How to change your service configuration for Managed Monitoring as a Service

Overview

With Managed Monitoring as a Service, our Cloud Operations team monitors your devices, receiving and reacting to any abnormal events, only escalating those events that genuinely require your attention.

When we first provision the service, unless you specify otherwise in your initial request, we set the service up with *default thresholds* for the devices you've selected to monitor. At any time, you can raise a Service Request, via the My Calls section of the UKCloud Portal, to change these thresholds and other service configuration details.

This article shows you how to change your Managed Monitoring as a Service configuration.

Changing your service configuration

To make any changes to Managed Monitoring as a Service, log a Service Request via the My Calls section of the UKCloud Portal. For general information about raising a Service Request, see *How to use My Calls in the UKCloud Portal*.

To make changes, you'll need to fill in the appropriate details in the Managed IT Operations - Add or Remove Device spreadsheet (UKC-FRM-303) spreadsheet, which enables us to automate your requested changes. This is the same spreadsheet as the one you used to originally set up your service. The Service Request template will include a link to download the spreadsheet. When filling out the spreadsheet, ensure that you follow the instructions provided.

If you want to download the spreadsheet ahead of raising the request, click here.

Defining the monitoring method

You can request to change the monitoring method used for any of your monitored devices.

The UKCloud monitoring system is capable of using either `snmpv2c` or `snmpv3` to perform the basic, standard template checks against an device. Alternatively, if the only checks required are performed remotely (such as ping, port checks, HTTP content checks and so on), you can use `remote-only`.

> [!NOTE] Do not select the `monitoring-agent` method unless previously discussed and agreed with UKCloud.

1. In My Calls, raise a ticket using the **Managed IT Operations - Make changes to my managed devices** template.

2. Download the spreadsheet linked in the template.

If you'd like to make changes, please download the spreadsheet below to specify the list of items that need amending. This will be the same spreadsheet that was originally used during your onboarding. When filling out the spreadsheet, ensure that you follow the instructions on the form. Once updated with your changes, please attach the file to the request offering before submitting to UKCloud.
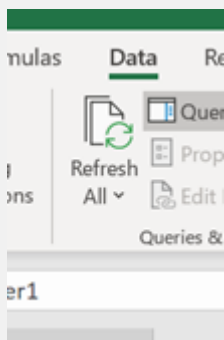
Click here to download the XLS file.

3. On the **Credentials** tab of the spreadsheet, add the set of credentials to be used for the Base/Primary Host template SNMP monitoring protocol.

4. On the **Device Information** tab, enter the details of the device(s) for which you want to change the monitoring method, making sure to select **Yes** in the **ManagedMonitoring** column.

> [!TIP] You can find the details of your devices on previous spreadsheets if you have them. If you don't, and can't remember your device details, contact UKCloud Support, who will be able to provide you with the necessary information.

5. On the **Monitoring - Device Settings** tab, in the row for the appropriate device, from the list in the **MonitoringMethod** column, select the monitoring method you want to use for the device: `snmpv2c`, `snmpv3` or `remote-only`.

> [!TIP] Device names from the **Device Information** tab are auto-populated into the **Monitoring - Device Settings** tab. If the information doesn't auto-populate, in the **Data** ribbon, select **Refresh All**.
>
> Device names will then auto-populate in the **PrimaryDeviceName** column.

6. In the **BaseMonitoringCredentials** column, select the name of the credentials you created on the **Credentials** tab.

7. When you've finished completing the spreadsheet, in your My Calls ticket either click **Select files** and browse to the completed spreadsheet or drag the spreadsheet into the template.

8. Enter the date from which you want the changes to be effective.

9. When you're done, click **Review & Submit** then **Submit**.

As per our standard customer service targets, we aim to resolve your request within two working days.

Overriding default monitoring settings

If the default monitoring thresholds do not meet your requirements, you can request to override them.

1. In My Calls, raise a ticket using the **Managed IT Operations - Make changes to my managed devices** template.

2. Download the spreadsheet linked in the template.
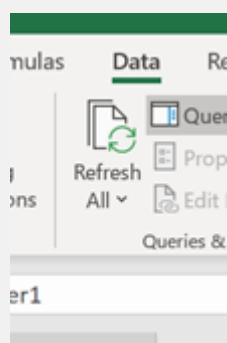

3. On the **Device Information** tab of the spreadsheet, enter the details of the device for which you want to override the default settings, making sure to select **Yes** in the **ManagedMonitoring** column.

> [!TIP] You can find the details of your devices on previous spreadsheets if you have them. If you don't, and can't remember your device details, contact UKCloud Support, who will be able to provide you with the necessary information.

4. On the **Monitoring - Overrides** tab, in the **PrimaryDeviceName** column, select the device you want to change.

> [!TIP] Device names from the **Device Information** tab are auto-populated into the **Monitoring - Overrides** tab. If the information doesn't auto-populate, in the **Data** ribbon, select **Refresh All**.
>
>
>
> Device names will then appear in the **PrimaryDeviceName** dropdown list.

