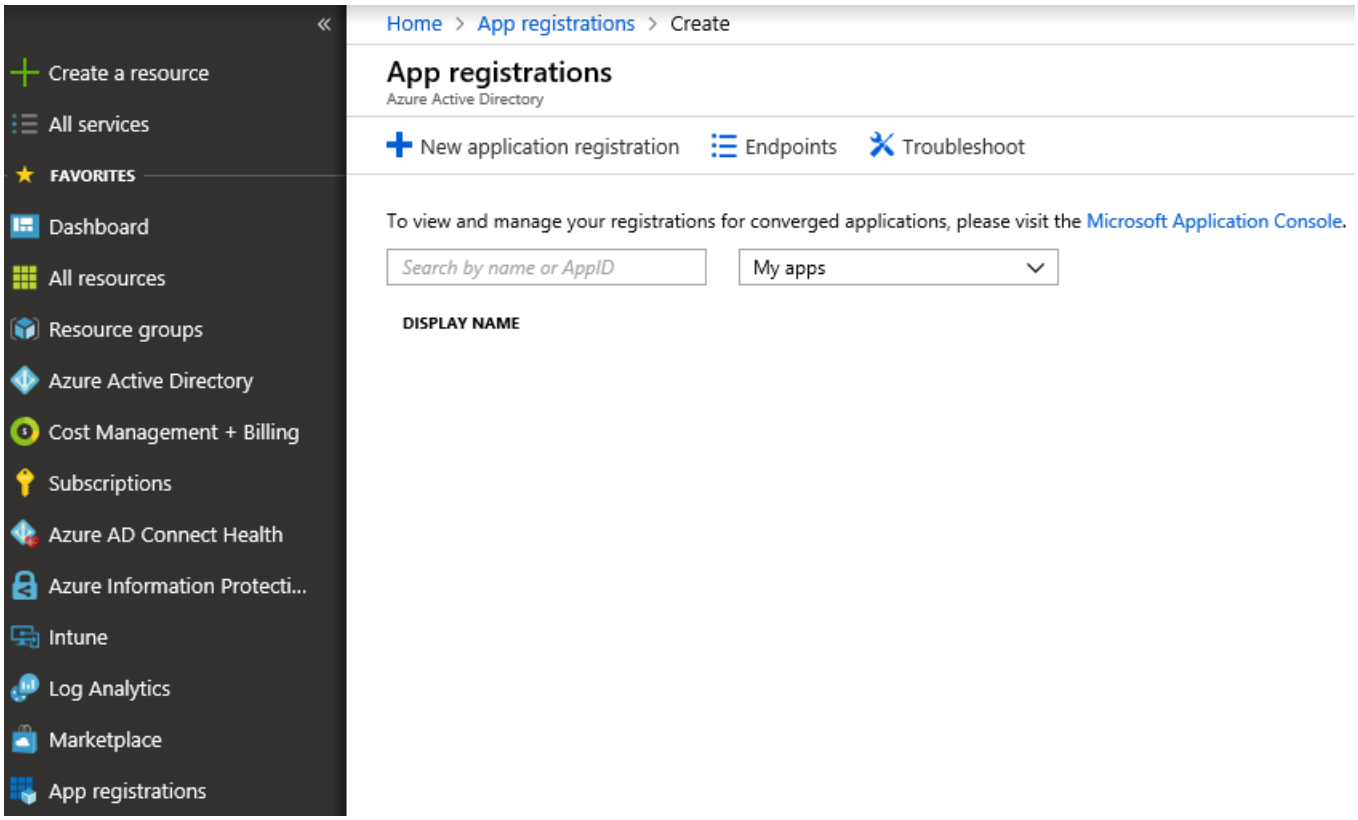
6.3 Integrate Upgrade Readiness with Configuration Manager

Integrate Upgrade Readiness with Configuration Manager to access client upgrade compatibility data in the Configuration Manager console. Then use this data to create collections, and target devices for upgrade or remediation.

6.3.1 Web app creation

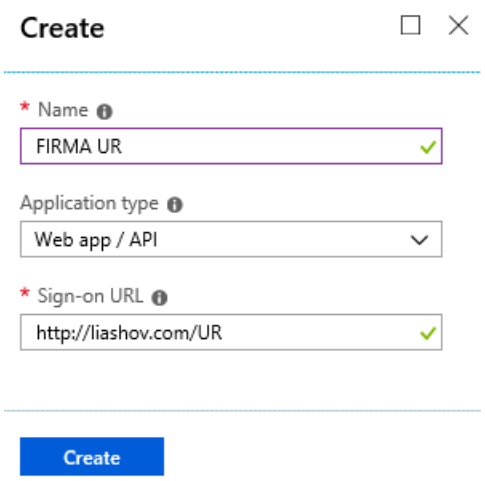
Open the Azure Management portal (https://portal.azure.com) and go to **App registrations** pane. The Azure services wizard uses this app registration to allow Configuration Manager to communicate securely with Azure AD and connect your infrastructure to your Upgrade Readiness data.

Click **Create**:

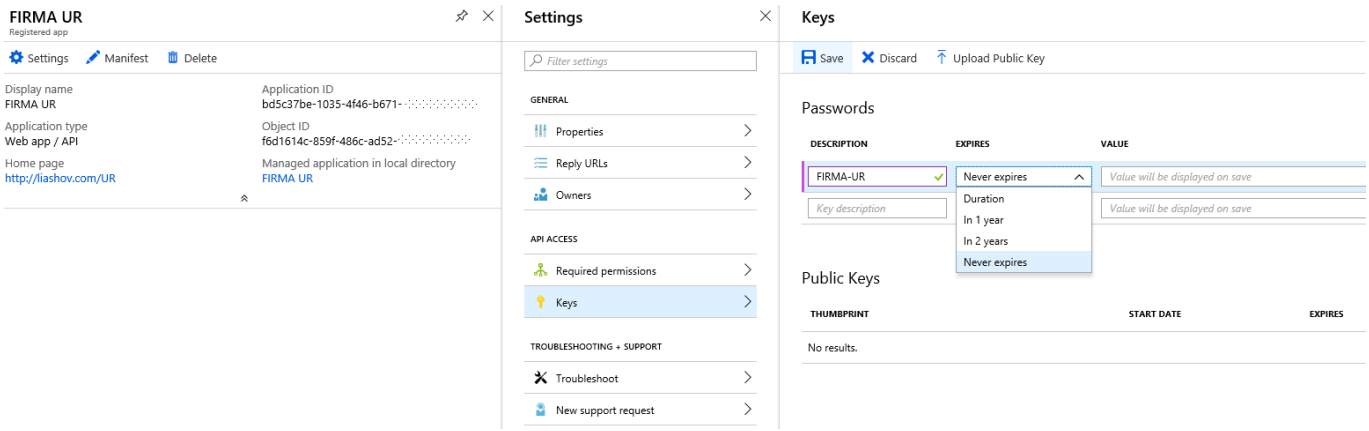


Enter the following information :

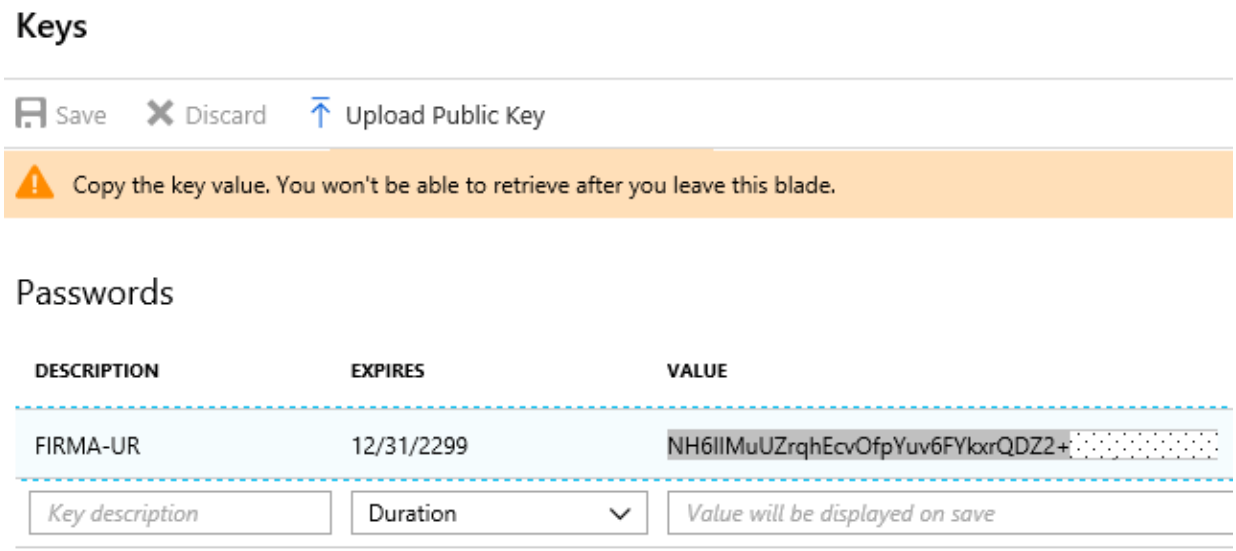
- **Name:** Specify a name for the application
- **Type: Web app / API**
- **Sign-on URL:** Specify any URL. (This URL doesn't need to resolve)



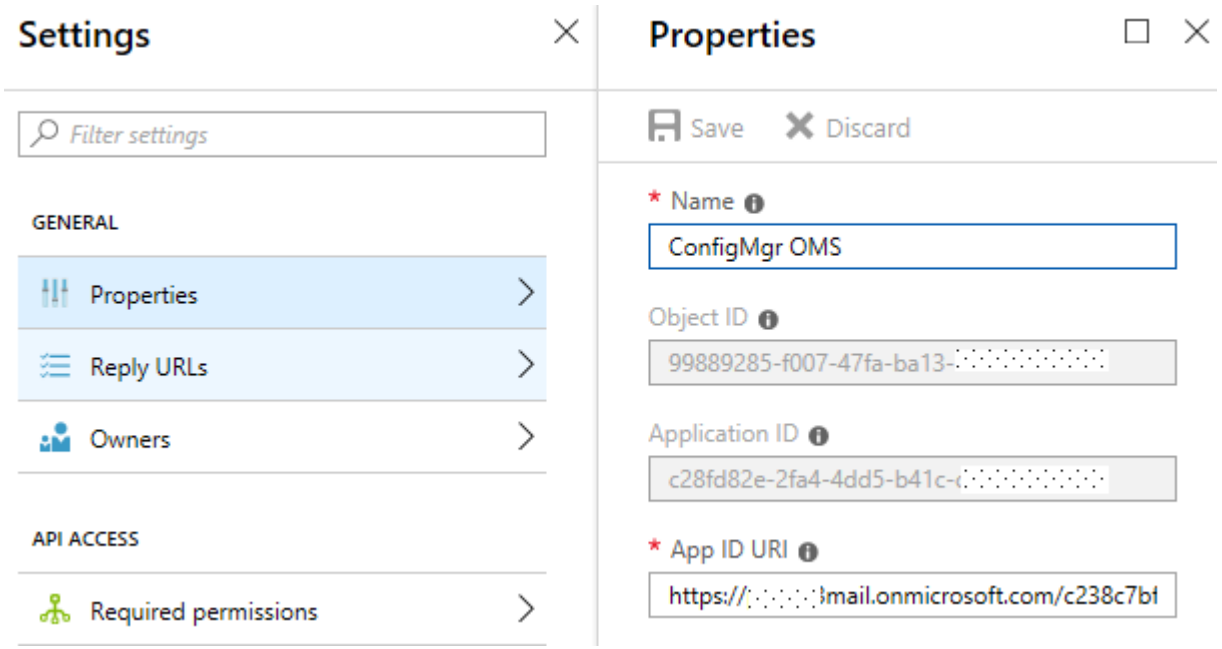
And click **Create**. Select your application and click on **All Settings**. Click on **Keys,** enter a name, select a duration and click **Save.** The key will be created after clicking **Save** and can only be retrieved on this page:



Copy the **Key** and **Application ID** from this page. It will be needed later.



Still in your application, click on **General / Properties** and copy the **App ID URI**:

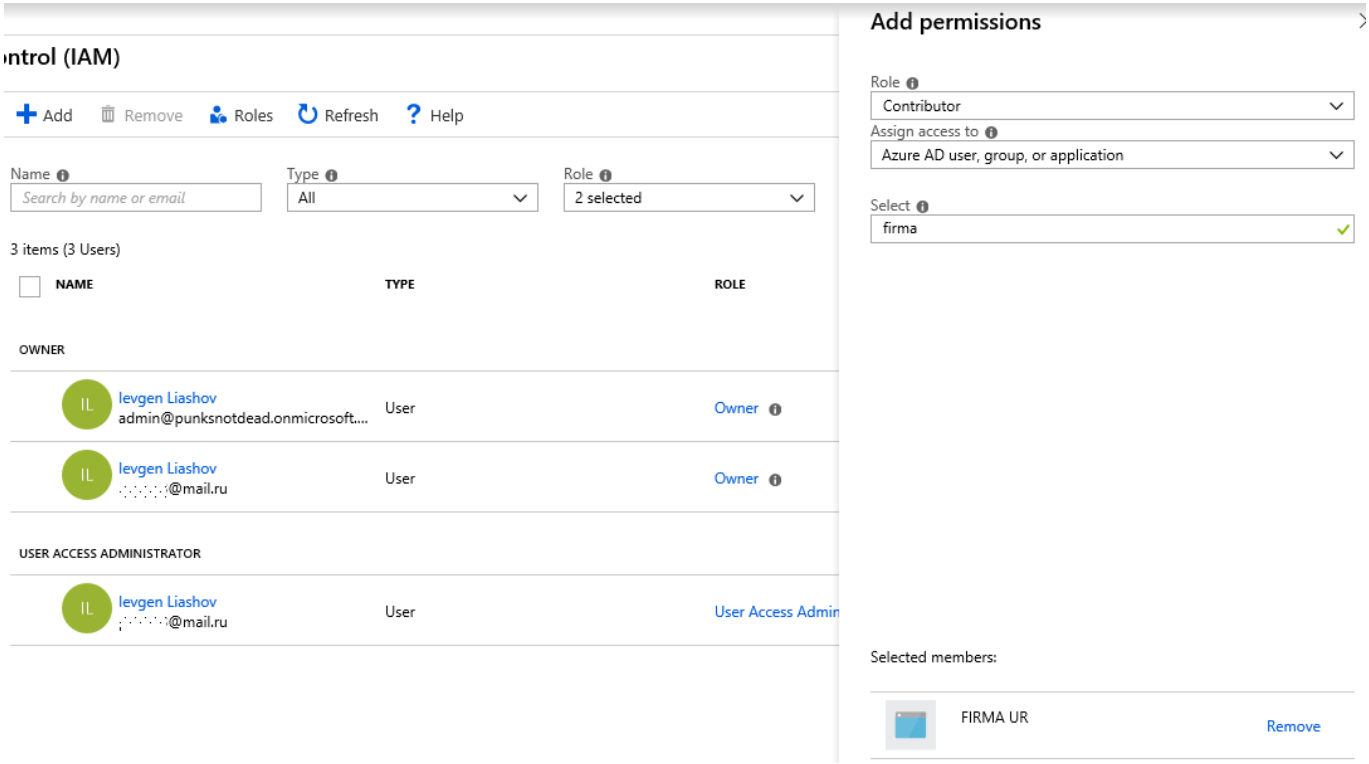


6.3.2 Web app permissions

Grant *contributor* permissions to the app itself, not to an Azure AD user identity. It's the registered app that accesses the data on behalf of your Configuration Manager infrastructure. To grant the permissions, search for the name of the app registration in the **Add users** area when assigning the permission.

