adaptiva

Adaptiva Endpoint Health User Guide

Updated: June 5, 2023

Endpoint Health

Table of Contents

Introduction

Adaptiva Endpoint Health performs scheduled or instant health checks, on either a specific device or a collection/group, to help you maximize the success of your computer management services. Automatic or manual remediation is available to fix common problems on failing machines. The Health Checks and Remediations can be extended with custom scripts to integrate with an organization's requirements.

Features

- Independent Monitoring Framework: Does not use ConfigMgr, Intune or VMware client-side framework
- Reduced Cost: For managing Applications, Operating Systems and devices
- Centralized: Visibility and control for administrators
- Extensible: Ability to add custom checks or edit existing checks. Health Checks are exportable for re-use and sharing
- Endpoint Health Policies: Scheduled and instant
- Can be run on individual devices or on collections/groups
- Automatic or manual remediation
- ConfigMgr agent - installation, version, service status, site assignment, heartbeat discovery
- ConfigMgr infrastructure pings - Software and Hardware inventory, Policy, Package
- Operating System component checks
- System performance checks
- Security checks and validations – malware vulnerability for Bad Rabbit, Wanna Cry
- Windows 10 – Credential Guard, Device Guard, Edge version, UEFI, WMI
- Windows Update checks
- Failed check collections (when integrated with ConfigMgr)
- Detailed Dashboards: SQL Server Reporting Services is not required. Results are viewable for devices, collections/groups or Health Checks. Displays the results of the Health Check and any Remediation.

Getting Started

We want you to have the most productive experience using Endpoint Health. Please review this guide and consider the following points before beginning your usage of Endpoint Health.

1. The Adaptiva Client must be installed on all machines to target for Health Checks.
2. The **Deploying Health Checks** section below describes how to quickly schedule clients for Health Checks. The remaining sections of this document provide an in-depth explanation of various features and components.

How Adaptiva Endpoint Health Applies to a Common Scenario

The Situation

IT organizations are traditionally effective at diagnosing and repairing issues that arise for users. Unfortunately, they have been limited in their ability to detect problems and guarantee that the systems are healthy. Unreported issues do not get fixed and leave the administrators with systems that become increasingly difficult to manage. Additionally, IT administrators spend much of their time troubleshooting and fixing similar problems over and over again.

The Problem

A typical organization has a system in place to track issues. As problems occur on machines, users create reports and technicians are dispatched to resolve these issues. However, there is no guarantee that the user will report their issues. This becomes compounded by the fact that many IT management solutions rely on client software running on user machines, even though the user is unaware of its existence. For example, when critical ConfigMgr features are failing on a client, the administrator is unable to detect those problems until he attempts to perform an operation on that machine. His time is wasted diagnosing and fixing these common issues.

The Solution

Adaptiva Endpoint Health allows the IT organization to guarantee that a system is in a healthy state, reducing time required for updates and distribution. Problems are reported and addressed proactively, causing less disruption to users. It also frees up administrators from performing repetitive tasks through automation, reducing cost for the IT organization.

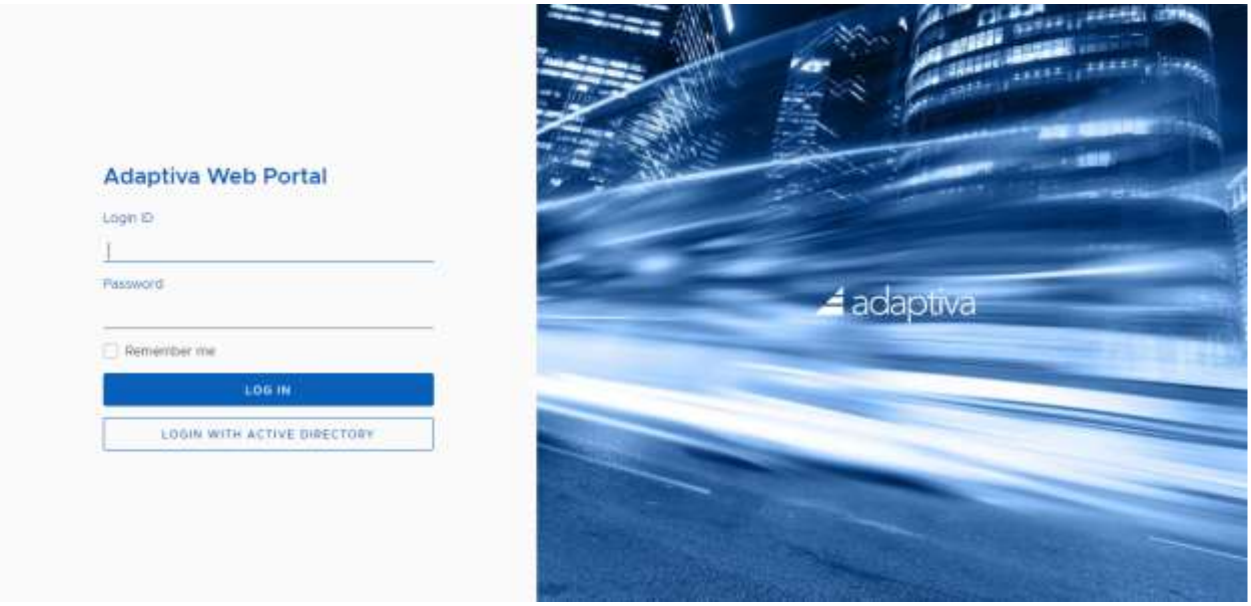
Using Adaptiva Endpoint Health, administrators can:

- Automate Health Checks to guarantee system health
- Automatically fix common problems to free up their time
- Instantly run Health Checks or Remediations as a response to user issues
- Modify or create new Health Checks to define what system health means for their organization

Navigating the Adaptiva Web Portal

To launch the Adaptiva Web Portal, open any web browser, other than Internet Explorer, Edge or Chrome is recommended, and enter http://AdaptivaServerFQDN[:port] where :port is optional. If the server is already using port 80, for example, the web site might use port 9678. Confirm the port with the Adaptiva administrator.

User Authentication



The Adaptiva Web Portal Login dialog will open.

- **Use Native Adaptiva Login** – To use an Adaptiva native login account, enter the Login ID (email address), and password and click **LOG IN**

  Check the box **Remember me** to save the Login ID for next time accessing the Web Portal

- **Use Currently Logged on User's Windows Credentials** – Click **Login with Active Directory** will allow the user to login using their current login token – it does not have to be an AD Account.

By default, when you install Adaptiva Server, the person installing either selects a Windows AD account to be used as the SuperAdmin or creates an Adaptiva login which is used as the SuperAdmin. This can be used for the initial logon. An administrator can later create new logins (administrators in the interface) and assign roles and permissions.

Licensing Adaptiva

Adaptiva products require a license for each active client reporting to the site for which it is installed. The Adaptiva Server will periodically count all active, healthy, reporting clients as licensed clients.

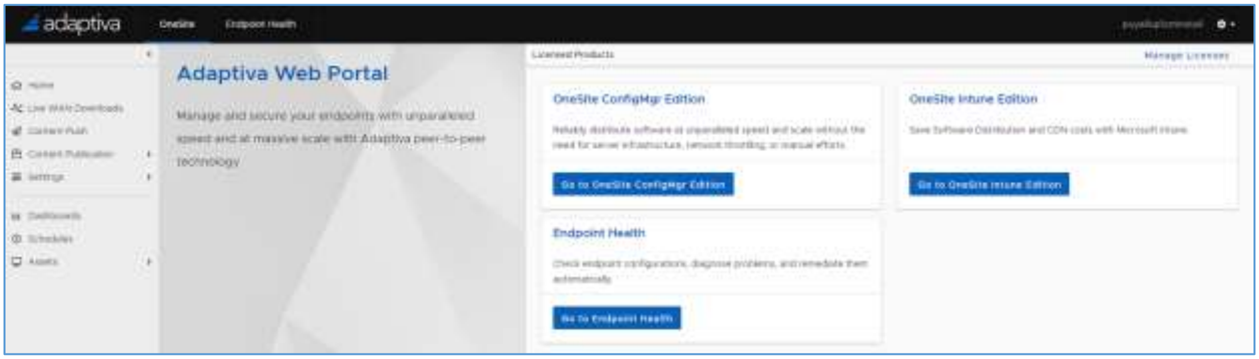
The license key will contain the licensed Company name and client count. The license key needs to be entered using the Adaptiva Web Portal or Adaptiva Workbench.