5. In the **AlertType** column, select the monitoring element that you want to override:

   ○ **CPU** - Checks the processor load of the monitored device

   ○ **RAM** - Checks the available memory of the monitored device

   ○ **UNIX_DISK** - Checks the disk spaced used by the monitored device

- **WINDOWS_DISK** - Checks the disk spaced used by the monitored device

- **PING** - Checks the response from the monitored device

6. If you selected **UNIX_DISK** or **WINDOWS_DISK** in the **AlertTarget** column, enter the resource the override will apply to, for example:

   - Disk: For the UNIX_DISK monitoring element, the alert target refers to the mount point to monitor for Linux space/disk consumption, for example, `/home` or `/usr`

   - Windows drive: For the WINDOWS_DISK monitoring element, the alert target refers to the drive letter to monitor for Windows space/disk consumption, for example `C` or `D`

7. From the list in the **RemoveServiceCheck** column, select **TRUE** if you want to disable the check for this monitoring element.

   > [!TIP] If you select **TRUE** in this column, or if the **AlertType** is PING, you do not need to complete the information in the remaining columns.

8. In the **MajorThreshold** column, enter the threshold (as a percentage) above which a major level alert will be raised for the monitoring element, for example `80`.

9. In the **CriticalThreshold** column, enter the threshold (as a percentage) above which a critical level alert will be raised for the monitoring element, for example `95`.

10. When you've finished completing the spreadsheet, in your My Calls ticket either click **Select files** and browse to the completed spreadsheet or drag the spreadsheet into the template.

11. Enter the date from which you want the changes to be effective.

12. When you're done, click **Review & Submit** then **Submit**.

As per our standard customer service targets, we aim to resolve your request within two working days.

Adding additional monitoring elements

Managed Monitoring as a Service provides a default set of monitoring elements (CPU, RAM, UNIX_DISK, WINDOWS_DISK or PING). You can request additional monitoring elements if required.

Currently supported monitoring elements are:

- **URL** - Checks the response from the specified URL; any return of a 200 status code is expected and considered correct

- **URL_CONTENT** - Checks for a specific response from a URL and a looks for a specified string in the returned content

- **CERT_EXPIRY** - Checks whether the specified certificate has expired

- **HOST_PORT** - Checks for a valid connection to the specified port

- **WINDOWS_SERVICE** - Checks the status of the specified service

- **AGENT_PORT** - Checks for a valid connection to the specified agent port

- **UNIX_PROCESS** - Checks whether the specified process is running

To add a monitoring element:

1. In My Calls, raise a ticket using the **Managed IT Operations - Make changes to my managed devices** template.

2. Download the spreadsheet linked in the template.

   If you'd like to make changes, please download the spreadsheet below to specify the list of items that need amending. This will be the same spreadsheet that was originally used during your onboarding. When filling out the spreadsheet, ensure that you follow the instructions on the form. Once updated with your changes, please attach the file to the request offering before submitting to UKCloud.

   Click here to download the XLS file.

   > [!TIP] If you want to download the spreadsheet in advance, you can download it from here

3. On the **Device Information** tab of the spreadsheet, enter the details of the device for which you want to specify additional monitoring elements, making sure to select **Yes** in the **ManagedMonitoring** column.

   > [!TIP] You can find the details of your devices on previous spreadsheets if you have them. If you don't, and can't remember your device details, contact UKCloud Support, who will be able to provide you with the necessary information.

4. On the **Monitoring - Advanced** tab, in the **PrimaryDeviceName** column, select the device to which you want to add the monitoring element.

   > [!TIP] Device names from the **Device Information** tab are auto-populated into the **Monitoring - Advanced** tab. If the information doesn't auto-populate, in the **Data** ribbon, select **Refresh All**.
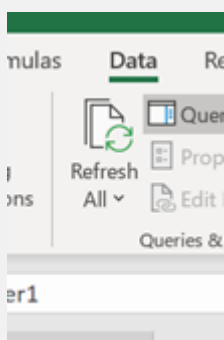
   > Device names will then appear in the **PrimaryDeviceName** dropdown list.

5. In the **AdvancedAlertType** column, select the type of monitoring element you want to add to the device.

6. Complete the rest of the spreadsheet as follows:

Monitoring element	Column	Value
URL	AlertTarget	The URL to check; this may be HTTPS or HTTP
URL_CONTENT	AlertTarget	The URL to check; this may be HTTPS or HTTP
	AlertArgument1	The response code to check for
	AlertArgument2	The string to check for in the returned content
CERT_EXPIRY	AlertTarget	
HOST_PORT	AlertTarget	The port number of the endpoint to check
WINDOWS_SERVICE	AlertTarget	The service name to check the status of
AGENT_PORT	AlertTarget	The port number of the endpoint that the agent installed on the device should be checking
UNIX_PROCESS	AlertTarget	The process name to check the status of

7. When you've finished completing the spreadsheet, in your My Calls ticket either click **Select files** and browse to the completed spreadsheet or drag the spreadsheet into the template.

8. Enter the date from which you want the changes to be effective.

9. When you're done, click **Review & Submit** then **Submit**.

   As per our standard customer service targets, we aim to resolve your request within two working days.

Related articles

- *Default monitoring thresholds and alert handling procedures*

- *How to add and remove devices*

- *How to update contact information for Managed IT Operations*

- *How to provide notification of maintenance windows*

Feedback

If you find a problem with this article, click **Improve this Doc** to make the change yourself or raise an issue in GitHub. If you have an idea for how we could improve any of our services, send an email to feedback@ukcloud.com.