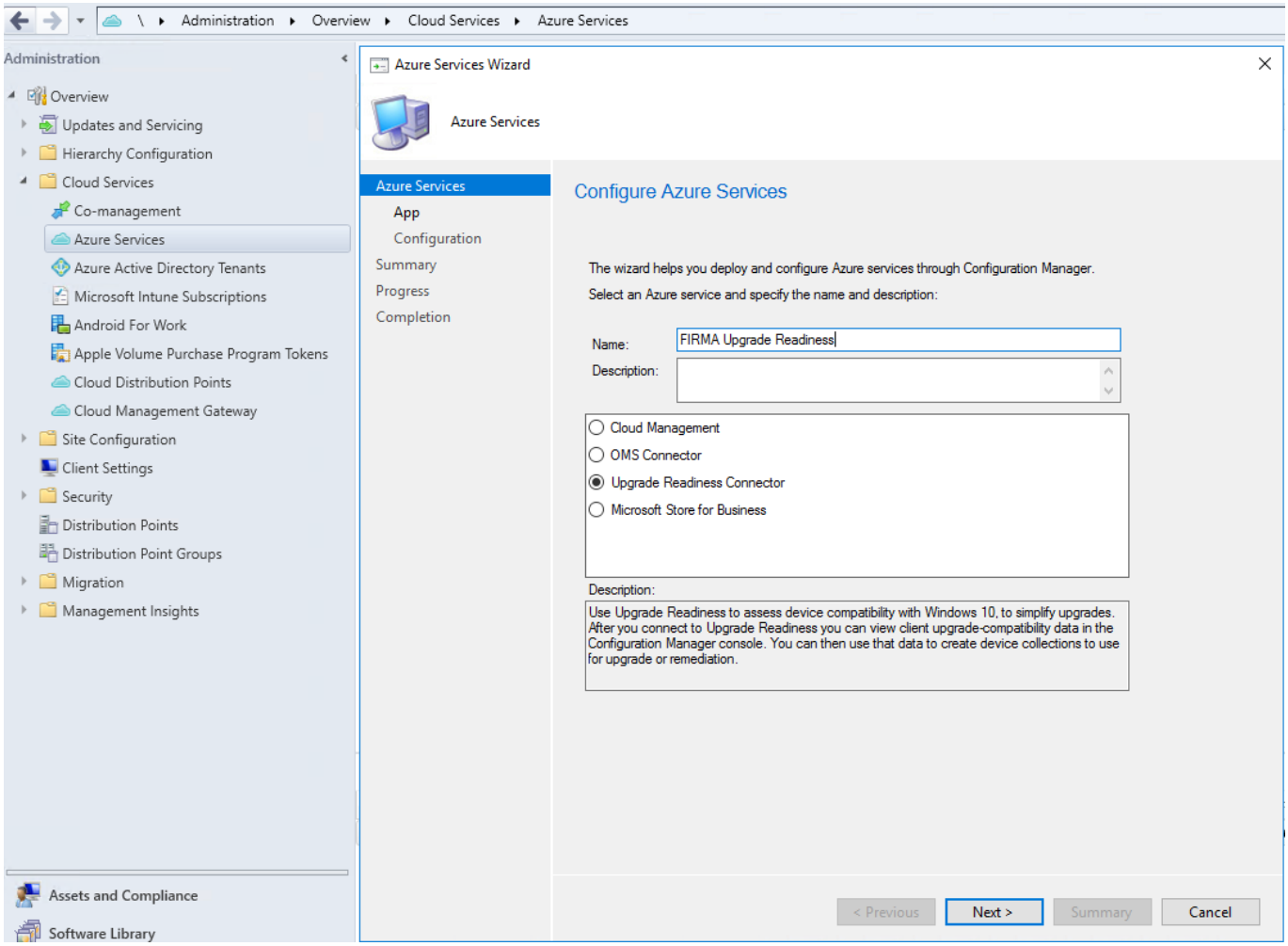
This process is the same as when providing Configuration Manager with permissions to Log Analytics. These steps must be completed before the app registration is imported into Configuration Manager with the *Azure services wizard*.

Go to **Resource groups,** select the resource group in which you create your OMS Workspace. Select **Access Control (IAM)**, then click **Add**. Select the **Contributor** role and select your application, click **Save**.



6.3.3 Configure the SCCM Upgrade Readiness Connector

Open the SCCM Console. Go to **Administration / Cloud Services / Azure Services.** Right-click **Azure Services** and select **Configure Azure Services**. On the **Azure Services** tab, name your connection and select **Upgrade Readiness Connector**:

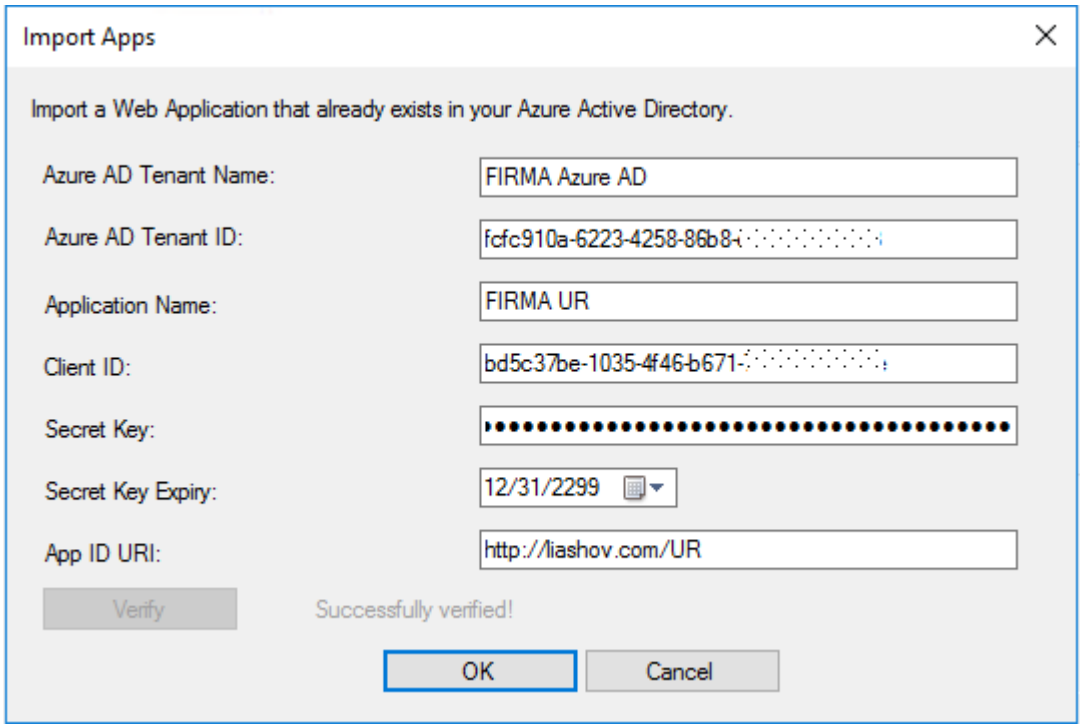


On the **App** page, select your Azure environment and click **Import**.

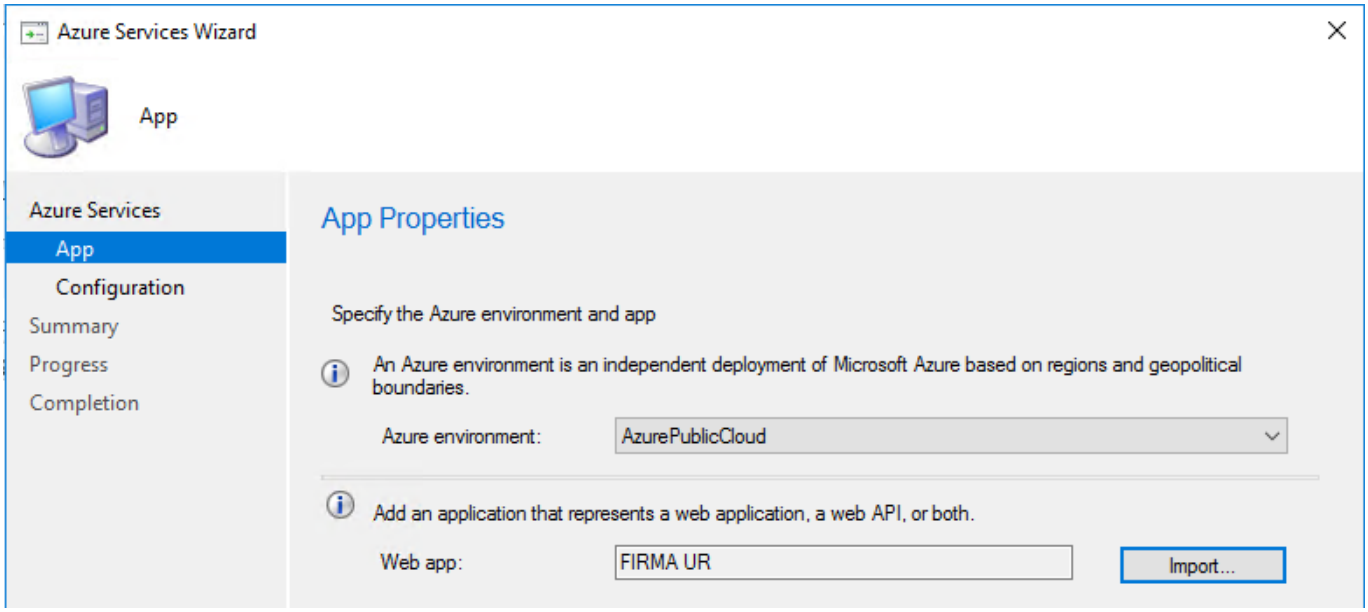
On the **Import Apps** page, specify the following information :

- **Azure AD Tenant** Name: Specify any name
- **Azure AD Tenant ID**: Specify the Azure AD tenant – You can find this information under **Azure Active Directory / Properties**
- **Application Name** – Specify your application name
- **Client ID**: Specify the **Application ID** of the created Azure AD app. You can see where to find this information in the previous steps
- **Secret key**: Specify the Client secret key of the created Azure AD app. You can see where to find this information in the previous steps
- **Secret Key expiry:** Specify the expiration date of your key
- **App ID URI:** Specify the **App ID URI** of the created Azure AD app. You can see where to find this information in the previous steps

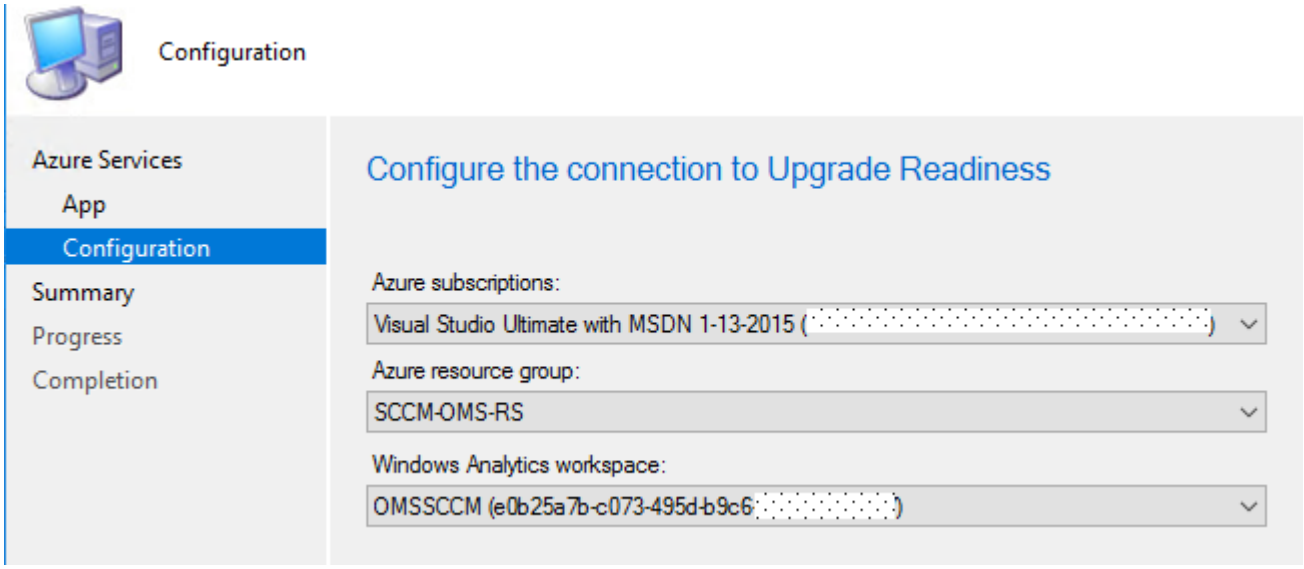
Click on **Verify** then **OK**:



Check **App Properties** again:



Then click **Next**. On the configuration page, the information will be pre-populate once the Azure AD app has enough permissions on the resource group. If the fields are empty, your application doesn't have the necessary rights.

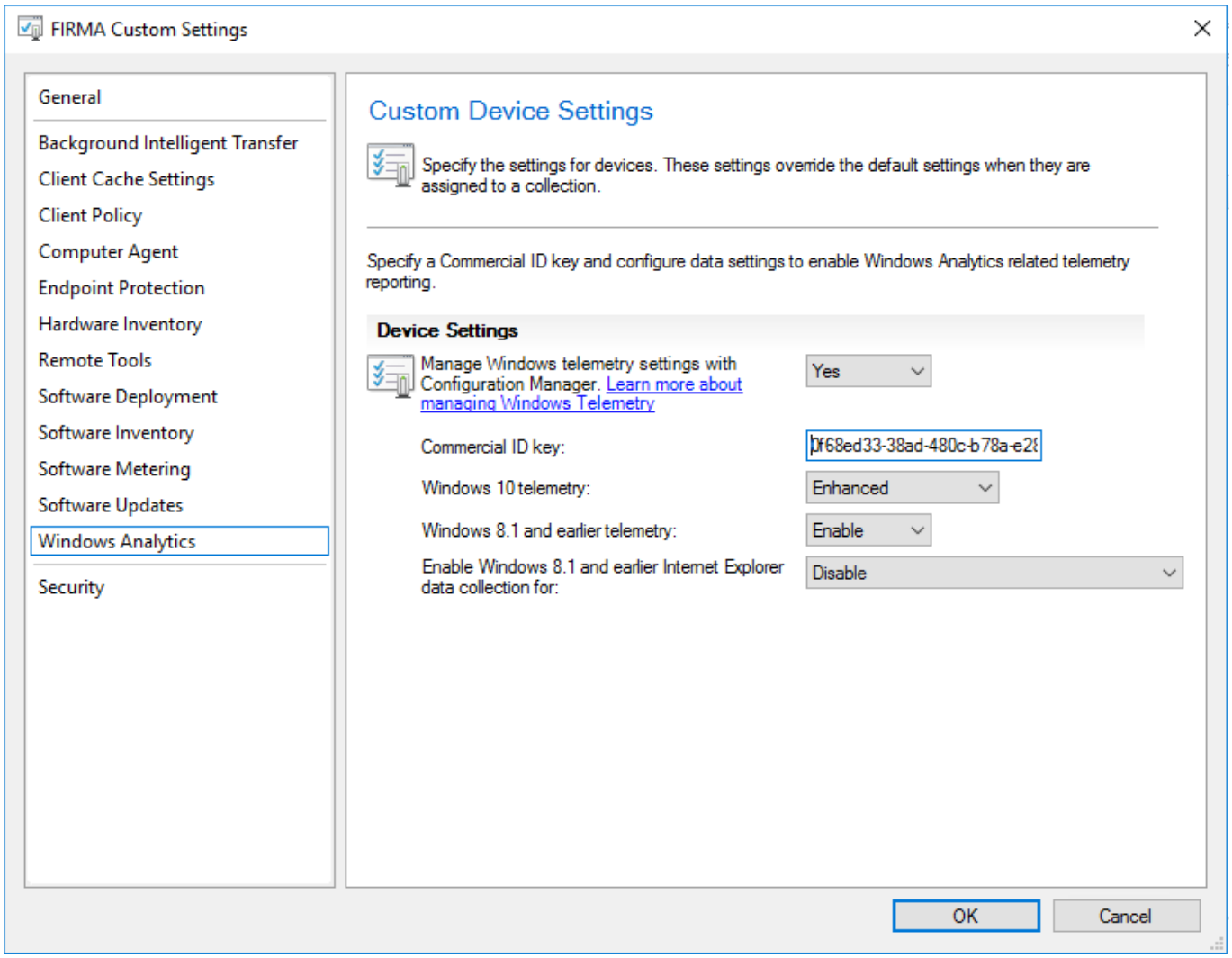


And finish the configuration wizard.

6.3.4 Configure SCCM device settings

Go to SCCM client settings, enable Windows Analytics section and configure next parameters:

- **Manage Windows telemetry**: Yes
- **Commercial ID key**: provide the key you collected before
- **Windows 10 telemetry**: Enhanced
- **Windows 8.1 and earlier telemetry**: Enable
- **Enable Windows 8.1 and earlier Internet Explorer data collection for**: Disabled



Then deploy these settings on a collection you want to enable collecting telemetry for Windows Analytics.

6.4 Pre-configuring infrastructure for supporting Windows Analytics

Microsoft uses a unique commercial ID to map information from user computers to your OMS workspace. This should be generated for you automatically. Copy your commercial ID key in OMS and then deploy it to user computers.

6.4.1 Enable data sharing

To enable data sharing, configure your proxy server to whitelist the following endpoints. You might need to get approval from your security group to do this.