- If you are starting the Adaptiva Web Portal for the first time or your key has expired, you will be prompted for a key at login.
- You can view keys or add more by selecting ⚙, **Product Licensing**. This is also accessible at the URL: http://AdaptivaServerFQDN[:port]/licensing

Products will function for a period of 30 days from the date of installation for evaluation purposes. If additional evaluation is required, please contact ticket@adaptiva.com.

Web Page Orientation

The Adaptiva Web Portal is used to configure Adaptiva and display Dashboards of the results of the Adaptiva solutions, OneSite Cloud, OneSite ConfMgr Edition, OneSite Intune Edition, OneSite VMWare Edition, and Endpoint Health.



Manage and secure your endpoints with unparalleled speed and at massive scale with Adaptiva peer-to-peer technology

Reliably distribute software at unparalleled speed and scale without the need for server infrastructure, network throttling, or manual efforts.

Save Software Distribution and CDN costs with Microsoft Intune.

Check endpoint configurations, diagnose problems, and remediate them automatically.

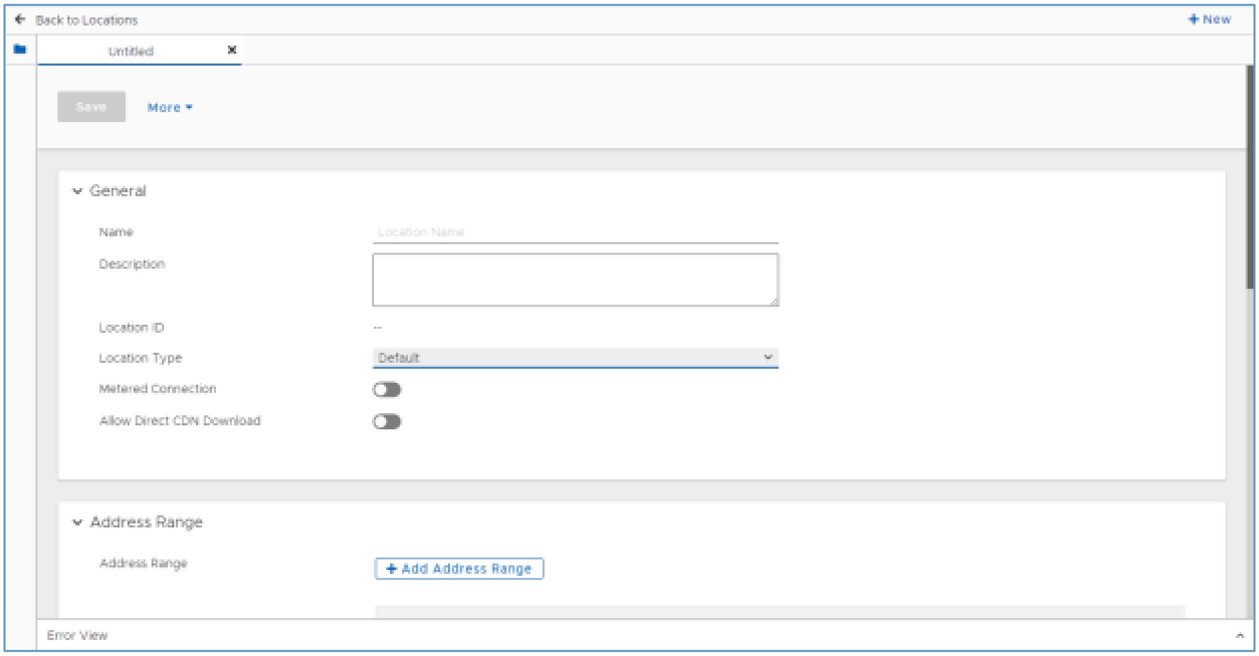
On the left is the Activity pane. The top section of the Activity pane is specific to each solution and below the line are activities common to all solutions. These items will either display a Dashboard or drill into the specific activity, e.g., Content Push or Content Publication.

There are also menu items to create new Schedules, view Devices, Groups and Locations.

Some Activity pane items have pull-out menus. To display the pull-out menu, select it or hover over it and the pull-out menu will display. Select the desired item from the pull-out menu.

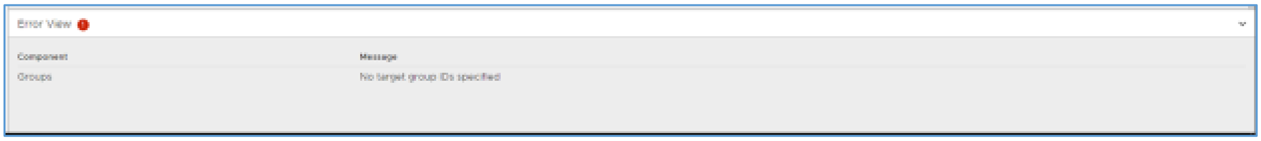
If a pull-out menu is stuck out, simply click in the blank space on the page to make it disappear.

At the bottom of Editor pages, will be a collapsed section named **Error View**, which will display any errors found when saving a form.



Name	Location Name
Description	
Location ID	--
Location Type	Default
Metered Connection	○
Allow Direct CDN Download	○
Address Range	+ Add Address Range

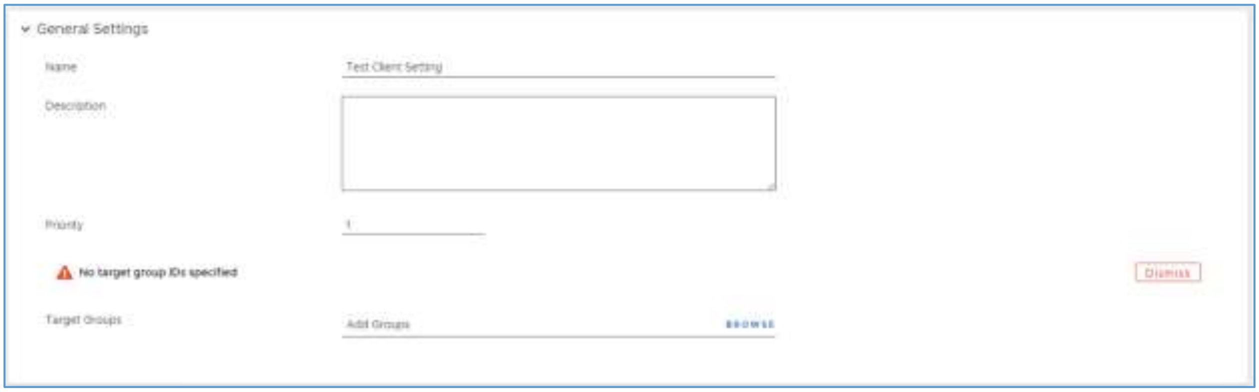
Clicking on Error View will expand the section and show any relevant errors for that Editor.



Error View

Component	Message
Groups	No target group IDs specified

The error will also be displayed in the form.



General Settings

Name: Test Client Setting

Description:

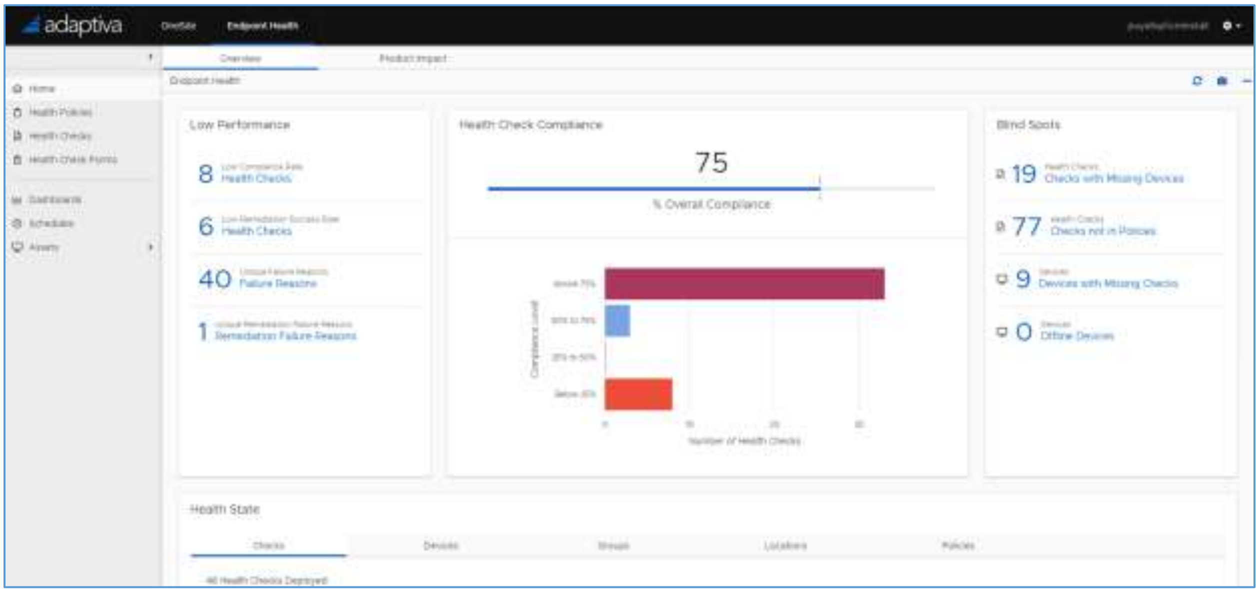
Priority: 1

No target group IDs specified — Dismiss

Target Groups: Add Groups — BROWSE

Endpoint Health

The Endpoint Health Home page provides an overview of the health checks that have been run in your environment.


adaptiva
OneSite
Endpoint Health
Overview
Product Impact
Endpoint Health
Home
Health Policies
Health Checks
Health Check Forms
Dashboards
Schedules
Alerts
Low Performance
8 Low Compliance Rate Health Checks
6 Low Remediation Success Rate Health Checks
40 Unique Failure Reasons Failure Reasons
1 Unique Remediation Failure Reasons Remediation Failure Reasons
Health Check Compliance
75
% Overall Compliance
Above 75%
50% to 75%
25% to 50%
Below 25%
Compliance Level
0
10
20
30
Number of Health Checks
Blind Spots
19 Health Checks Checks with Missing Devices
77 Health Checks Checks not in Policies
9 Devices Devices with Missing Checks
0 Devices Offline Devices
Health State
Checks
Devices
Groups
Locations
Policies
46 Health Checks Deployed

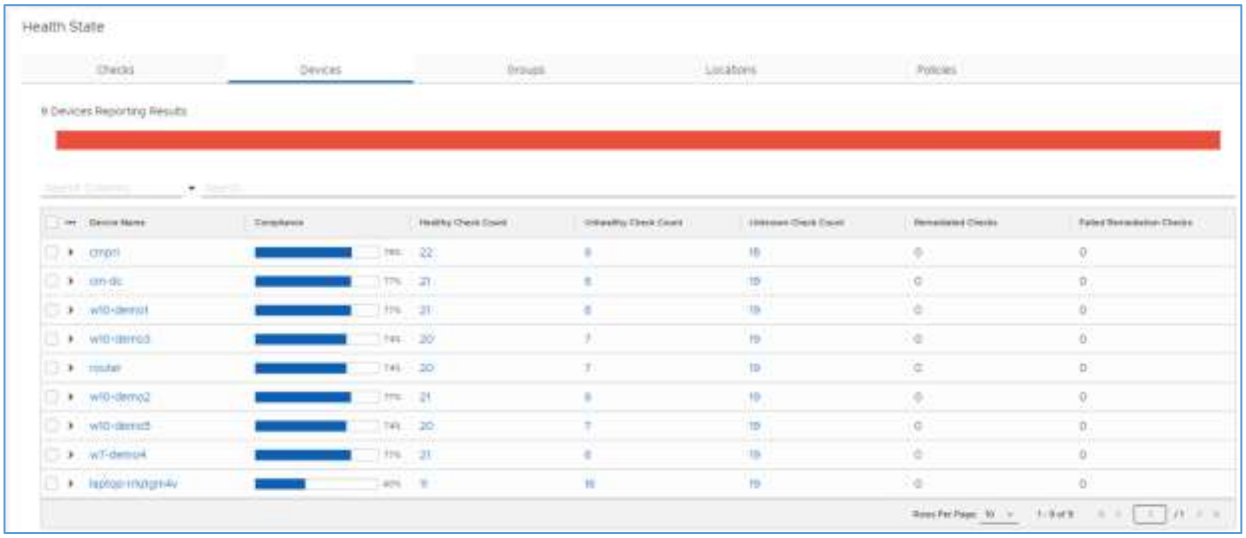
The Endpoint Health Overview page has the following sections:

Low Performance provides information on the number of health checks with low compliance, low remediation success as well as the total number of unique failures and unique remediation failures. Each item can be drilled into to show the list of health checks or failure reasons.

Blind Spots shows what is not being analyzed. Which health checks are targeting no devices, which health checks are not included in policies. What devices are not being checked and which devices have not checked in. Blind Spots helps to ensure you are covering the entire environment.

The main tile is the Health Check Compliance. This shows the overall compliance of all scheduled health checks as well as the Compliance Level of the scheduled health checks.

At the bottom of the page is the Health State summary. This shows the compliance of each health check that has been run. The number of healthy, unhealthy and remediated devices. This is shown by Health Check, by Device, by Group (Adaptiva Groups only), by Location and by policy (this includes legacy Health Checks as well). The picture below shows the Device compliance results.



9 Devices Reporting Results

Device Name	Compliance	Healthy Check Count	Unhealthy Check Count	Unknown Check Count	Remediated Checks	Failed Remediation Checks
cmpri	78%	22	6	18	0	0
cm-dc	77%	21	6	19	0	0
w10-demo1	77%	21	6	19	0	0
w10-demo3	74%	20	7	19	0	0
router	74%	20	7	19	0	0
w10-demo2	77%	21	6	19	0	0
w10-demo5	74%	20	7	19	0	0
w7-demo4	77%	21	6	19	0	0
laptop-mutgn4v	40%	11	16	19	0	0

Rows Per Page: 10 1 - 9 of 9 1 / 1

Security and Access Control

The Adaptiva Workbench and the Adaptiva Web Portal support two forms of user authentication:

- Active Directory User (Recommended)
- Internal Adaptiva User ID

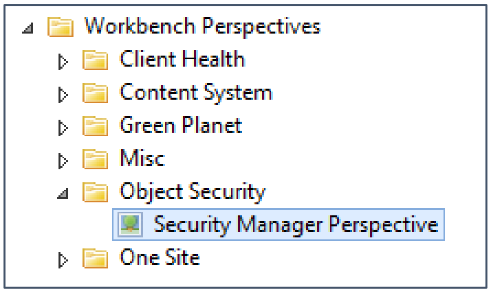
During the installation of the Adaptiva Server, the installer allows the administrator to create an Adaptiva User ID or specify an AD user account as SuperAdmin. The SuperAdmin account has the maximum permissions in the Adaptiva environment.