Endpoint	Function
https://v10.events.data.microsoft.com	Connected User Experience and Diagnostic component endpoint for use with Windows 10, version 1803
https://v10.vortex-win.data.microsoft.com	Connected User Experience and Diagnostic component endpoint for Windows 10, version 1709 or earlier
https://vortex-win.data.microsoft.com	Connected User Experience and Diagnostic component endpoint for operating systems older than Windows 10
https://v10c.events.data.microsoft.com	Connected User Experience and Diagnostic component endpoint for use with Windows versions that have KB4458469 installed
https://settings-win.data.microsoft.com	Enables the compatibility update to send data to Microsoft.
http://adl.windows.com	Allows the compatibility update to receive the latest compatibility data from Microsoft.
https://watson.telemetry.microsoft.com	Windows Error Reporting (WER); required for Device Health and Update Compliance AV reports. Not used by Upgrade Readiness.
https://oca.telemetry.microsoft.com	Online Crash Analysis; required for Device Health and Update Compliance AV reports. Not used by Upgrade Readiness.
https://login.live.com	This endpoint is required by Device Health to ensure data integrity and provides a more reliable device identity for all of the Windows Analytics solutions on Windows 10. If you want to disable end-user managed service account (MSA) access, you should apply the appropriate policy instead of blocking this endpoint.

Endpoint	Function
https://www.msftncsi.com	Windows Error Reporting (WER); required for Device Health to check connectivity.
https://www.msftconnecttest.com	Windows Error Reporting (WER); required for Device Health to check connectivity.

6.4.2 Configuring endpoint access with SSL inspection

To ensure privacy and data integrity Windows checks for a Microsoft SSL certificate when communicating with the diagnostic data endpoints. Accordingly SSL interception and inspection is not possible. To use Windows Analytics services you should exclude the above endpoints from SSL inspection.

6.4.3 Configuring endpoint access with proxy server authentication

If your organization uses proxy server authentication for outbound traffic, use one or more of the following approaches to ensure that the diagnostic data is not blocked by proxy authentication:

- **Best option: Bypass** Configure your proxy servers to **not** require proxy authentication for traffic to the diagnostic data endpoints. This is the most comprehensive solution and it works for all versions of Windows 10.
- **User proxy authentication:** Alternatively, you can configure devices to use the logged on user's context for proxy authentication. First, update the devices to Windows 10, version 1703 or later. Then, ensure that users of the devices have proxy permission to reach the diagnostic data endpoints. This requires that the devices have console users with proxy permissions, so you couldn't use this method with headless devices.
- **Device proxy authentication:** Another option--the most complex--is as follows: First, configure a system level proxy server on the devices. Then, configure these devices to use machine-account-based outbound proxy authentication. Finally, configure proxy servers to allow the machine accounts access to the diagnostic data endpoints.

6.4.4 Deploy the compatibility update and related updates

The compatibility update scans your devices and enables application usage tracking. If you don’t already have these updates installed, you can download the applicable version from the Microsoft Update Catalog or deploy it using Windows Server Update Services (WSUS) or your software distribution solution, such as System Center Configuration Manager.

Operating System	Updates
Windows 10	Windows 10 includes the compatibility update, so you will automatically have the latest compatibility update so long as you continue to keep your Windows 10 devices up-to-date with cumulative updates.
Windows 8.1	KB 2976978 Performs diagnostics on the Windows 8.1 systems that participate in the Windows Customer Experience Improvement Program. These diagnostics help determine whether compatibility issues might be encountered when the latest Windows operating system is installed. For more information about this update, see https://support.microsoft.com/kb/2976978
Windows 7 SP1	KB2952664 Performs diagnostics on the Windows 7 SP1 systems that participate in the Windows Customer Experience Improvement Program. These diagnostics help determine whether compatibility issues might be encountered when the latest Windows operating system is installed. For more information about this update, see https://support.microsoft.com/kb/2952664

Important

Restart devices after you install the compatibility updates for the first time.

6.5 Enroll a few pilot devices

6.5.1 Overview of Upgrade Readiness deployment script

You can use the Upgrade Readiness deployment script to automate and verify your deployment. The recommended way is manually running this script on a few representative devices to verify things are properly configured and the device can connect to the diagnostic data endpoints. Make sure to run the pilot version of the script, which will provide extra diagnostics.

After data is sent from devices to Microsoft, it generally takes 48-56 hours for the data to populate in Windows Analytics. The compatibility update takes several minutes to run. If the update does not get a chance to finish running or if the computers are inaccessible (turned off or sleeping for example), data will take longer to populate in Windows Analytics. For this reason, you can expect most of your devices to be populated in Windows Analytics in about 1-2 weeks after deploying the update and configuration to user computers.

Either version of the script will do the following:

- Sets commercial ID key + CommercialDataOptIn + RequestAllAppraiserVersions keys.
- Verifies that user computers can send data to Microsoft (note that this check does not currently work in auth proxy environments).
- Verifies that the latest version of KB package 10.0.x is installed (version 10.0.14913 or later is

required).
- Checks whether the computer has a pending restart.
- If enabled, turns on verbose mode for troubleshooting.
- Initiates the collection of the telemetry data that Microsoft needs to assess your organization's upgrade readiness.
- If enabled, displays the script's progress in a cmd window, providing you immediate visibility into issues (success or fail for each step) and/or writes to log file.

6.5.2 Running the script manually

There should be no performance impact caused by the script. The script is a light wrapper of Windows in-box components that undergo performance testing and optimization to avoid any performance impact. However, typically the script is scheduled to be run outside of working hours.

Do not run the script at each sign-on. It is recommended to run the script once every 30 days.

The length of time the script takes to run on each system depends on the number of apps and drivers, and the type of hardware. Anti-virus software scanning simultaneously can increase the script run time, but the script should require no longer than 10 minutes to run, and typically the time is much shorter. If the script is observed running for an extended period of time, please run the Pilot script, and collect logs to share with Microsoft. Log files are created in the drive that is specified in the RunConfig.bat file. By default, this is set to: **%SystemDrive%\UADiagnostics**.

To run the Upgrade Readiness deployment script:

1. Download the Upgrade Readiness deployment script and extract the .zip file. Inside, there are two folders: **Pilot** and **Deployment**. The **Pilot** folder contains advanced logging that can help troubleshoot issues and is intended to be run from an elevated command prompt.
   The **Deployment** folder offers a lightweight script intended for broad deployment through ConfigMgr or other software deployment system. We recommend manually running the Pilot version of the script on 5-10 machines to verify that everything is configured correctly. Once you have confirmed that data is flowing successfully, proceed to run the Deployment version throughout your organization.
2. Edit the following parameters in RunConfig.bat:

a. Provide a storage location for log information. You can store log information on a remote file share or a local directory. If the script is blocked from creating the log file for the given path, it creates the log files in the drive with the Windows directory. Example: %SystemDrive%\UADiagnostics

b. Input your commercial ID key. This can be found in your OMS workspace under Settings -> Connected Sources -> Windows Telemetry.

c. By default, the script sends log information to both the console and the log file. To change the default behavior, use one of the following options:

logMode = 0 log to console only

logMode = 1 log to file and console

logMode = 2 log to file only

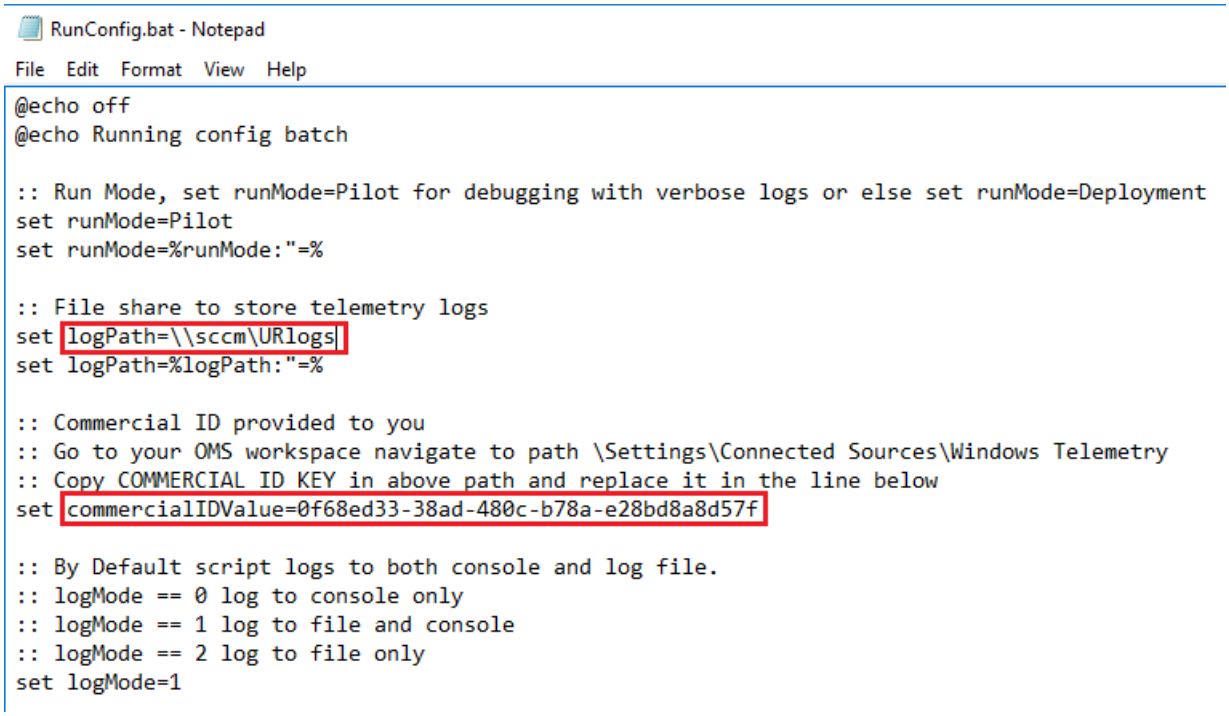
3. To enable Internet Explorer data collection, set AllowIEData to IEDataOptIn. By default, AllowIEData is set to Disable. Then use one of the following options to determine what Internet Explorer data can be collected:

IEOptInLevel = 0 Internet Explorer data collection is disabled

IEOptInLevel = 1 Data collection is enabled for sites in the Local intranet + Trusted sites + Machine local zones

IEOptInLevel = 2 Data collection is enabled for sites in the Internet + Restricted sites zones

IEOptInLevel = 3 Data collection is enabled for all sites



4. A recent version of the deployment script is configured to collect and send diagnostic and debugging data to Microsoft. If you wish to disable sending diagnostic and debugging data to Microsoft, set **AppInsightsOptIn = false**. By default, **AppInsightsOptIn** is set to **true**.

   The data that is sent is the same data that is collected in the text log file that captures the events and error codes while running the script. This file is named in the following format: **UA_yyyy_mm_dd_hh_mm_ss_machineID.txt**. Log files are created in the drive that is specified in the RunConfig.bat file. By default this is set to: **%SystemDrive%\UADiagnostics**.

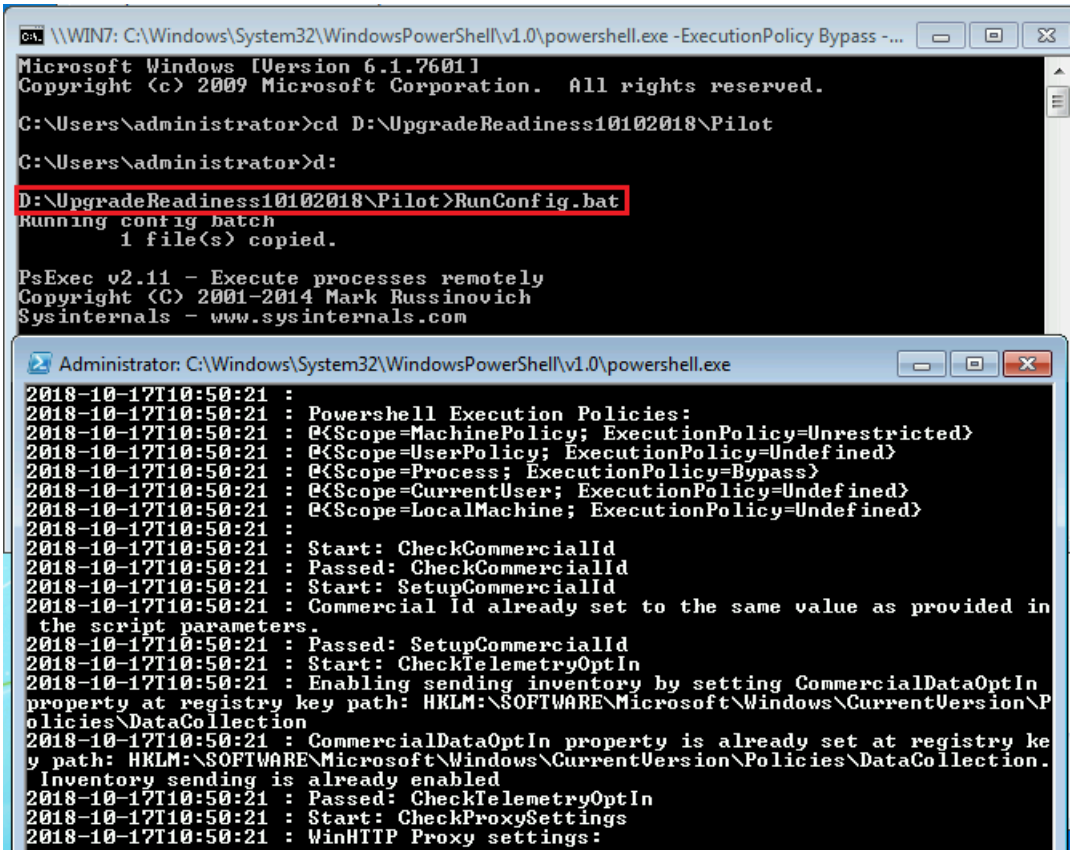
   This data gives us the ability to determine the status of your machines and to help troubleshoot issues. If you choose to opt-in to and send this data to Microsoft, you must also allow https traffic to be sent to the following wildcard endpoints:

   vortex.data.microsoft.com
   settings.data.microsoft.com

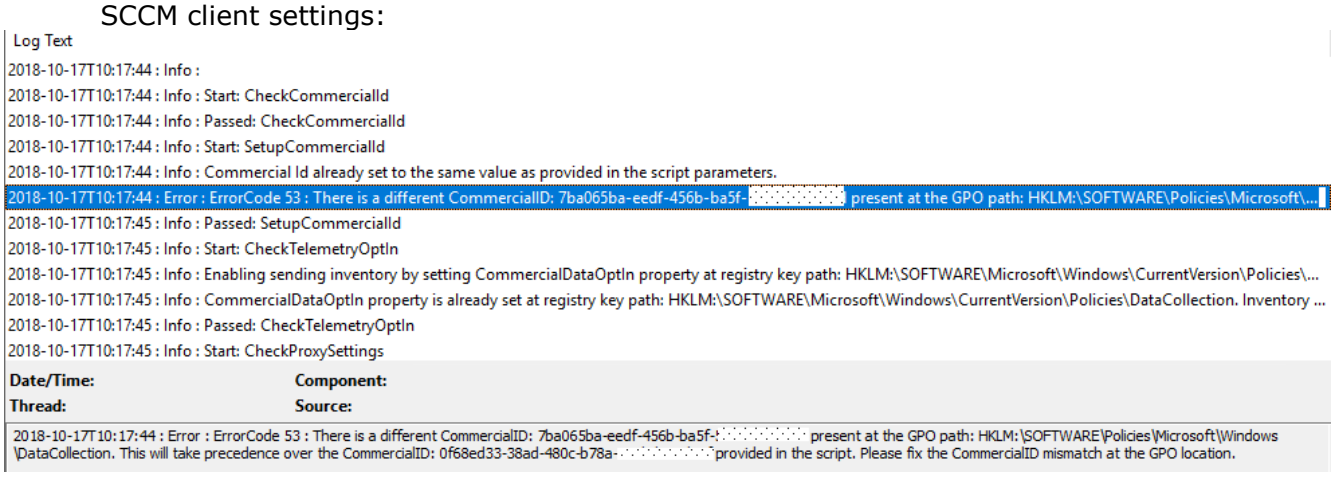
5. The latest version of the deployment script configures insider builds to continue to send the device name to the diagnostic data management service and the analytics portal. If you do not want to have insider builds send the device name sent to analytics and be available in the analytics portal, set **DeviceNAmeOptIn = false**. By default it is true, which preserves the behavior on previous versions of Windows. This setting only applies to insider builds. Note that

the device name is also sent to AppInsights, so to ensure the device name is not sent to either place you would need to also set **AppInsightsOptIn = false**.