Security can only be managed using the Adaptiva Workbench.

Security Manager Perspective

OneSite's security model is administered from the **Security Manager Perspective**.

To manage security, open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **Object Security** folder, and select **Security Manager Perspective**.



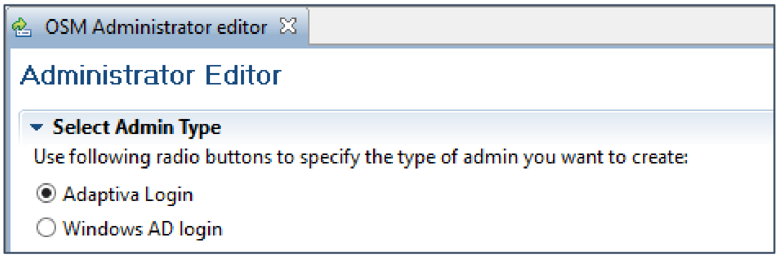
In the **OSM Task Navigator** pane, the following **Tasks** are available:

- Create new Role
- Create new Administrator
- Manage Roles
- Manage Administrators
- Manage class level permissions
- Manage folder level permissions
- View resulting permissions
- View access list

Adding New Administrators

To add a new administrator, in the **Security Manager Perspective**, select **Create new Administrator**.

1. In the center of the workbench, the **Administrator Editor** will appear.
2. In the **Select Admin Type** section, choose either **Adaptiva Login** or **Windows AD login**.



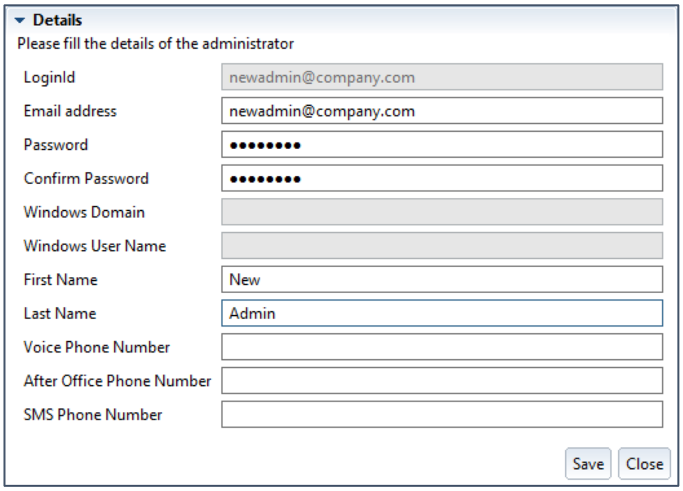
Use following radio buttons to specify the type of admin you want to create:

● Adaptiva Login

○ Windows AD login

a. If selecting Adaptiva Login, in the **Details** section, fill in the following required fields:

Email address, Password, First Name, and Last Name. The remaining fields are optional. Click **Save** to create the login.



Details

Please fill the details of the administrator

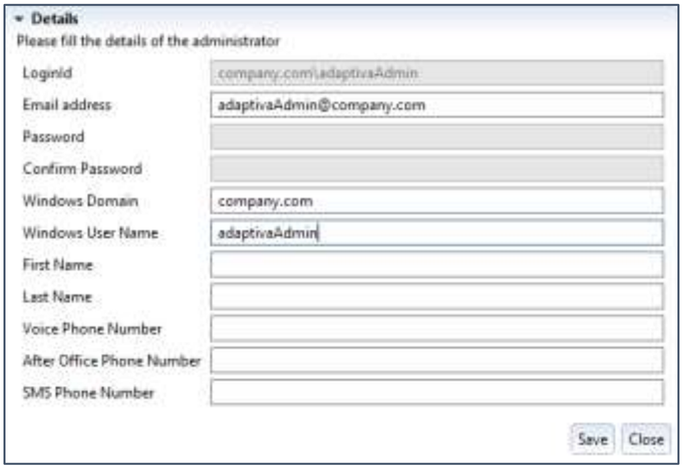
LoginId	newadmin@company.com
Email address	newadmin@company.com
Password	••••••••
Confirm Password	••••••••
Windows Domain	
Windows User Name	
First Name	New
Last Name	Admin
Voice Phone Number	
After Office Phone Number	
SMS Phone Number	

NOTE: Strong passwords are enforced for Adaptiva accounts, the password must be at least 10 characters long, and contain at least 1 or more digit, uppercase and lowercase letter.

In the **Select Administrator** dialog, select the **OneSite Admins** folder and click **OK**.

b. If selecting **Windows AD login**, in the **Details** section, fill in the following required fields:

Email address, Windows Domain, and Windows User Name. The remaining fields are optional. Click **Save** to create the login.



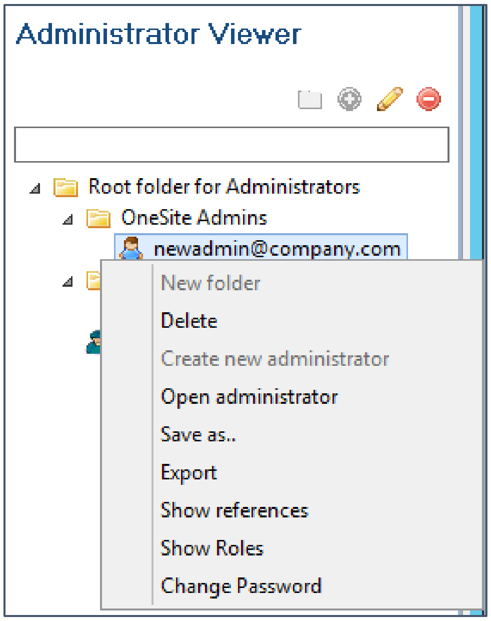
Details

Please fill the details of the administrator

LoginId	company.com\adaptivaAdmin
Email address	adaptivaAdmin@company.com
Password	
Confirm Password	
Windows Domain	company.com
Windows User Name	adaptivaAdmin
First Name	
Last Name	
Voice Phone Number	
After Office Phone Number	
SMS Phone Number	

In the **Select Administrator** dialog, select the **Windows Administrators** folder and click **OK**.

3. On the right of the workbench, in the **Administrator Viewer** pane, the new administrative accounts will appear. For example, to edit or delete an account, simply right-click the account and select the appropriate option in the context menu.



Administrator Viewer

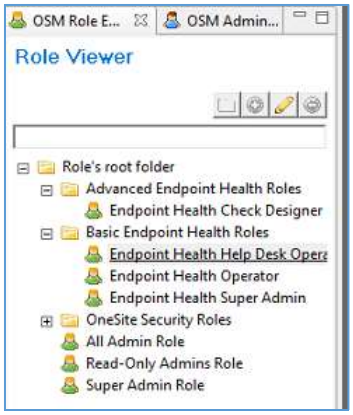
Assigning Roles to Administrators

By default, all new users created are added to the **All Admin** role which has limited access. To add a user to another security role, in the **Security Manager Perspective**, select **Manage Roles**.

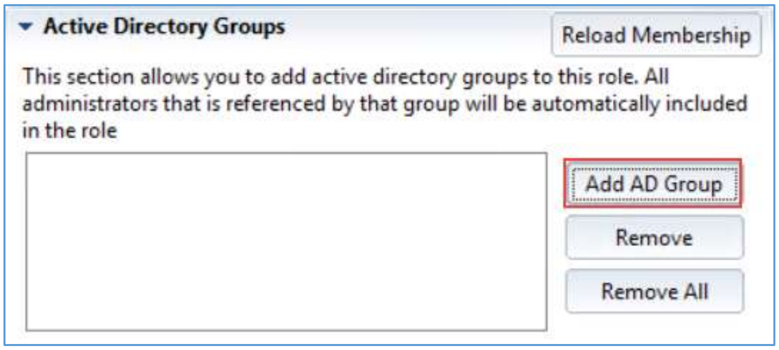
Endpoint Health adds the following roles:

Role Name	Role Description
Endpoint Health Check Designer	Members of this role can create Health Checks
Endpoint Health Help Desk Operator	Members of this role can run Instant Health Checks against an individual computer or collection or group of computers
Endpoint Health Operator	Members this role can use all existing Health Checks, create scheduled Health Checks, run Instant Health Checks
Endpoint Health Super Admin	Members of this role can do all the Operator can do including the ability to Import and Export Health Checks and their related objects

1. On the right of the workbench, in the **Role Viewer** pane, expand **Role's root folder**, then double-click the role to edit it. For example, to grant someone Endpoint Health Help Desk Operator rights, open the Endpoint Health Help Desk Operator Role.



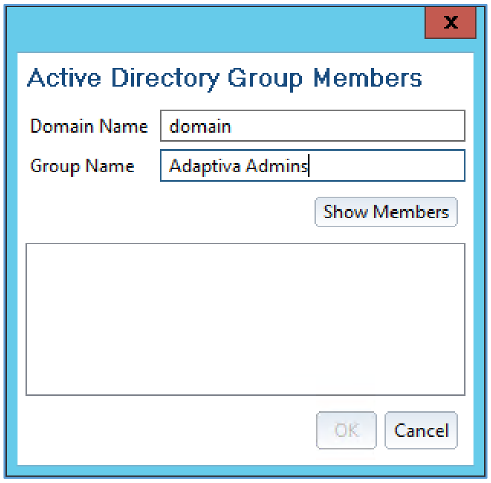
2. In the center of the workbench, the **Role Editor** will appear. In the **Role Properties** section, the name and group can be customized.
3. To add a user to the **Direct Administrators** section, click on the **OSM Administrators Explorer** tab and then drag and drop the individual administrator from the **Administrator Viewer** pane to the box. Alternatively, you may click the **Add Administrator** button to select the account.
4. In the **Active Directory Groups** section, click **Add AD Group** to search for and add an AD group to the role.



This section allows you to add active directory groups to this role. All administrators that is referenced by that group will be automatically included in the role

NOTE: Currently, Universal Groups are not supported and cannot be selected

5. In the **Active Directory Group Members** dialog, enter the **Domain Name**, and the **Group Name** then click the **Show Members** button. The **OK** button will become active after listing the group members. Click **OK** to add the group to the role.



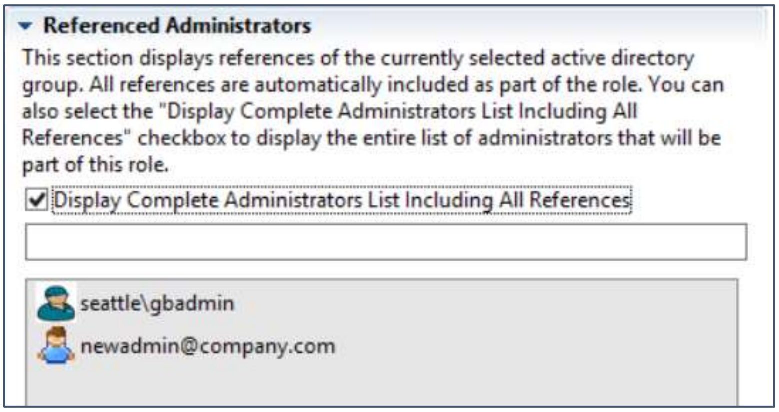
Active Directory Group Members

Domain Name: domain

Group Name: Adaptiva Admins

NOTE: Currently, nested group membership is not supported, only direct members will be returned

6. In the **Referenced Administrators** section, to enumerate the list of Administrators, including those in groups, check the box: **Display Complete Administrators List Including All References**.



Referenced Administrators

This section displays references of the currently selected active directory group. All references are automatically included as part of the role. You can also select the "Display Complete Administrators List Including All References" checkbox to display the entire list of administrators that will be part of this role.

☑ Display Complete Administrators List Including All References

seattle\gbadmin

newadmin@company.com

NOTE: This will show who is currently in the role. Save and re-open to ensure the newly added members are listed.

7. Once complete, click **Save** at the top of the editor.

Creating New Roles

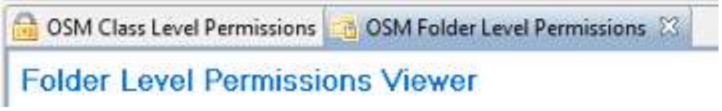
Some organizations may want to create custom roles to control access to what some administrators can view or change.

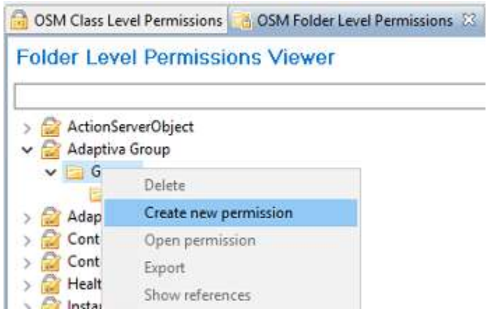
1. To create a new custom role, in the **Security Manager Perspective**, select **Create new Role**.
2. In the **Role Editor**, enter a **Name** for the new role and optionally provide a description.
3. Click **Add an Administrator** or **Add an AD Group** to add the respective accounts. Repeat for all Administrators or Groups.

> ***NOTE: You must add at least one administrator to the role to enable the Save button. However, you can remove the administrator if you desire to create an empty role.***

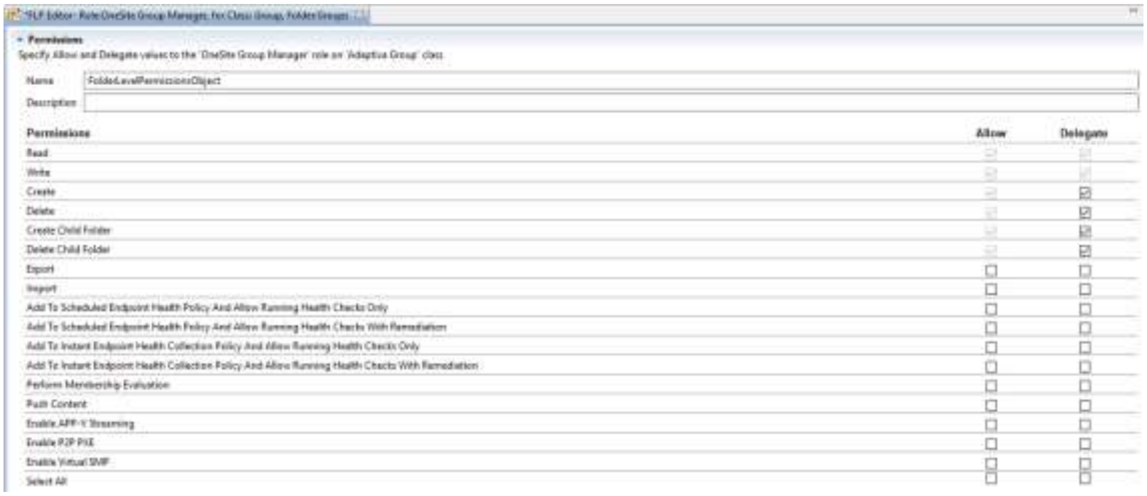
4. Click **Save** to create the role
5. In the **Role Viewer** dialog box, select a folder for the role such as **OneSite Security Roles**
6. Click **Close**

Assigning Permissions to a Role

1. In the Workbench, under the editor are two views which are used to manage permissions:
1. OSM Class Level Permissions – Manages access to the different classes within OneSite
2. OSM Folder Level Permissions – Manages access to different folders within OneSite
3. 
OSM Class Level Permissions
OSM Folder Level Permissions
Folder Level Permissions Viewer
4. For example, if a role was created named OneSite Group Manager where they will be granted access to create and manage Adaptiva groups. Select the **OSM Folder Level Permissions** tab.
2. In the **OSM Folder Level Permissions Viewer** expand the object **Adaptiva Group** then right-click the child object **Groups** and select **Create new permission**.