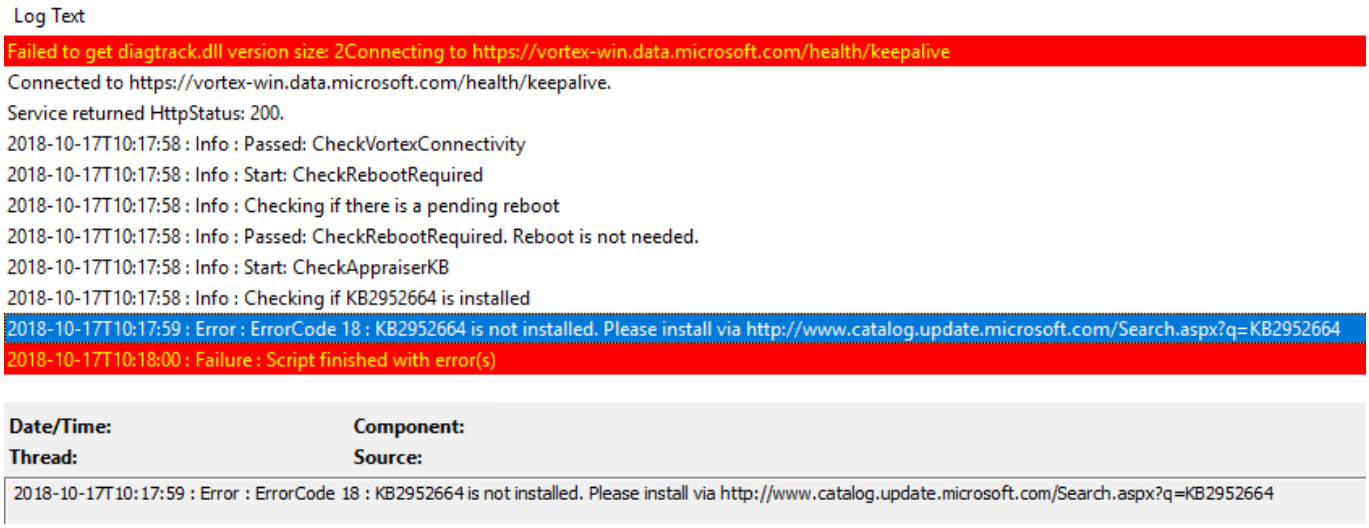
6. After you finish editing the parameters in RunConfig.bat, you are ready to run the script. If you are using the Pilot version, run RunConfig.bat from an elevated command prompt. If you are using the Deployment version, use ConfigMgr or other software deployment service to run RunConfig.bat as system.
7. Run the script on a test computer with a local administrator rights:



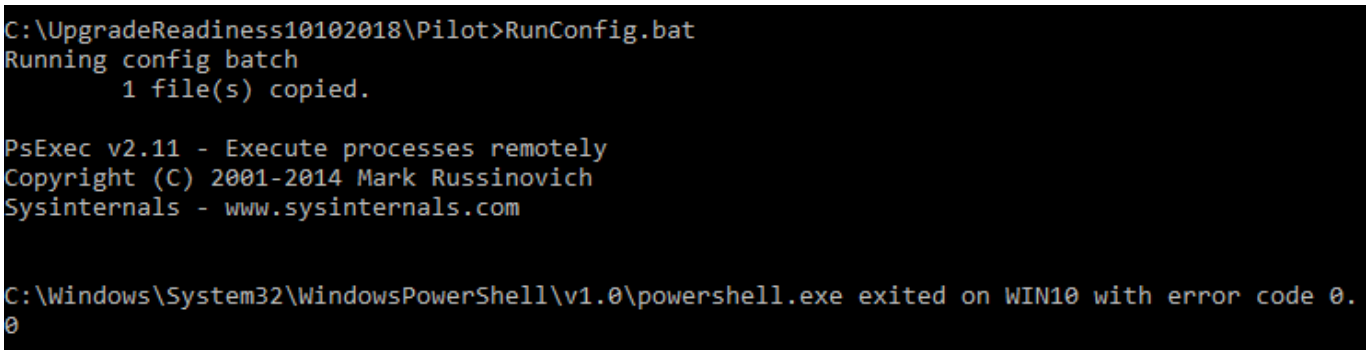
8. If an exit code is different than 0, check captured errors in generated log. For example, there is a conflict between two Commercial IDs – first is configured in GPO, second comes from SCCM client settings:



Or computer requires to install a KB before capturing the telemetry:



9. Exit code 0 means computer was configured in a proper way and telemetry data was successfully sent to Windows Analytics service:



6.5.3 Exit codes

The deployment script displays the following exit codes to let you know if it was successful, or if an error was encountered.

Exit code and meaning	Suggested fix
0 - Success	N/A
1 - Unexpected error occurred while executiEng the script.	The files in the deployment script are likely corrupted. Download the latest script from the download center and try again.
2 - Error when logging to console. $logMode = 0. (console only)	Try changing the $logMode value to **1** and try again. $logMode value 1 logs to both console and file.

3 - Error when logging to console and file. $logMode = 1.	Verify that you have set the logPath parameter in RunConfig.bat, and that the configuration script has access to connect and write to this location.
4 - Error when logging to file. $logMode = 2.	Verify that you have set the logPath parameter in RunConfig.bat, and that the configuration script has access to connect and write to this location.
5 - Error when logging to console and file. $logMode = unknown.	Verify that you have set the logPath parameter in RunConfig.bat, and that the configuration script has access to connect and write to this location.
6 - The commercialID parameter is set to unknown. Modify the runConfig.bat file to set the CommercialID value.	The value for parameter in the runconfig.bat file should match the Commercial ID key for your workspace. See Generate your Commercial ID key for instructions on generating a Commercial ID key for your workspace.
8 - Failure to create registry key path: **HKLM:\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\DataCollection**	The Commercial Id property is set at the following registry key path: **HKLM:\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\DataCollection** Verify that the context under which the script in running has access to the registry key.
9 - The script failed to write Commercial Id to registry. Error creating or updating registry key: **CommercialId** at **HKLM:\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\DataCollection**	Verify that the context under which the script in running has access to the registry key.
10 - Error when writing **CommercialDataOptIn** to the registry at **HKLM:\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\DataCollection**	Verify that the deployment script is running in a context that has access to the registry key.
11 - Function **SetupCommercialId**	The **SetupCommercialId** function updates the Commercial Id at the registry key

failed with an unexpected exception.	path: **HKLM:\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\DataCollection** Verify that the configuration script has access to this location.
12 - Can't connect to Microsoft - Vortex. Check your network/proxy settings.	**Http Get** on the end points did not return a success exit code. For Windows 10, connectivity is verified by connecting to https://v10.vortex-win.data.microsoft.com/health/keepalive. For previous operating systems, connectivity is verified by connecting to https://vortex-win.data.microsoft.com/health/keepalive. If there is an error verifying connectivity, this will prevent the collected data from being sent to Upgrade Readiness. To resolve this issue, verify that the required endpoints are correctly whitelisted. For more information, see Enrolling devices in Windows Analytics
13 - Can't connect to Microsoft - setting.	An error occurred connecting to https://settings.data.microsoft.com/qos. This error will prevent the collected data from being sent to Upgrade Readiness. To resolve this issue, verify that the required endpoints are correctly whitelisted. For more information, see Enrolling devices in Windows Analytics. Verify that the required endpoints are whitelisted correctly. See Whitelist select endpoints for more details. 14
14 - Can't connect to Microsoft - compatexchange.	An error occurred connecting to CompatibilityExchangeService.svc. This error will prevent the collected data from being sent to Upgrade Readiness. To resolve this issue, verify that the required endpoints are correctly whitelisted. For more information, see Enrolling devices in Windows Analytics.
15 - Function CheckVortexConnectivity failed with an unexpected exception.	This error will prevent the collected data from being sent to Upgrade Readiness. To resolve this issue, verify that the required endpoints are correctly whitelisted. For more information, see Enrolling devices in Windows Analytics. Check the logs for the exception message and the HResult.

16 - The computer requires a reboot before running the script.	A reboot is required to complete the installation of the compatibility update and related KBs. Reboot the computer before running the Upgrade Readiness deployment script.
17 - Function **CheckRebootRequired** failed with an unexpected exception.	A reboot is required to complete installation of the compatibility update and related KBs. Check the logs for the exception message and the HResult.
18 - Appraiser KBs not installed or **appraiser.dll** not found.	Either the Appraiser KBs are not installed, or the **appraiser.dll** file was not found. For more information, see appraiser diagnostic data events and fields information in the Data collectionand privacy topic.
19 - Function **CheckAppraiserKB**, which checks the compatibility update KBs, failed with unexpected exception.	Check the logs for the Exception message and HResult. The script will not run further if this error is not fixed.
20 - An error occurred when creating or updating the registry key **RequestAllAppraiserVersions** at **HKLM:\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\Appraiser**	The registry key is required for data collection to work correctly. Verify that the script is running in a context that has access to the registry key.
21 - Function **SetRequestAllAppraiserVersions** failed with an unexpected exception.	Check the logs for the exception message and HResult.
22 - **RunAppraiser** failed with unexpected exception.	Check the logs for the exception message and HResult. Check the **%windir%\System32** directory for the file **CompatTelRunner.exe**. If the file does not exist, reinstall the required compatibility updates which include this file, and check your organization's Group Policy to verify it does not remove this file.
23 - Error finding system variable **%WINDIR%**.	Verify that this environment variable is configured on the computer.

24 - The script failed when writing **IEDataOptIn** to the registry. An error occurred when creating registry key **IEOptInLevel** at **HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection**	This is a required registry key for IE data collection to work correctly. Verify that the deployment script in running in a context that has access to the registry key. Check the logs for the exception message and HResult.
25 - The function **SetIEDataOptIn** failed with unexpected exception.	Check the logs for the exception message and HResult.
27 - The script is not running under **System**account.	The Upgrade Readiness configuration script must be run as **System**.
28 - Could not create log file at the specified **logPath**.	Make sure the deployment script has access to the location specified in the **logPath** parameter.
29 - Connectivity check failed for proxy authentication.	Instal cumulative updates on the computer and enable the **DisableEnterpriseAuthProxy**authentication proxy setting. The **DisableEnterpriseAuthProxy** setting is enabled by default for Windows 7. For Windows 8.1 computers, set the **DisableEnterpriseAuthProxy** setting to **0** (not disabled). For more information on authentication proxy support, see Authentication proxy support added in new version (12.28.16) of the Upgrade Readiness deployment script.
30 - Connectivity check failed. Registry key property **DisableEnterpriseAuthProxy** is not enabled.	The **DisableEnterpriseAuthProxy** setting is enabled by default for Windows 7. For Windows 8.1 computers, set the **DisableEnterpriseAuthProxy** setting to **0** (not disabled). For more information on authentication proxy support, see this blog post.
31 - There is more than one instance of the Upgrade	Use the Windows Task Manager to check if **CompatTelRunner.exe** is running, and wait until it has

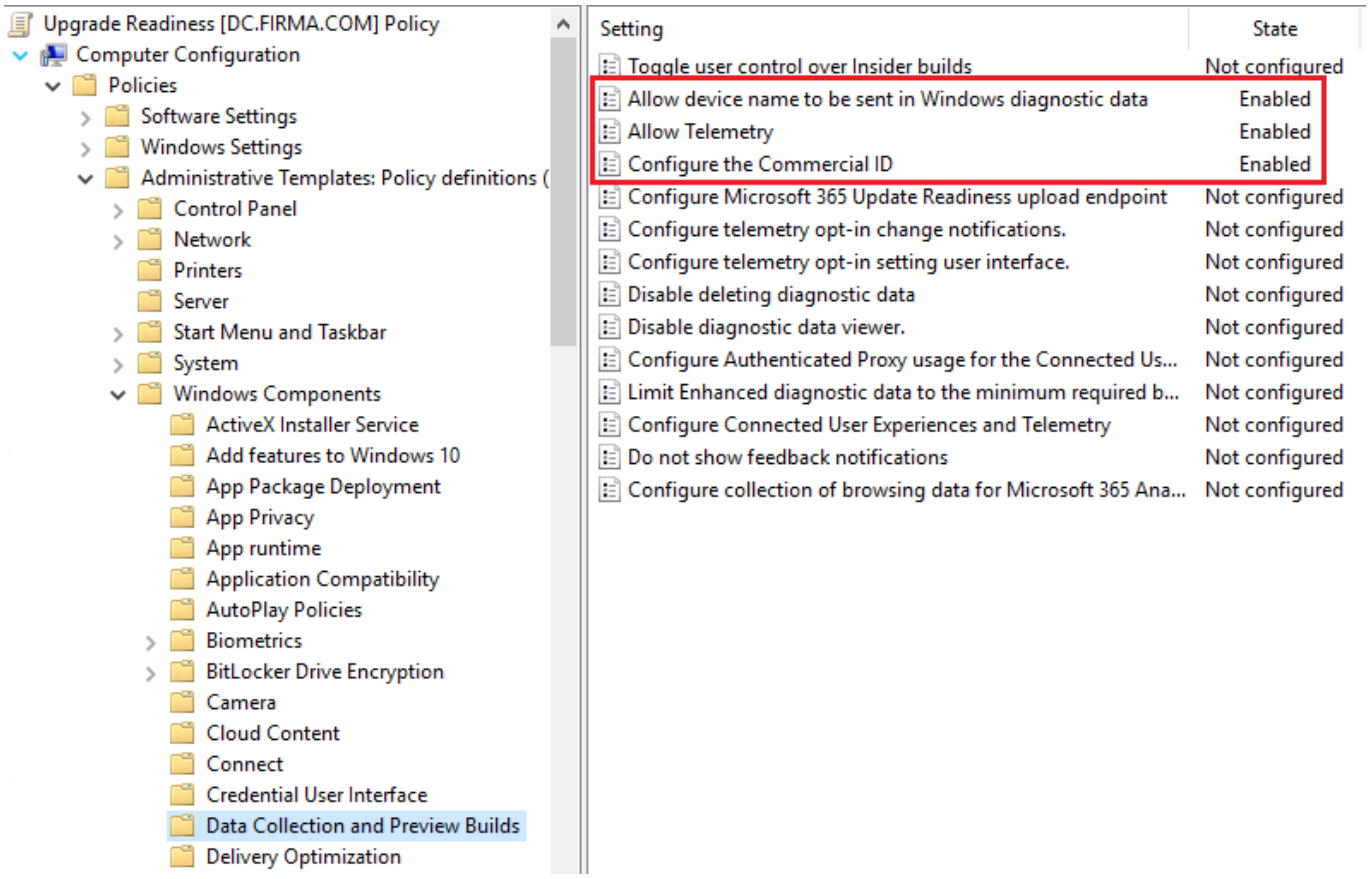
Readiness data collector running at the same time on this computer.	completed to rerun the script. The Upgrade Readiness task is scheduled to run daily at 3 a.m.
32 - Appraiser version on the machine is outdated.	The configuration script detected a version of the compatibility update module that is older than the minimum required to correctly collect the data required by Upgrade Readiness solution. Use the latest version of the compatibility update for Windows 7 SP1/Windows 8.1.
33 - **CompatTelRunner.exe** exited with an exit code	**CompatTelRunner.exe** runs the appraise task on the machine. If it fails, it will provide a specific exit code. The script will return exit code 33 when **CompatTelRunner.exe** itself exits with an exit code. Check the logs for more details. Also see the **Note** following this table for additional steps to follow.
34 - Function **CheckProxySettings** failed with an unexpected exception.	Check the logs for the exception message and HResult.>
35 - Function **CheckAuthProxy** failed with an unexpected exception.	Check the logs for the exception message and HResult.
36 - Function **CheckAppraiserEndPointsConnectivity**failed with an unexpected exception.	Check the logs for the exception message and HResult.
37 - **Diagnose_internal.cmd** failed with an unexpected exception.	Check the logs for the exception message and HResult.
38 - Function **Get-SqmID** failed with an unexpected exception.	Check the logs for the exception message and HResult.

39 - For Windows 10: AllowTelemetry property is not set to 1 or higher at registry key path **HKLM:\SOFTWARE\Policies\Microsoft \Windows\DataCollection** or **HKLM:\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\DataCollection**	For Windows 10 machines, the **AllowTelemetry** property should be set to 1 or greater to enable data collection. The script will throw an error if this is not true. For more information, see Configure Windows diagnostic data in your organization.
40 - Function **CheckTelemetryOptIn** failed with an unexpected exception.	Check the logs for the exception message and HResult.
41 - The script failed to impersonate the currently logged on user.	The script mimics the UTC client to collect upgrade readiness data. When auth proxy is set, the UTC client impersonates the logged on user. The script also tries to mimic this, but the process failed.
42 - Function **StartImpersonatingLoggedOnUser** failed with an unexpected exception.	Check the logs for the exception message and HResult.
43 - Function **EndImpersonatingLoggedOnUser** failed with an unexpected exception.	Check the logs for the exception message and HResult.
44 - Diagtrack.dll version is old, so Auth Proxy will not work.	Update the PC using Windows Update/Windows Server Update Services.
45 - Diagrack.dll was not found.	Update the PC using Windows Update/Windows Server Update Services.
46 - **DisableEnterpriseAuthProxy** property should be set to **1** for **ClientProxy=Telemetry** to work.	Set the **DisableEnterpriseAuthProxy** registry property to **1** at key path **HKLM:\SOFTWARE\Policies\Microsoft \Windows\DataCollection**.

47 - **TelemetryProxyServer** is not present in key path **HKLM:\SOFTWARE\Policies\Microsoft \Windows\DataCollection**.	**ClientProxy** selected is **Telemetry**, but you need to add **TelemetryProxyServer** in key path **HKLM:\SOFTWARE\Policies\Microsoft \Windows\DataCollection**.
48 - **CommercialID** mentioned in RunConfig.bat should be a GUID.	**CommercialID** is mentioned in RunConfig.bat, but it is not a GUID. Copy the commercialID from your workspace. To find the commercialID, in the OMS portal click **Upgrade Readiness > Settings**.
50 - Diagtrack Service is not running.	Diagtrack Service is required to send data to Microsoft. Enable and run the 'Connected User Experiences and Telemetry' service.
51 - RunCensus failed with an unexpected exception.	RunCensus explitly runs the process used to collect device information. The method failed with an unexpected exception. Check the ExceptionHResult and ExceptionMessage for more details.
52 - DeviceCensus.exe not found on a Windows 10 machine.	On computers running Windows 10, the process devicecensus.exe should be present in the \system32 folder. Error code 52 is returned if the process was not found. Ensure that it exists at the specified location.
53 - There is a different CommercialID present at the GPO path:**HKLM:\SOFTWARE\Policies\Microsoft \Windows\DataCollection**. This will take precedence over the CommercialID provided in the script.	Provide the correct CommercialID at the GPO location.

6.5.4 Deploying the Commercial ID with GPO

If you don't use SCCM you can deploy the Commercial ID with group policies. First, you need to import the latest administrative templates for Windows 10. Then you need to enable settings in **Windows Components – Data Collection and Preview Builds** and deploy this GPO on Organization Unit with computers required to send the telemetry:



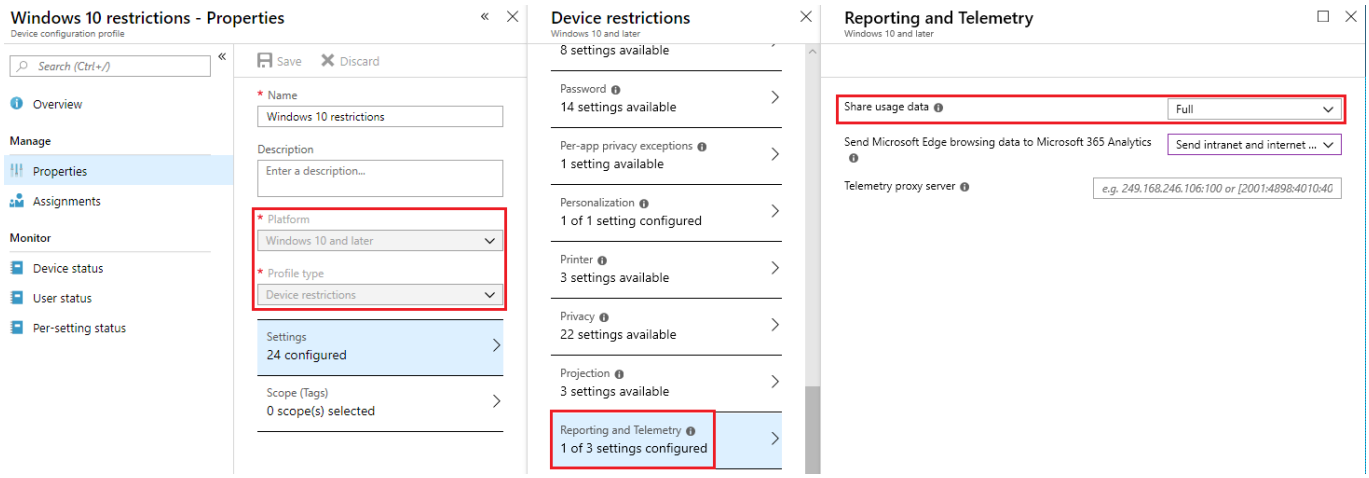
Allow device name to be send – This policy allows the device name to be sent to Microsoft as part of Windows diagnostic data.

Allow Telemetry – This policy setting determines the highest level of Windows diagnostic data sent to Microsoft (Security, Basic, Enhanced, Full).

Configure the Commercial ID – This policy setting defines the identifier used to uniquely associate this device's telemetry data as belonging to a given organization.

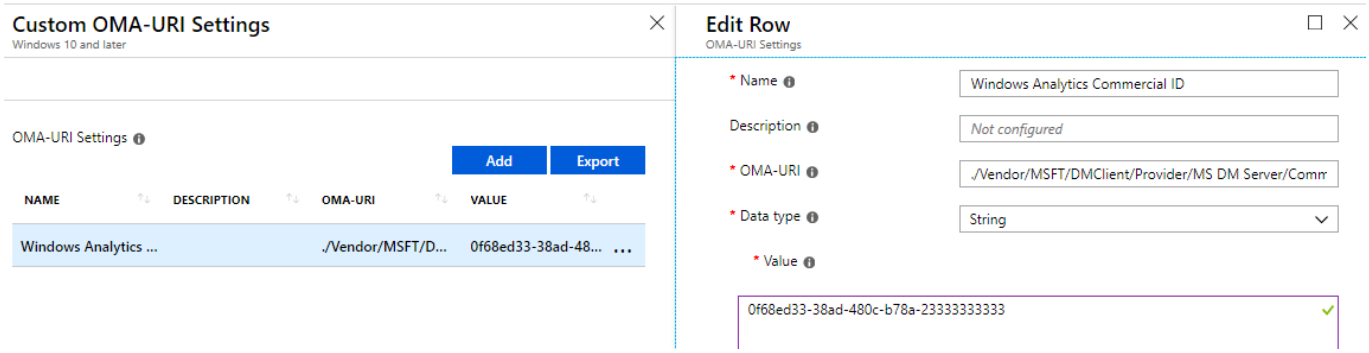
6.5.5 Deploying the Commercial ID with Intune

If you don't use SCCM or GPO you can deploy the Commercial ID with Intune Windows 10 configuration policies. First, you need to create and assign a **Device configuration profile** that enables sending the telemetry:

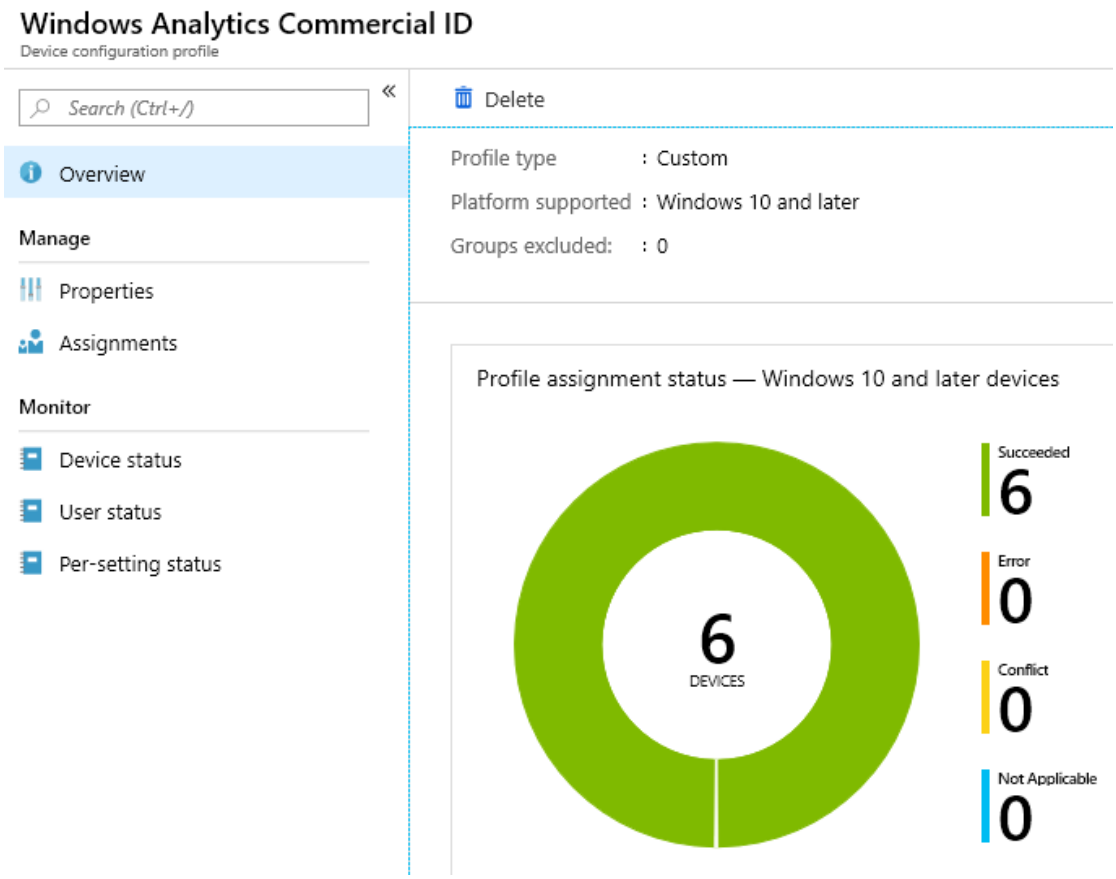


Then you need to create and assign a **Custom profile** for Windows 10 to deploy the Commercial ID with next parameters:

OMA-URI: ./Vendor/MSFT/DMClient/Provider/MS DM Server/CommercialID
Data type: String
Value: Your Commercial ID



Then check if computers successfully downloaded and applied a new settings:



6.6 Deploying Windows Analytics at scale

When you have completed a pilot deployment, you are ready to automate data collection and distribute the deployment script to the remaining devices in your organization.

6.6.1 Automate data collection

To ensure that user computers are receiving the most up-to-date data from Microsoft, we recommend that you establish the following data sharing and analysis processes:

- Enable automatic updates for the compatibility update and related updates. These updates include the latest application and driver issue information as we discover it during testing.
- Schedule the Upgrade Readiness deployment script to automatically run monthly. Scheduling the script ensures that full inventory is sent monthly even if devices were not connected or had low battery power at the time the system normally sends inventory. Make sure to run the production version of the script, which is lighter weight and non-interactive. The script also has a number of built-in error checks, so you can monitor the results. If you can't run the deployment script at scale, another option is to configure things centrally via Group Policy or Mobile Device Management (MDM). Although we recommend using the deployment script, both options are discussed in the sections below.

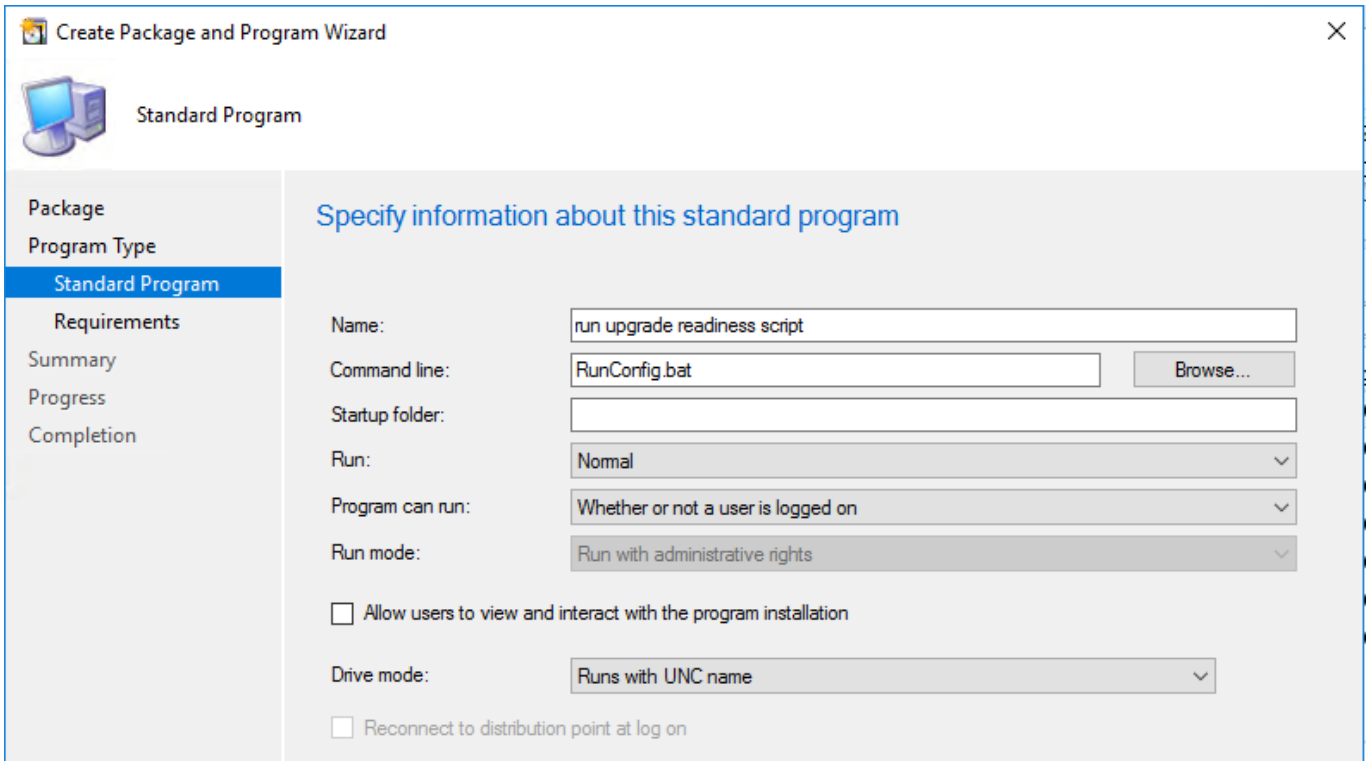
When you run the deployment script, it initiates a full scan. The daily scheduled task to capture the changes is created when the update package is installed. For Windows 10 devices, this task is already included in the operating system. A full scan averages about 2 MB, but the scans for changes are very small. The scheduled task is named "Windows Compatibility Appraiser" and can be found in the Task Scheduler Library under Microsoft > Windows > Application Experience. Changes

are invoked via the nightly scheduled task. It attempts to run around 3:00AM every day. If the system is powered off at that time, the task will run when the system is turned on.

6.6.2 Distribute the deployment script at scale

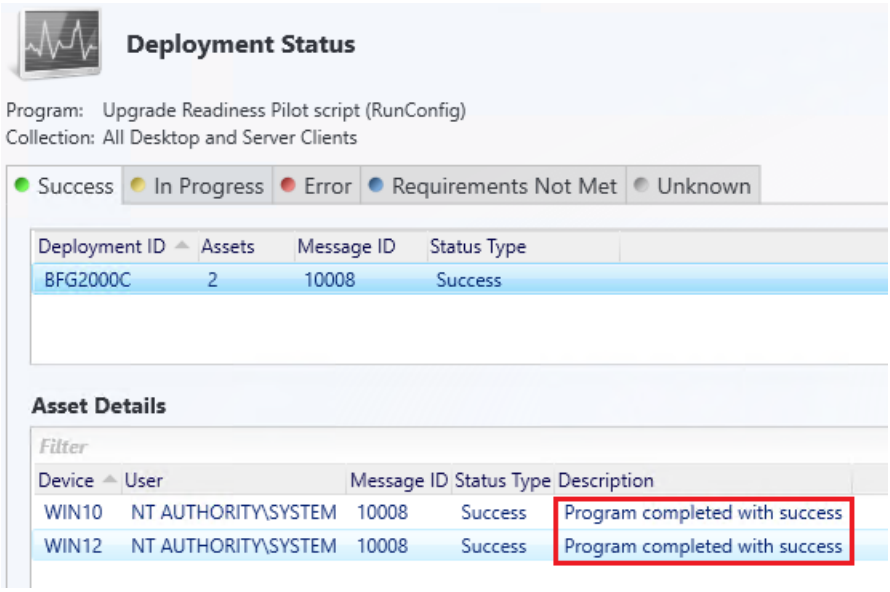
Use a software distribution system such as System Center Configuration Manager to distribute the Upgrade Readiness deployment script at scale.