3. In the **Select the role…** dialog, select the role the permissions should be applied to. In this example, select the **Adaptiva Group Manager** role and then click **OK**.
4. In the editor, use the **Allow** checkboxes to grant granular access (permission will be denied, if left unchecked).
5. Use the **Delegate** checkboxes to allow this user to granularly assign permissions to other user accounts. Click **Save** to apply the permissions.



*FLP Editor - Role OneSite Group Manager, for Class Group, Folder Groups

Permissions

Specify Allow and Delegate values to the 'OneSite Group Manager' role on 'Adaptiva Group' class

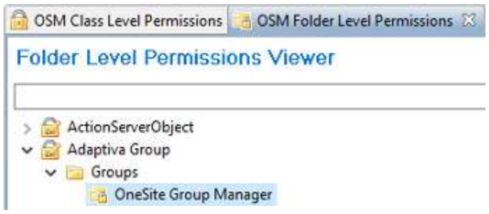
Name: FolderLevelPermissionsObject

Description:

Permissions	Allow	Delegate
Read	☑	☑
Write	☑	☑
Create	☑	☑
Delete	☑	☑
Create Child Folder	☑	☑
Delete Child Folder	☑	☑
Export	☐	☐
Import	☐	☐
Add To Scheduled Endpoint Health Policy And Allow Running Health Checks Only	☐	☐
Add To Scheduled Endpoint Health Policy And Allow Running Health Checks With Remediation	☐	☐
Add To Instant Endpoint Health Collection Policy And Allow Running Health Checks Only	☐	☐
Add To Instant Endpoint Health Collection Policy And Allow Running Health Checks With Remediation	☐	☐
Perform Membership Evaluation	☐	☐
Push Content	☐	☐
Enable APP-V Streaming	☐	☐
Enable P2P PXE	☐	☐
Enable Virtual SMP	☐	☐
Select All	☐	☐

5. Click **Close** to close the **Permissions** tab

6. Expand **Groups** in the **OSM Folder Level Permissions** viewer to see the role has been added


OSM Class Level Permissions
OSM Folder Level Permissions
Folder Level Permissions Viewer
ActionServerObject
Adaptiva Group
Groups
OneSite Group Manager

Deploying Endpoint Health Checks

Health Policies define the Where/When/How of Health Check execution. The administrator provides a collection/group, a schedule and includes specific health checks to run on the target machines.

Health Policies can be executed on a defined scheduled or can be run instantaneously as an Instant Health Policy. Instant Health Policies can be targeted to one device or, along with Health Policies, targeted to a group/collection of devices.

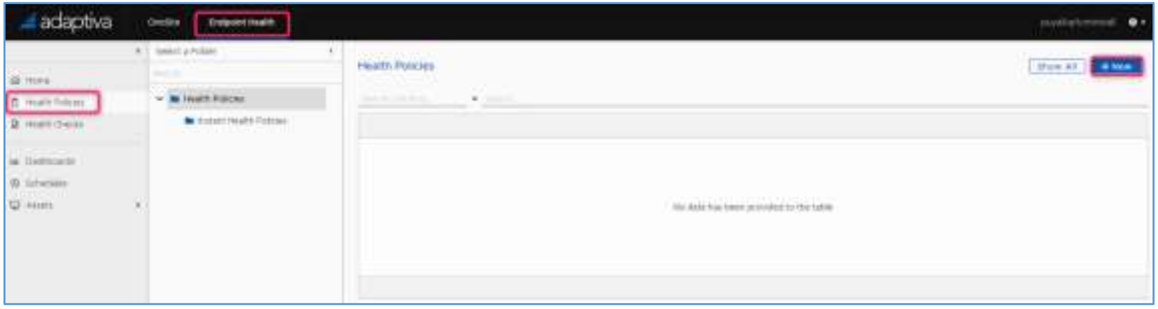
The Health Checks included in a Health Policy will be run sequentially, and remediation can be enabled/disabled for each Health Check individually.

The administrator can specify whether to perform remediation on failure, or force remediation to execute on a healthy machine. Any additional parameters required for running the health check will be displayed in the policy for editing.

Please see the section: **List of Health Checks** for information regarding health checks that ship with the product.

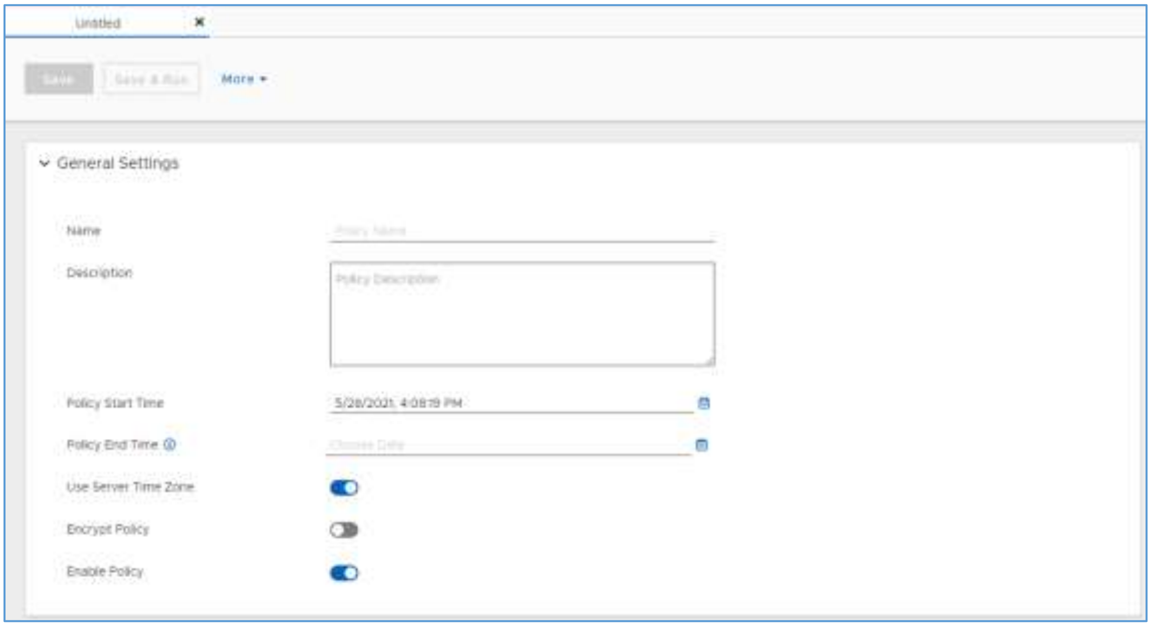
Creating a Health Policy

1. In a web browser connect to the Adaptiva Web Portal (except Internet Explorer) – http://AdaptivaServerFQDN[:port]
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click **Go to Endpoint Health** or click **Endpoint Health** from the Solution list across the top
4. Select **Health Policies** from the Activity workspace on the left