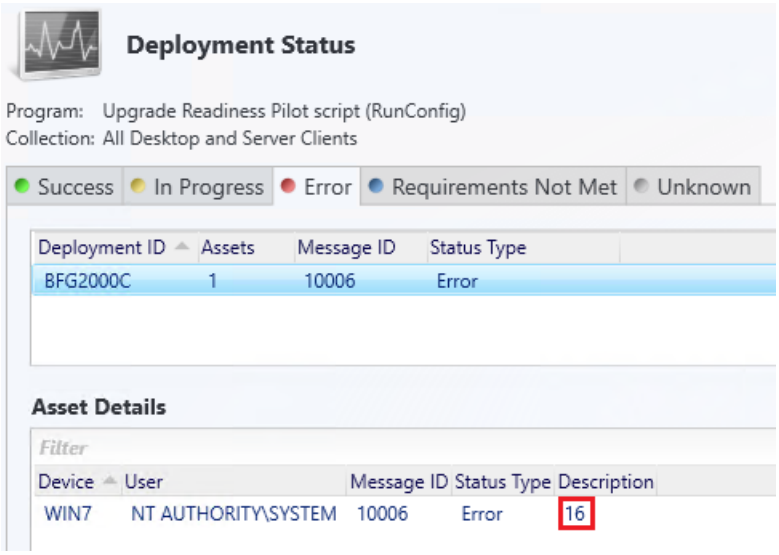
After editing RunConfig.bat you can create a package and deploy it on collections with computers you want to enable and collect the telemetry:



6.6.3 Checking the deployment status

You can check the deployment status in a Monitoring workplace and compare the results with error codes table that provided above:

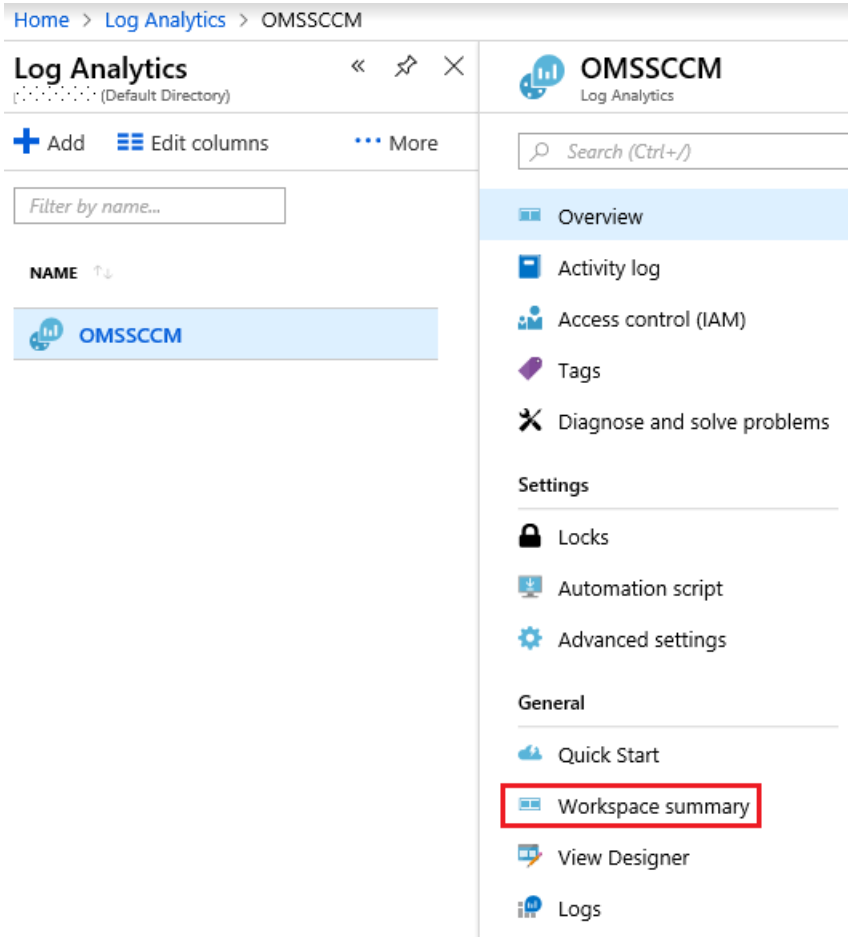




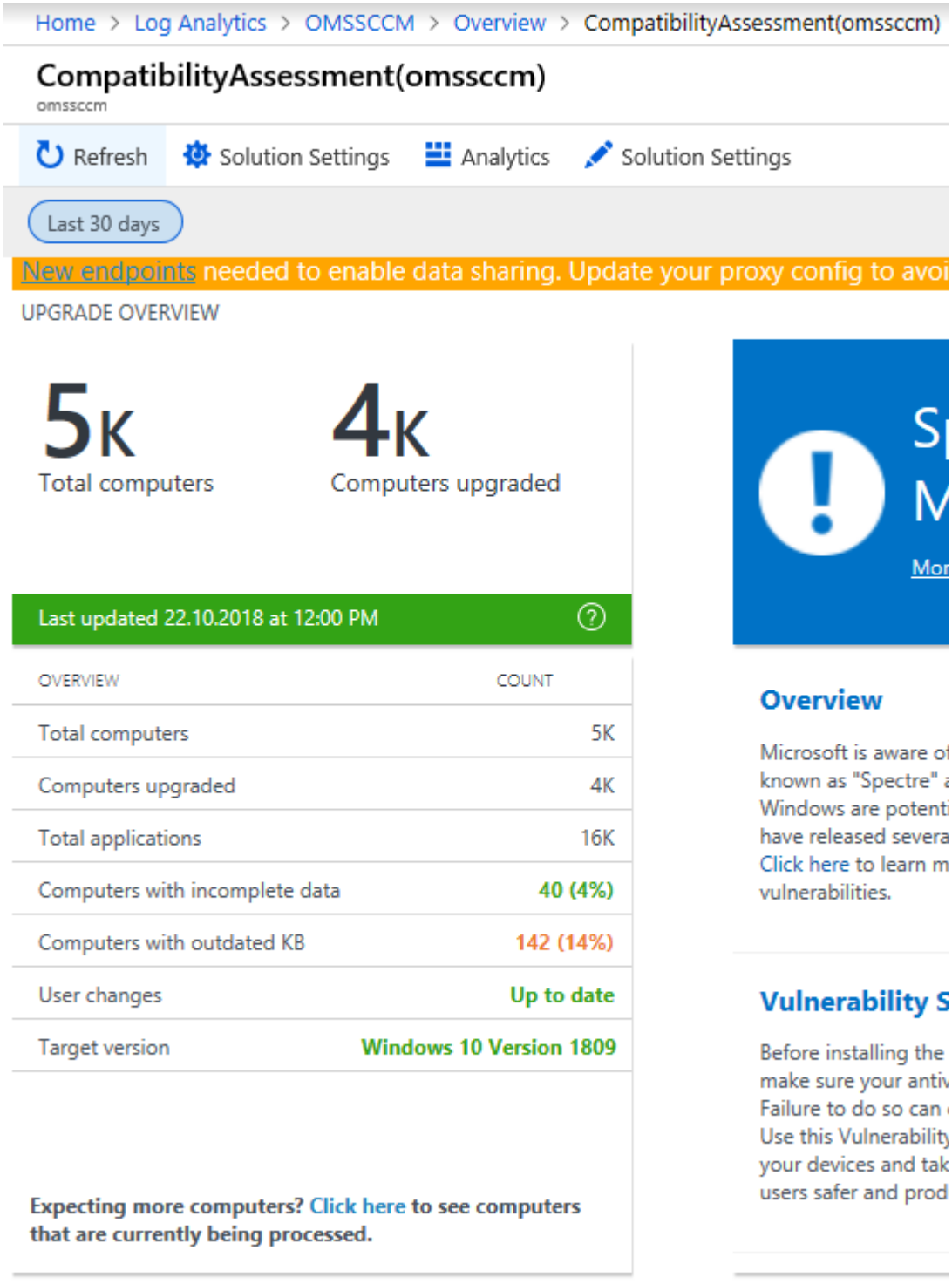
7. Checking collecting telemetry information

7.1 Checking collecting telemetry in Azure console

Open Log Analytics in your Azure Subscription, choose created OMS workspace and click Workspace summary:

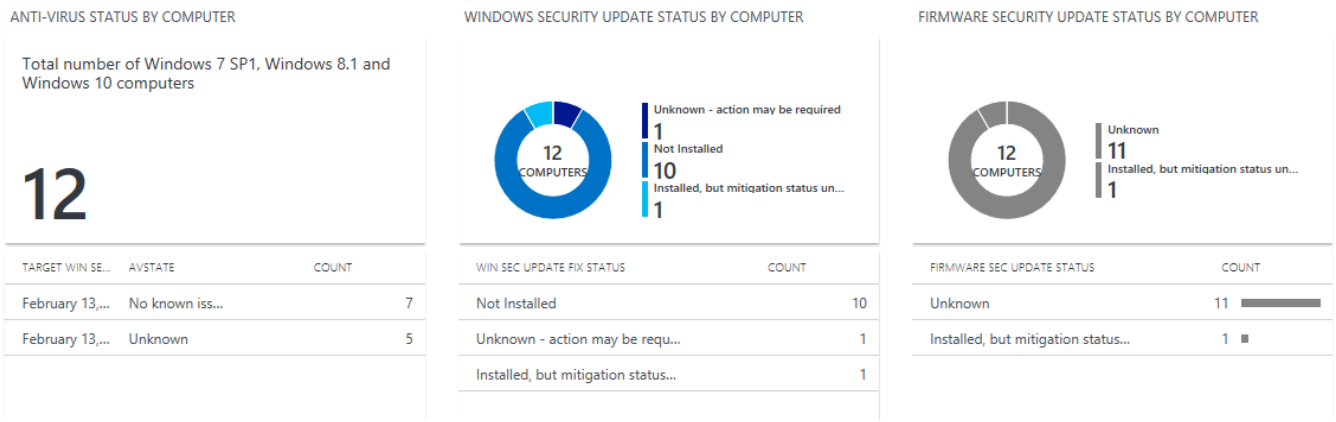


On the **Overview** pane click on a summary dashboard **Upgrade Readiness**:



In Spectre and Meltdown section you can check:

- Anti-virus status by computer
- Windows security update status by computer
- Firmware security update status by computer



7.1.1 Identify important apps

Go to **STEP 1: Identify important apps** section and click on numbers. Then you can apply different filters to get more reliable information:

IMPORTANCE (2)

Low install count	15K
Not reviewed	867

ISSUE (6)

No known issues	16K
Application is removed during upgrade	19
Does not work with new OS, but won't block upgrade	4
Evaluate application on new OS	2
Reinstall application after upgrading	1
Does not work with new OS, and will block upgrade	1

[-] Less

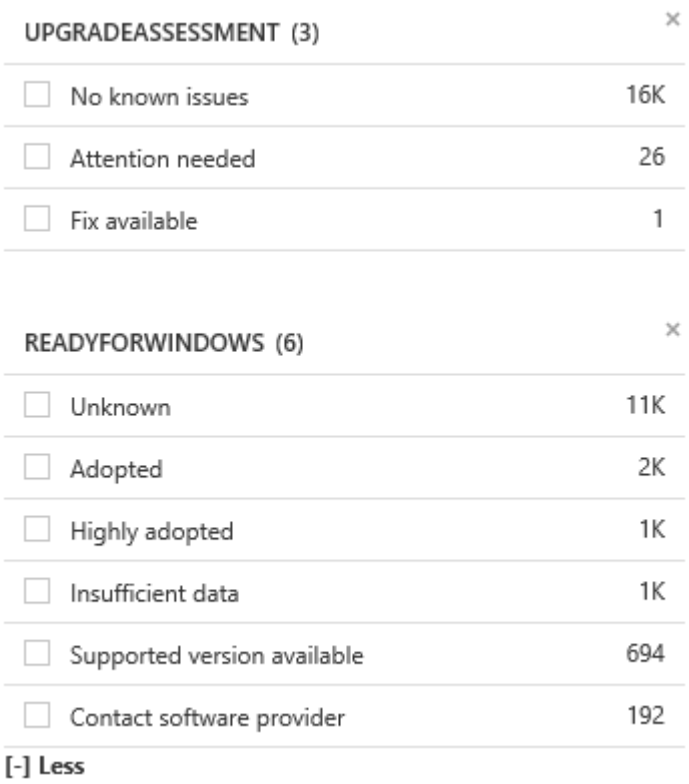
UPGRADEDECISION (2)

Ready to upgrade	15K
Not reviewed	867

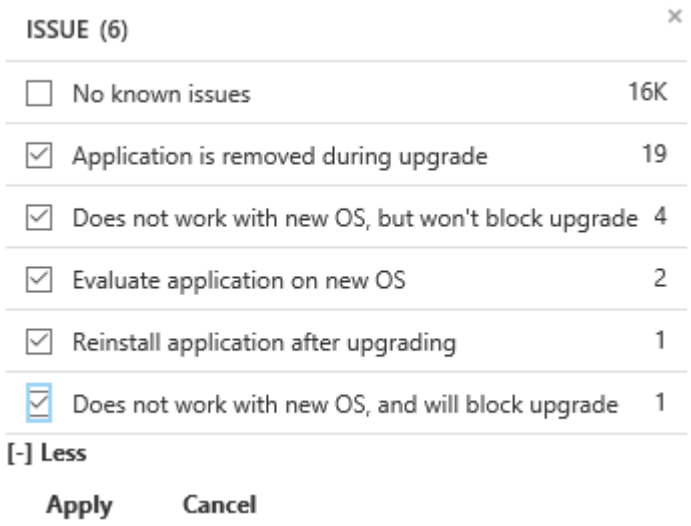
PERCENTACTIVECOMPUTERS (7)

0 %	14K
0 - 2 %	2K
2 - 5 %	20
10 - 20 %	11
5 - 10 %	5
20 - 30 %	1
30 - 50 %	1

[-] Less



For example, you want to check all reviewed apps with issues. To do this enable filters and click **Apply**:



Then click on numbers under APPCOUNT:

And change results view from **List** to **Table**:

27 Results List Table User changes

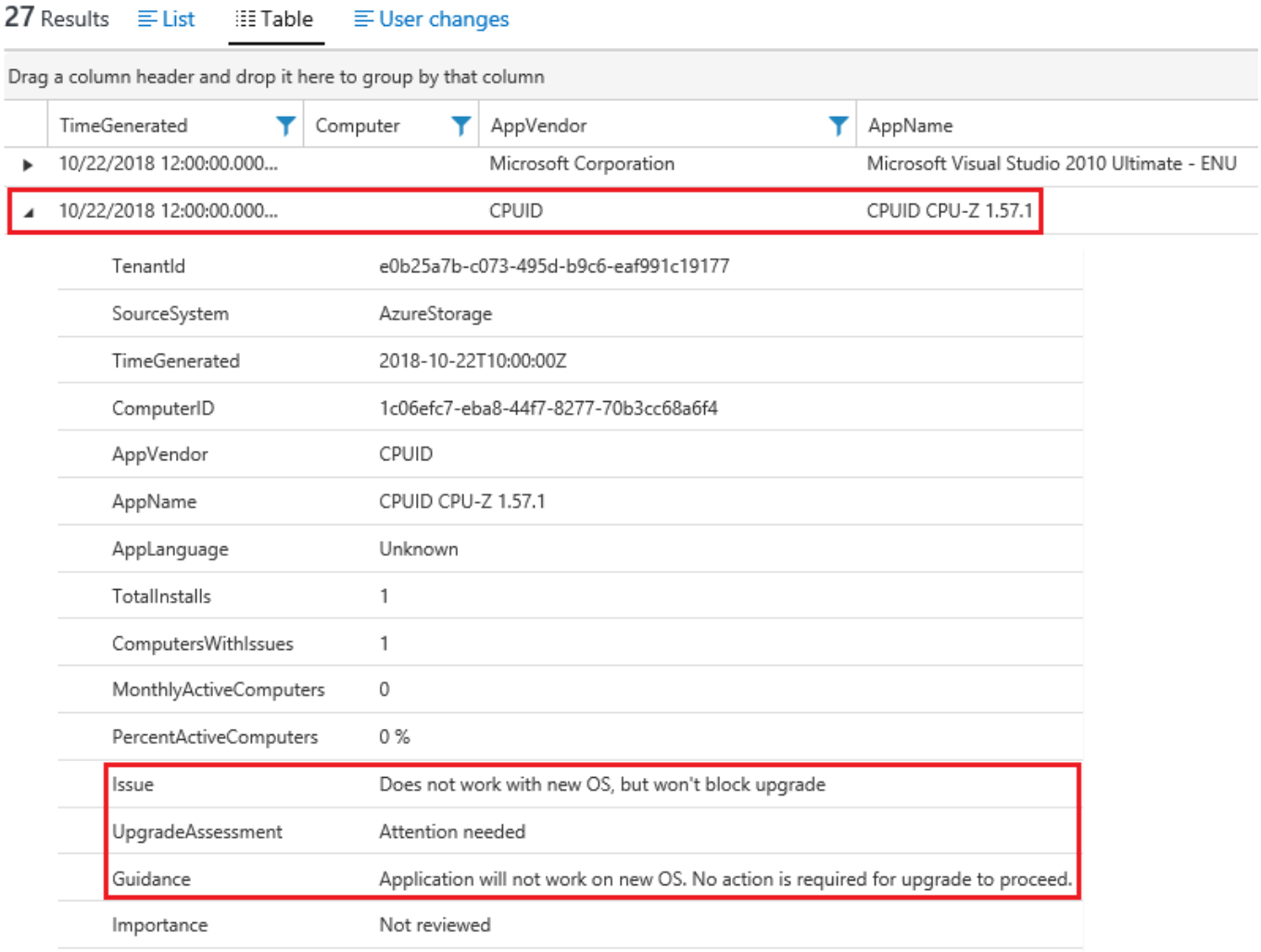
Drag a column header and drop it here to group by that column

TimeGenerated	Computer	AppVendor	AppName	AppVersion	AppLanguage	TotalInstalls
10/22/2018 12:00:00.000...		Broadcom Corporation	Broadcom 2070 Bluetooth 3.0	6.3.0.6300	Unknown	1
10/22/2018 12:00:00.000...		MagicISO, Inc.	MagicDisc 2.7.106		Unknown	1
10/22/2018 12:00:00.000...		Intel Corporation	Intel(R) USB 3.0 eXtensible Host Controller Driver	3.0.0.20	Unknown	1
10/22/2018 12:00:00.000...		Microsoft Corporation	Microsoft Visual Studio 2010 Ultimate - ENU	10.0.40219	English (United States)	1
10/22/2018 12:00:00.000...		CPUID	CPUID CPU-Z 1.57.1		Unknown	1
10/22/2018 12:00:00.000...		Check Point Software Technologies Ltd.	Check Point VPN	98.60.1031	English (United States)	1
10/22/2018 12:00:00.000...		Cisco Systems, Inc.	Cisco Systems VPN Client 5.0.07.0290	5.0.7	English (United States)	4
10/22/2018 12:00:00.000...		Microsoft Corporation	Windows Phone Emulator x64 - ENU	10.0.30319	English (United States)	1
10/22/2018 12:00:00.000...		DisplayLink Corp.	DisplayLink Core Software	7.4.51572.0	English (United States)	78

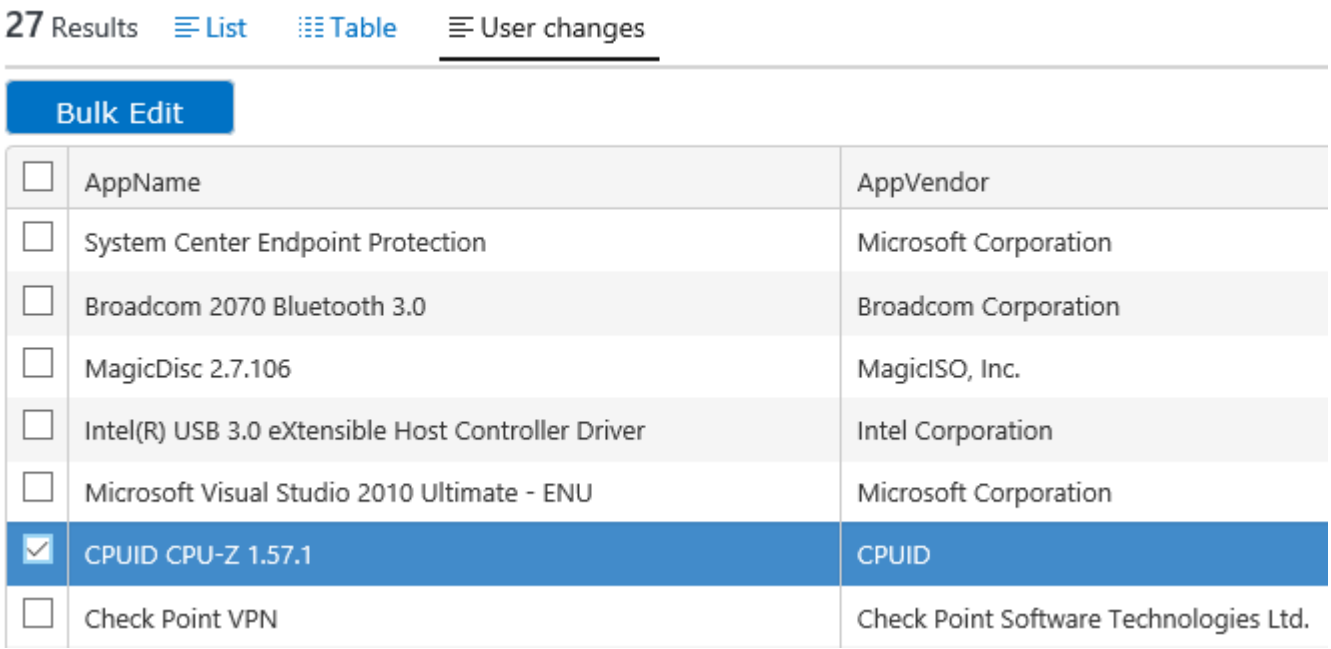
You can scroll right and check a summary for all apps with problems like **Issues** and **Guidance**:

Issue	UpgradeAssessment	Guidance
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No action is...
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No action is...
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No action is...
Does not work with new OS, but won't block upgrade	Attention needed	Application will not work on new OS. No action is required for upgrade to proc...
Does not work with new OS, but won't block upgrade	Attention needed	Application will not work on new OS. No action is required for upgrade to proc...
Evaluate application on new OS	Attention needed	Application may have issues on new OS. No action is required for upgrade to pr...
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No action is...
Does not work with new OS, but won't block upgrade	Attention needed	Application will not work on new OS. No action is required for upgrade to proc...
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No action is...
Does not work with new OS, but won't block upgrade	Attention needed	Application will not work on new OS. No action is required for upgrade to proc...
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No action is...
Reinstall application after upgrading	Fix available	No action is required for upgrade to proceed. Application will work on new OS,...
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No action is...

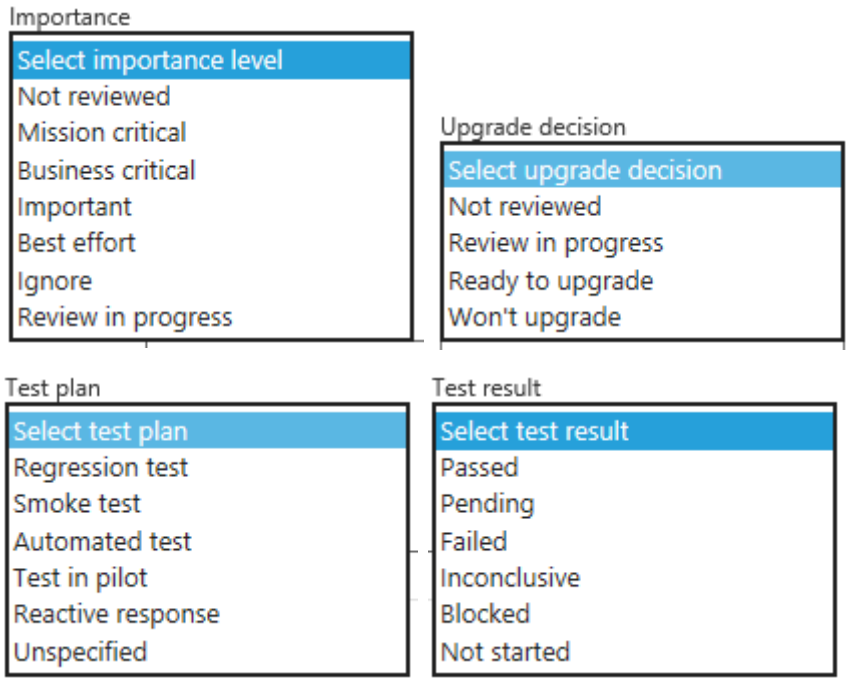
Or you can expand a line of the report and check an information about specific app:



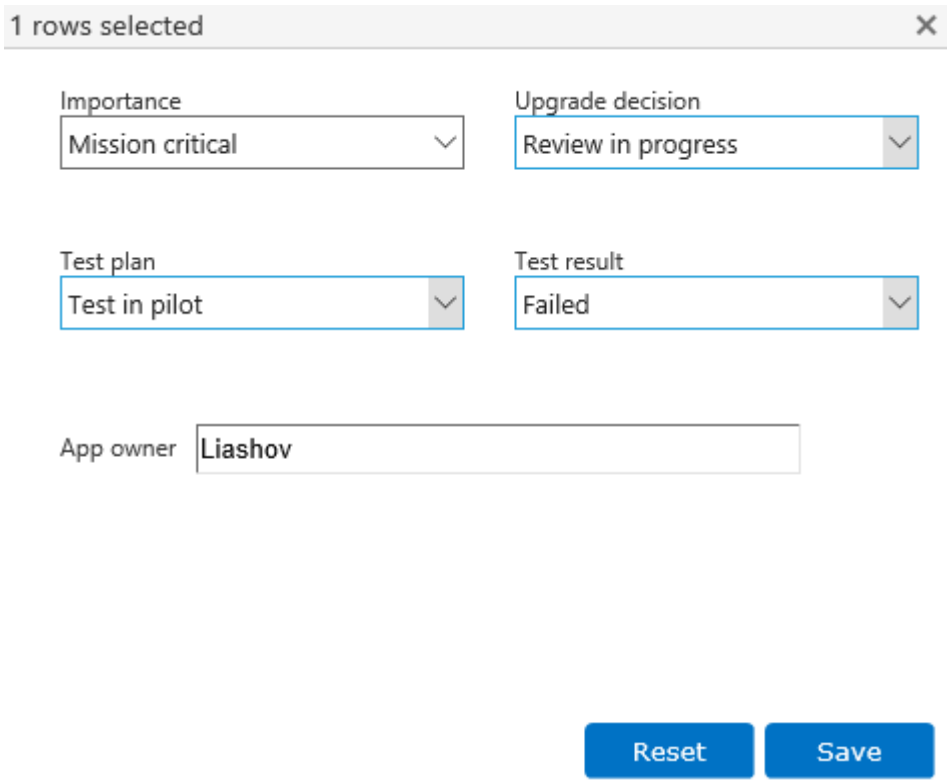
You can click on **User Changes**, select app and click **Bulk Edit**:



Then you can customize some important info about analyzed app:

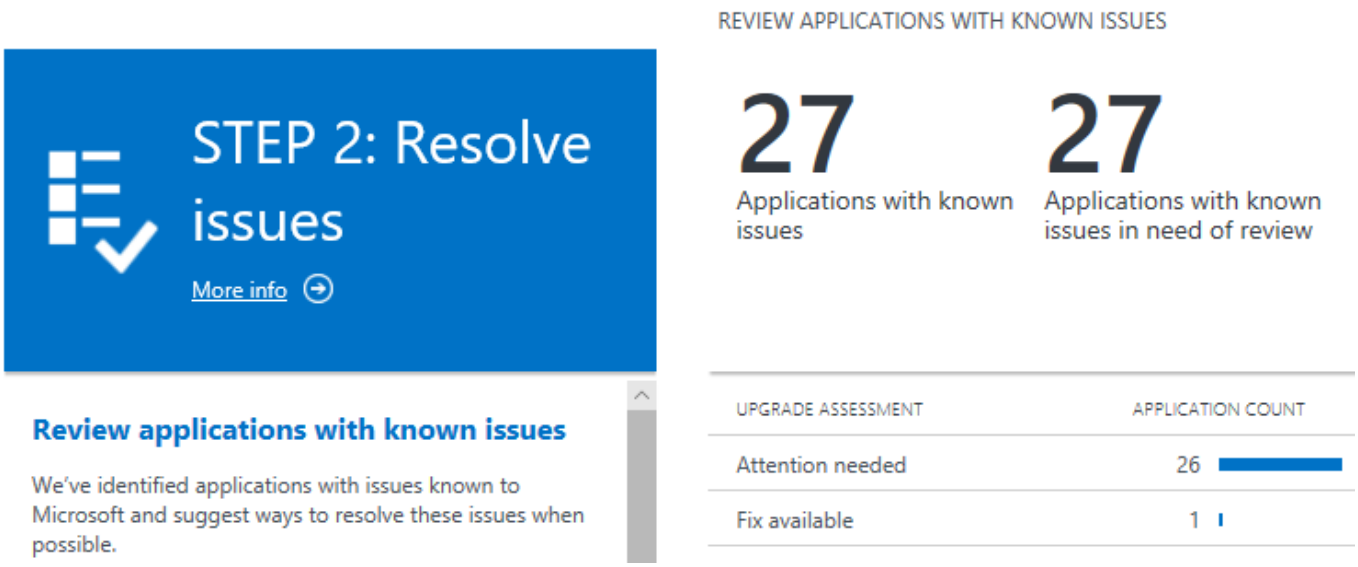


Then click **Save**:

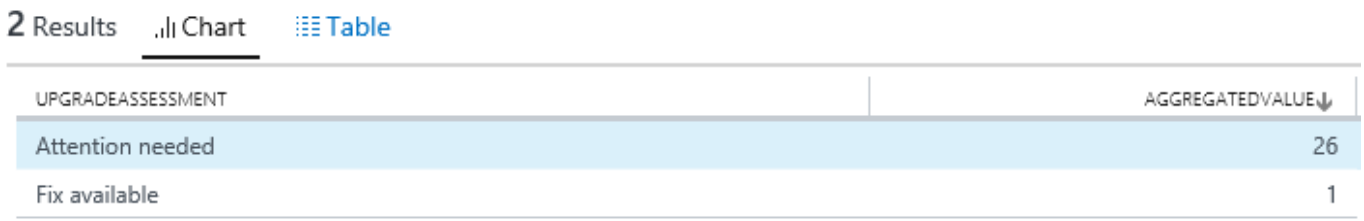


7.1.2 Resolve issues

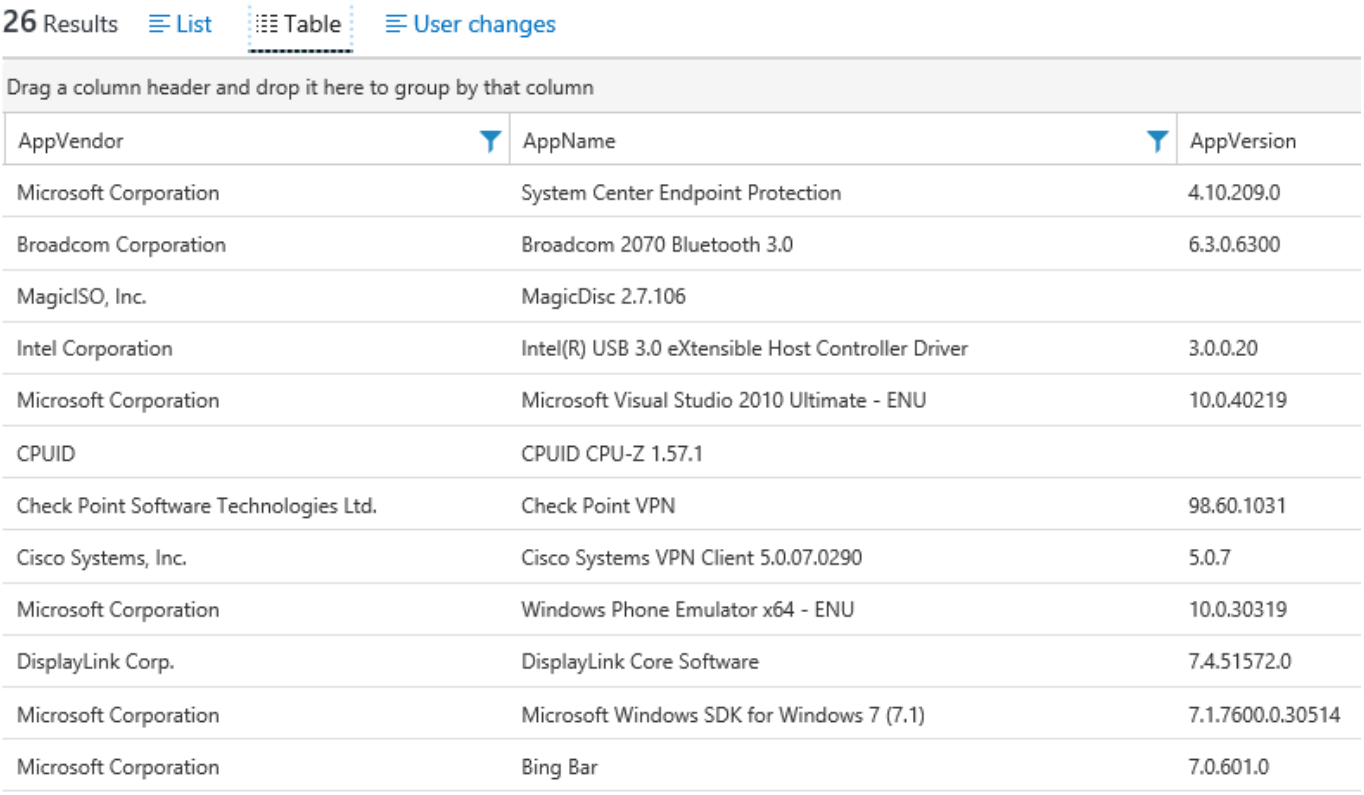
Come back to Compatibility Assessment dashboard and go to **STEP 2: Resolve issues**:



Click on numbers, then click on **Attention needed**:



Switch to **Table** mode and check summary details. They will be the same as in previous **STEP 1** if you didn't make some changes:

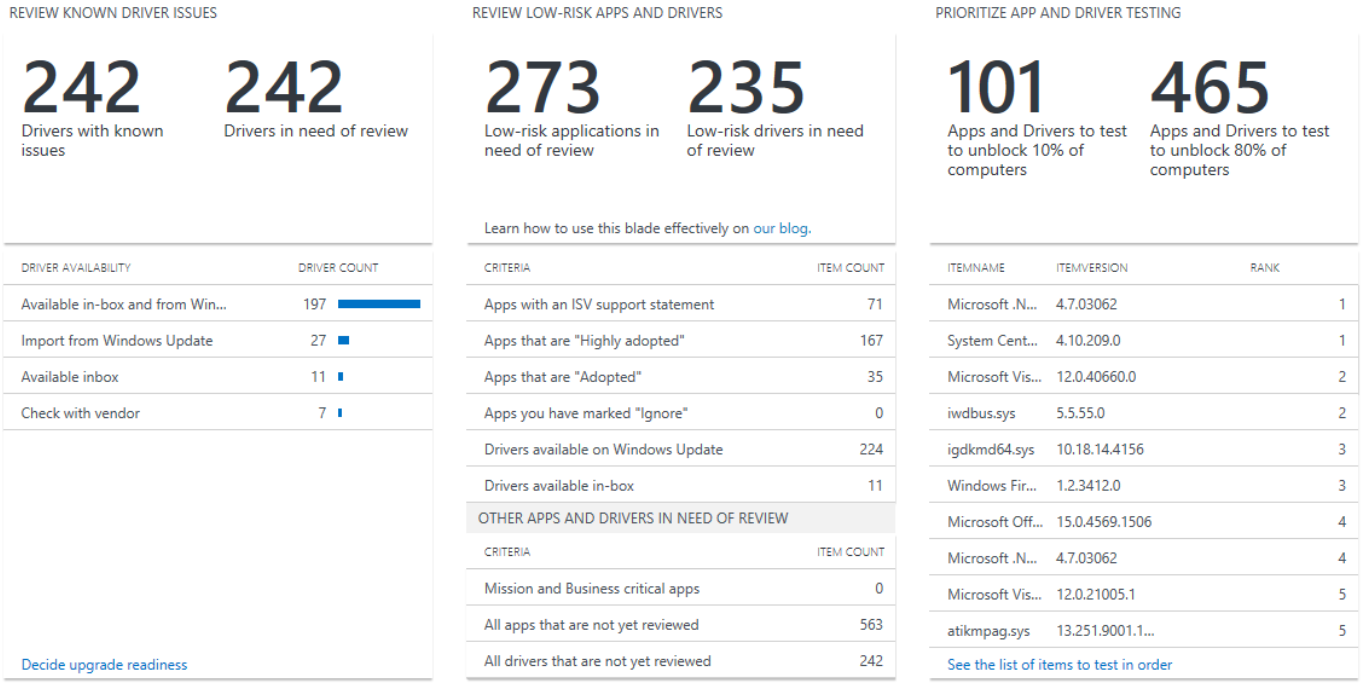


26 Results List Table User changes

Drag a column header and drop it here to group by that column

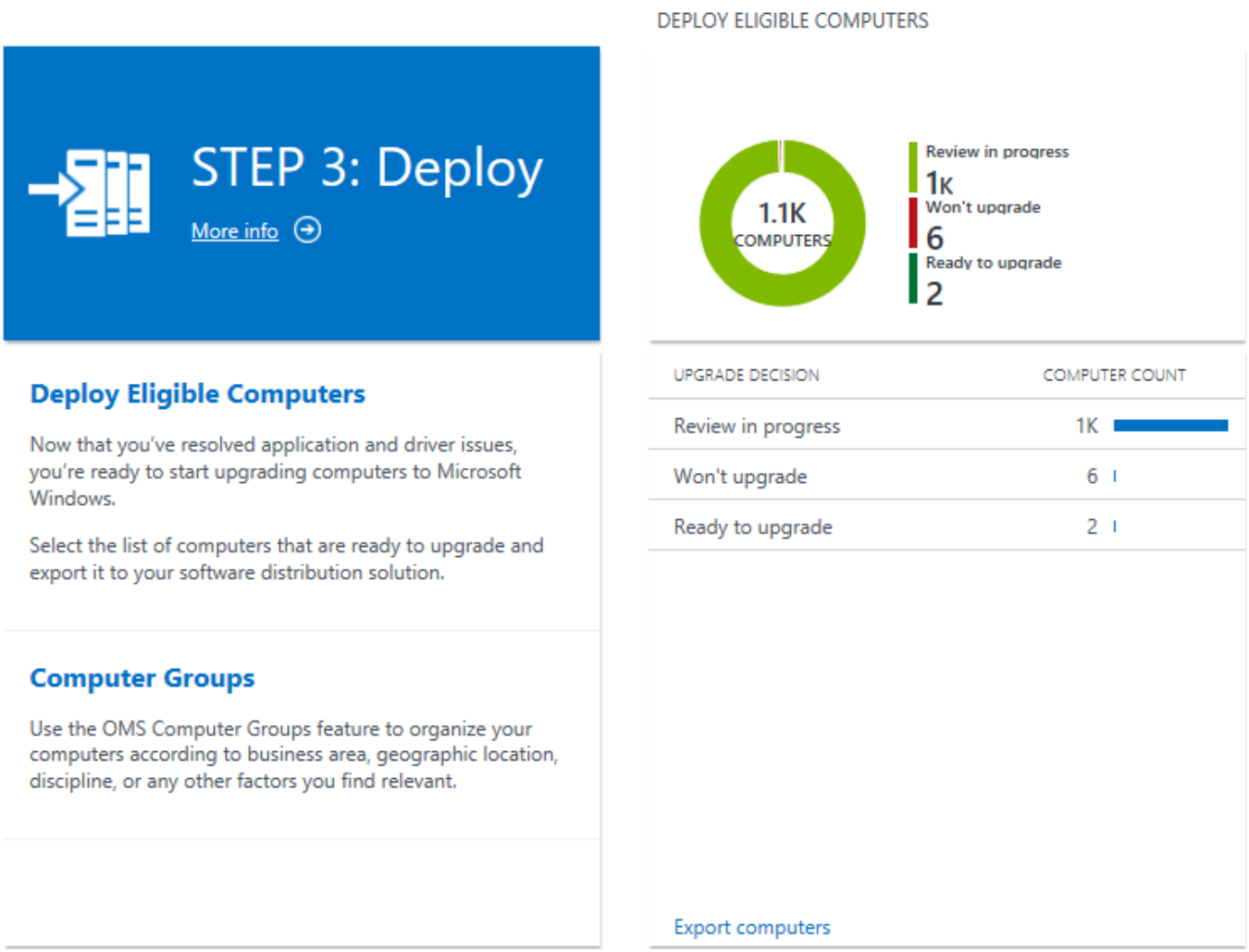
Issue	UpgradeAssessment	Guidance	Importance	UpgradeDecision
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No...	Not reviewed	Not reviewed
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No...	Not reviewed	Not reviewed
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No...	Not reviewed	Not reviewed
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No...	Not reviewed	Not reviewed
Does not work with new OS, but won't block upgrade	Attention needed	Application will not work on new OS. No action is required for upgrade...	Not reviewed	Not reviewed
Does not work with new OS, but won't block upgrade	Attention needed	Application will not work on new OS. No action is required for upgrade...	Not reviewed	Not reviewed
Evaluate application on new OS	Attention needed	Application may have issues on new OS. No action is required for upgr...	Not reviewed	Not reviewed
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No...	Not reviewed	Not reviewed
Does not work with new OS, but won't block upgrade	Attention needed	Application will not work on new OS. No action is required for upgrade...	Not reviewed	Not reviewed
Application is removed during upgrade	Attention needed	Application is removed during upgrade due to compatibility issues. No...	Not reviewed	Not reviewed
Does not work with new OS, but won't block upgrade	Attention needed	Application will not work on new OS. No action is required for upgrade...	Not reviewed	Not reviewed

On the same dashboard you can review driver issues:



7.1.3 Deploy Eligible Computers

Come back to Compatibility Assessment dashboard and go to **STEP 3: Deploy**:



Click on **Ready to upgrade**, then switch to **Table** view mode:

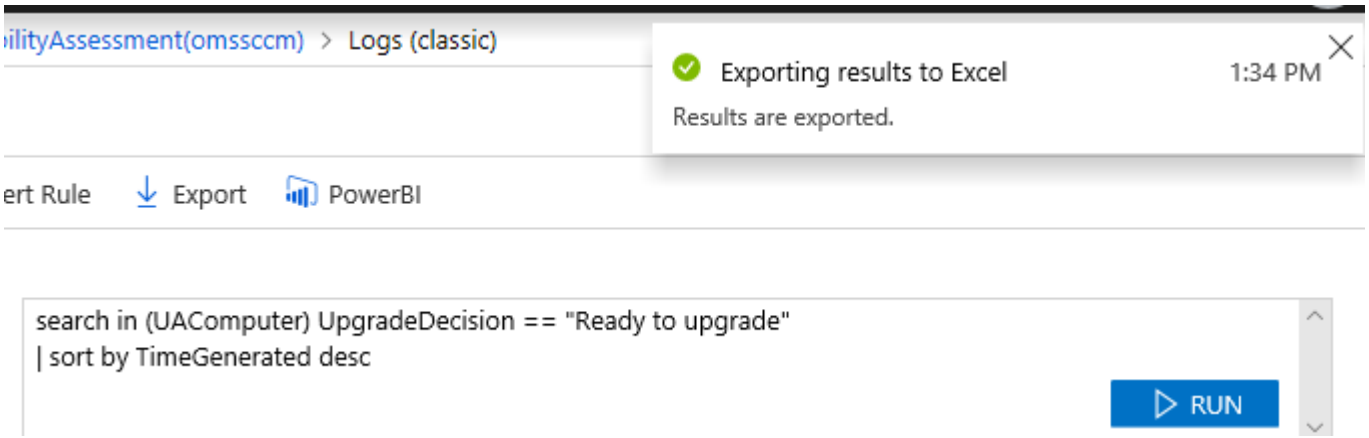
```
search in (UAComputer) UpgradeDecision == "Ready to upgrade"
| sort by TimeGenerated desc
```

2 Results List Table

Drag a column header and drop it here to group by that column

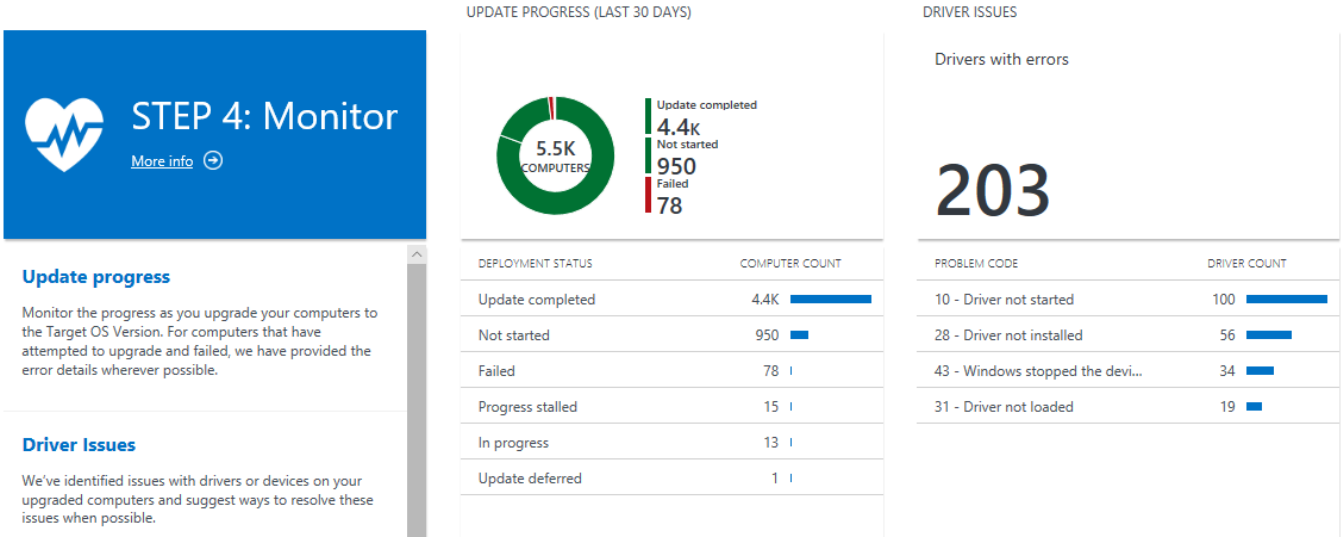
$table	TimeGenerated	Computer	Manufacturer	Model	OSVersion	OSEdition	OSArchitecture
UAComputer	10/22/2018 12:00:00.000...	MaryCh-Terminal.Contoso	Lenovo	4518PG1	Windows 8.1	Enterprise	amd64
UAComputer	10/22/2018 12:00:00.000...	DonnaGe-Book.Contoso	HP	HP Z400 Workstation	Windows 8.1	Enterprise	amd64

Then you can click on **Export** and exported list of computers are ready for upgrade to your OSD solution:



7.1.4 Update progress

Come back to Compatibility Assessment dashboard and go to **STEP 4: Monitor**:



You can check the update process with different statuses, for example, **Failed**:

Computer	Manufacturer	Model	OSVersion	OSEdition	OSArchitecture
DanaAr-Showroom.Contoso	HP	HP EliteBook 840 G4	Windows 10	Enterprise	amd64
LorinaHo-Office.Contoso	Microsoft	Surface Pro 4	Windows 10	Enterprise	amd64
StBook-Dsk.Contoso	HP	HP EliteBook 840 G4	Windows 10	Enterprise	amd64
BrianPa-Work.Contoso	Microsoft	Surface Pro 4	Windows 10	Enterprise	amd64
KimberlyBr-Demo.Contoso	Lenovo	X1 Yoga (1st Gen)	Windows 10	Enterprise	amd64
WaMichael-Terminal.Contoso	Microsoft	Surface Pro 3	Windows 10	Enterprise	amd64
ClKenneth-Office.Contoso	Microsoft	Surface Book	Windows 10	Enterprise	amd64

In a **Table** mode you can see a summarized information about upgrade process:

Computer	Manufacturer	Model	OSVersion	OSEdition	OSArchitecture
DanaAr-Showroom.Contoso	HP	HP EliteBook 840 G4	Windows 10	Enterprise	amd64
LorinaHo-Office.Contoso	Microsoft	Surface Pro 4	Windows 10	Enterprise	amd64
StBook-Dsk.Contoso	HP	HP EliteBook 840 G4	Windows 10	Enterprise	amd64
BrianPa-Work.Contoso	Microsoft	Surface Pro 4	Windows 10	Enterprise	amd64
KimberlyBr-Demo.Contoso	Lenovo	X1 Yoga (1st Gen)	Windows 10	Enterprise	amd64
WaMichael-Terminal.Contoso	Microsoft	Surface Pro 3	Windows 10	Enterprise	amd64
ClKenneth-Office.Contoso	Microsoft	Surface Book	Windows 10	Enterprise	amd64

In a **List** mode you can check computers one by one to get detailed information about the update status:

... TimeGenerated : 10/22/2018 12:00:00.000 PM
... Computer : DanaAr-Showroom.Contoso
... Manufacturer : HP
... Model : HP EliteBook 840 G4
... OSVersion : Windows 10
... OSEdition : Enterprise
... OSArchitecture : amd64
... ConfigMgrClientID : 80adc461-4cb0-450a-bca1-d9d54a0fb4b9
... DeploymentStatus : Failed
... OriginBuild : 16299
... OriginOSVersion : 1709
... TargetBuild : 17134
... TargetOSVersion : 1803
... HoursToUninstall : -1
... TotalIssues : 2
... SysReqIssues : 0
... AppIssues : 0
... DriverIssues : 2 [Query]
... UpgradeAssessment : OK to pilot with new driver from Windows Update
... UpgradeDecision : Review in progress
... ItemRank : 0
... SourceSystem : AzureStorage
... ComputerID : 0731810f-745a-4ab9-8232-2bcd0299c68e

```
... TimeGenerated      : 10/22/2018 12:00:00.000 PM
... Computer           : DanaAr-Showroom.Contoso
... HardwareName       : HP Wireless Button Driver
... HardwareType       : hidclass
... HardwareID         : acpi\ven_hpq&dev_6001
... DriverVendor       : HP
... DriverName         : wirelessbuttondriver64.sys
... DriverVersion      : 2.1.3.1
... TotalComputers     : 1
... DriverAvailability : Import from Windows Update
... Issue              : Driver will not migrate to new OS
... UpgradeAssessment  : OK to pilot with new driver from Windows Update
... Guidance           : If the computer automatically receives updates from Windows Update, no action is required. Otherwise, import a new driver from Windows Update after upgrading.
... UpgradeDecision    : Not reviewed
```

7.2 Checking collecting telemetry in SCCM console

After the configuration is completed you can view the numbers in **Monitoring / Upgrade Readiness**.