No data has been provided to the table

5. Click **+ New**



General Settings

Name: Policy Name

Description: Policy Description

Policy Start Time: 5/28/2021, 4:08:19 PM

Policy End Time: Choose Date

Use Server Time Zone: ●

Encrypt Policy: ○

Enable Policy: ●

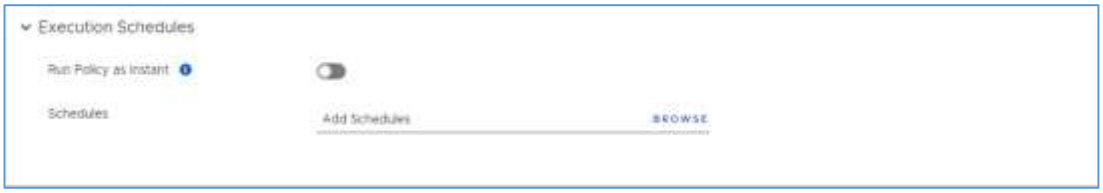
Complete the following sections:

General Settings

Name: Enter a name for the Health Policy. i.e. Daily Checks
Description: Enter a description
Policy Start Time: Enter the date and time this policy should run on the target devices
Policy End Time: (Optional) Enter the date and time this policy should stop running
Use Server Time Zone: If the Start and End Time should follow the time zone of the target devices, toggle is option off (to the left). By default, Health Check Policies will use the Server Time Zone
Encrypt Policy: Toggle (slide to the right) to encrypt the policy
Enable Policy: Toggle (slide to the left) to disable this policy.

> ***Target Devices will still receive the policy, but the policy will not execute until it is enabled***

Execution Schedules



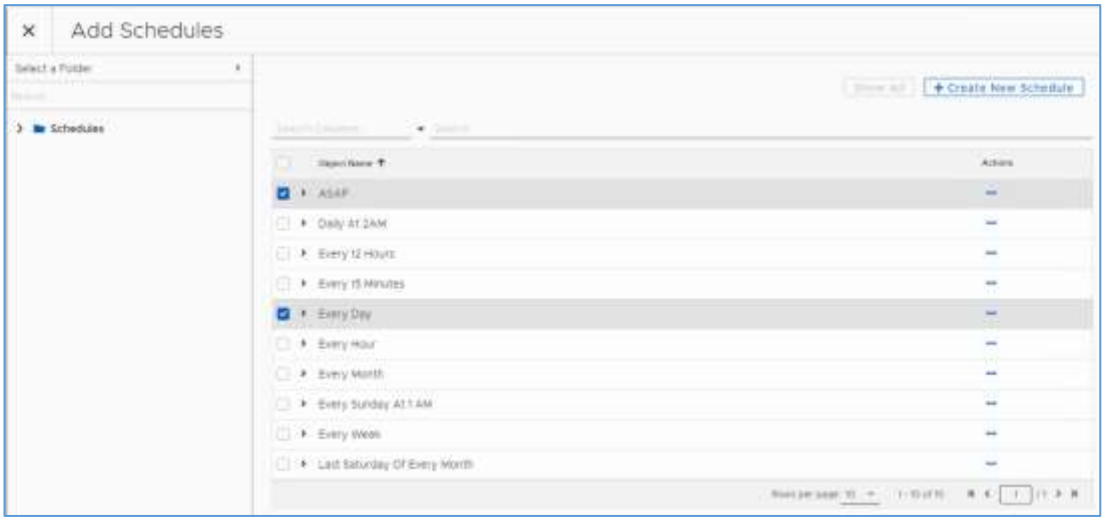
Execution Schedules

Run Policy as Instant: ○

Schedules: Add Schedules

Run Policy as Instant: Toggle (slide to the right) to create an Instant Health Policy. This will remove the schedule and report results only when executed.

Schedules: Click **Browse** to select the schedule to add



	Object Name	Actions
☑	ASAP	—
□	Daily At 2AM	—
□	Every 12 Hours	—
□	Every 15 Minutes	—
☑	Every Day	—
□	Every Hour	—
□	Every Month	—
□	Every Sunday At 1 AM	—
□	Every Week	—
□	Last Saturday Of Every Month	—

Rows per page: 10 1-10 of 10 1

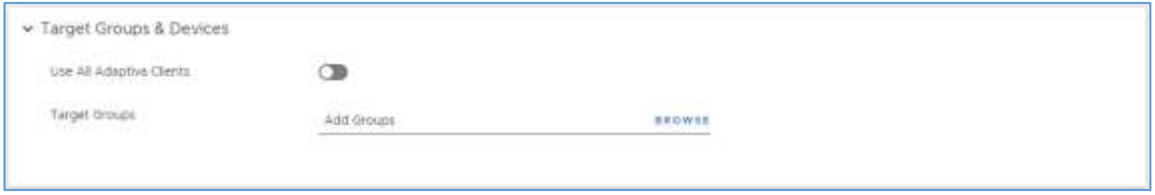
ASAP and non-recurring schedules run once and are not repeated. Recurring schedules are used for scheduling policies to be run on a regular basis. A recurring schedule is useful in the case where a machine hosting content from a content push policy goes offline and the additional copies of the content should be maintained. When the client runs the policy again, it will verify that the policy settings are being enforced and if additional copies of content need to be made, it will do so at that time.

A recurring schedule will take effect after the configured start time. When a task is scheduled for a particular day, it will run at the time of day provided in the start time. For example, if a policy is scheduled to run on the last day of the month, starting on March 5th, at 5pm, it will fire on March 31st at 5pm, April 30th at 5pm and so on.

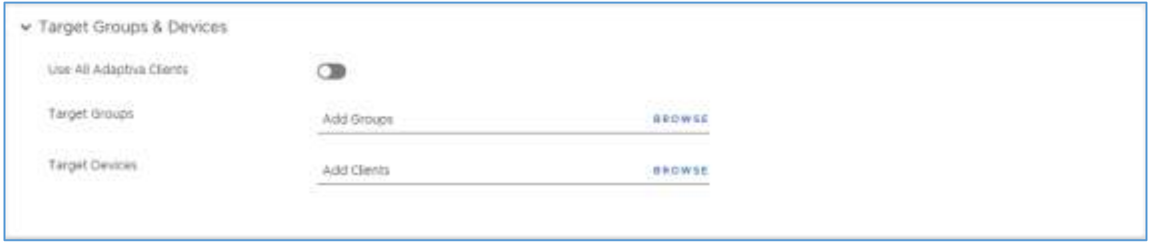
Check one or more boxes next to the desired schedule(s) or click **+Create New Schedule** to create a new Schedule

Click **Add to List** to return to the Health Policy

Target Groups & Devices

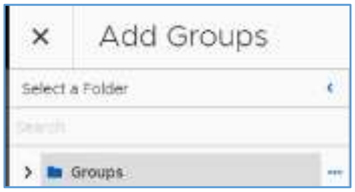


When **Run Policy as Instant** is selected, individual devices can be selected.



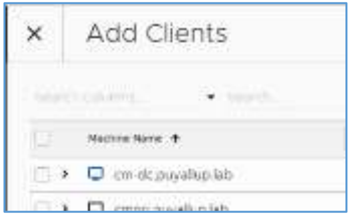
Use All Adaptiva Clients – Toggle (slide to the right) to target All Adaptiva clients

Target Groups – Or click on **Browse** to select specific Adaptiva Groups or ConfigMgr collections



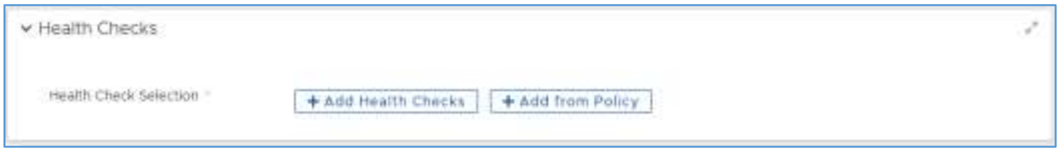
Check the box by the group name(s) and click **Add to List** to return to the Health Policy. Click on the Groups folder will list only the Adaptiva Groups. Click on ConfigMgr Collections \ Device Collections to browse the device collection from ConfigMgr

Target Devices – When Run Policy as Instant is select, individual devices can be selected. Click on **Browse** to select specific devices

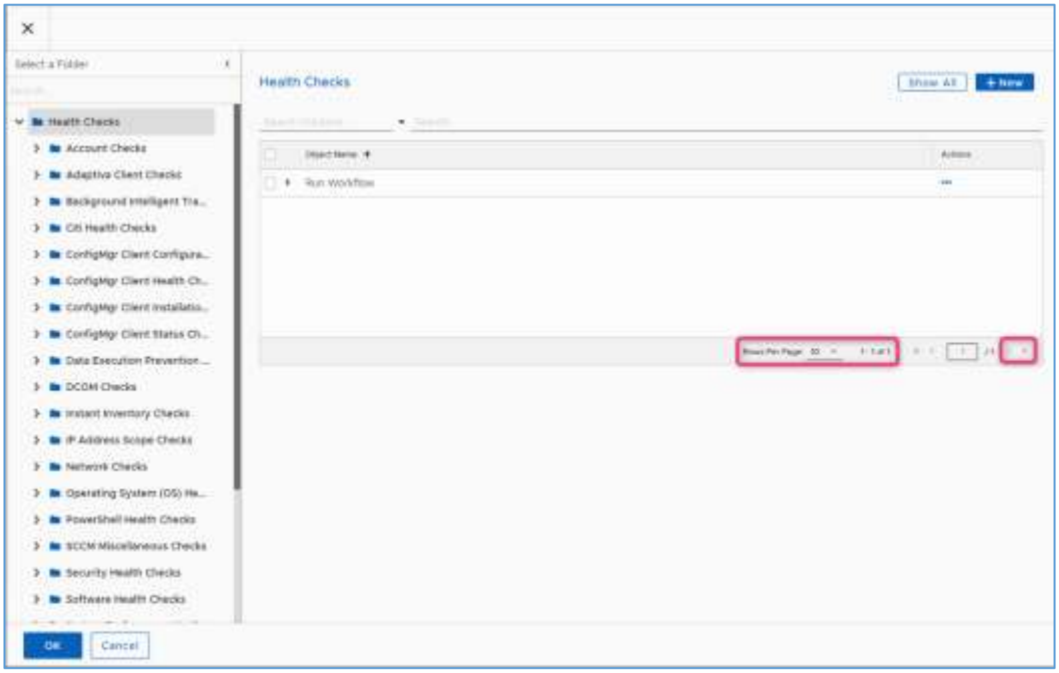


Check the box by the device name(s) and click **Add to List** to return to the Health Policy. Use the Search fields to find specific devices

Health Checks



Click on **Add Health Checks**

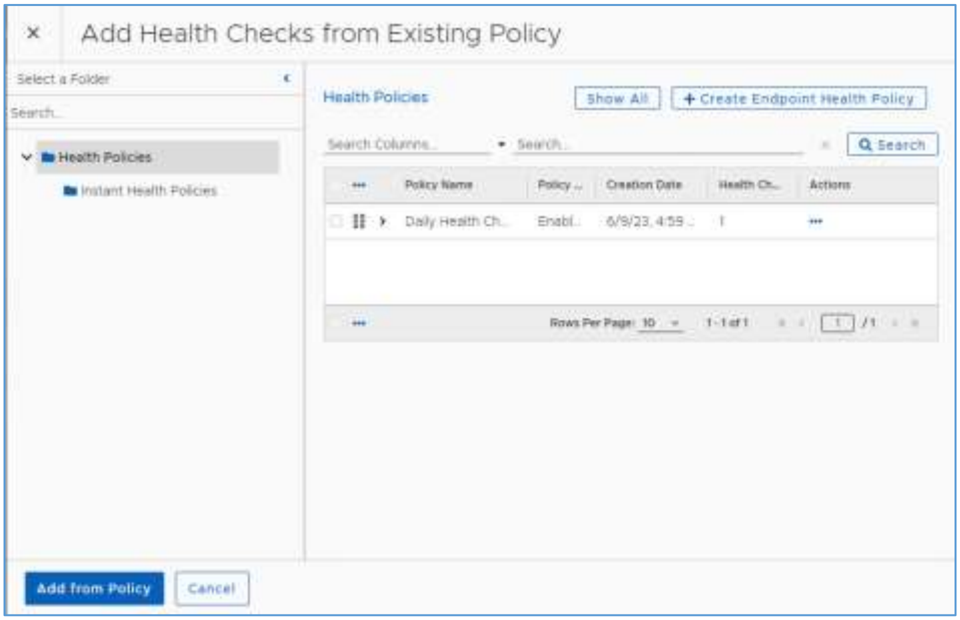


Check one or more boxes next to the desired Health Check(s) or click **+New** to create a new Health Check

The > next to the folder will expand the folder to show any subfolders. Click on the folder to see the Health Checks

Click **OK** to return to the Health Policy

Alternatively, click on **Add from Policy** to add all the health checks and their settings from another Health Policy.



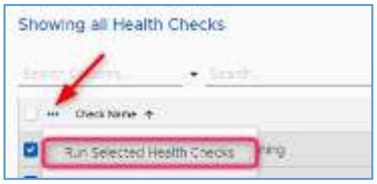
Policy Name	Policy ...	Creation Date	Health Ch...	Actions
Daily Health Ch...	Enabl...	6/9/23, 4:59 ...	1	•••

Select one or more Health Policies

Click **Add from Policy** to return to the Health Policy

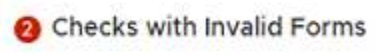
Be sure to note how many Health Checks were returned. By default only the first 10 are shown. Increase the rows per page to show more, or click on the > or >| button to go to the next page.

TIP: Another way to quickly create a Health Policy: Select Health Checks from the Activity Pane, Select Show All, Check the box next to each Health Check to be added to the Health Policy, click on the ellipses (…) at the top and select Run Selected Health Checks

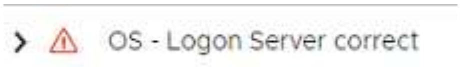


The Health Policy will default to an Instant Health Policy, but that can be turned off to create a Scheduled Health Policy

6. After the Health Checks are selected and returned to the Health Policy, if the Health Check has a form, the form will be checked for missing required parameters. If there are missing requirements the following will be displayed:



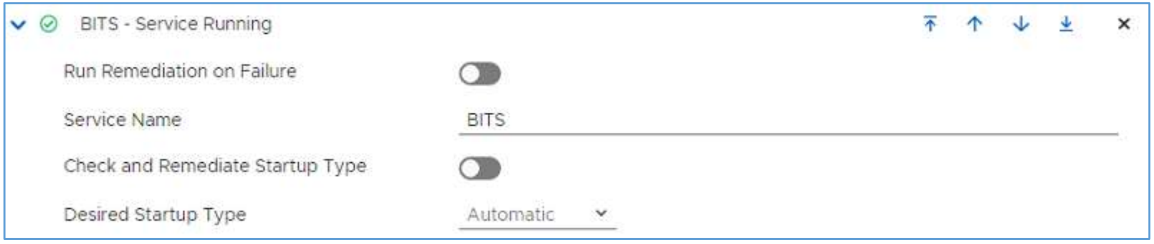
Scroll through the list of forms selected to find which forms need to be completed. For example:



If all forms are OK

All Check Forms Valid

7. For each Health Check click on **>** next to each name.
   If the Health Check has forms, enter the correct values.
   If the Health Check can be remediated toggle Run Remediation on Failure (slide to the right)



BITS - Service Running

Run Remediation on Failure	
Service Name	BITS
Check and Remediate Startup Type	
Desired Startup Type	Automatic

   Use the following icons to change the order of the health check policy execution

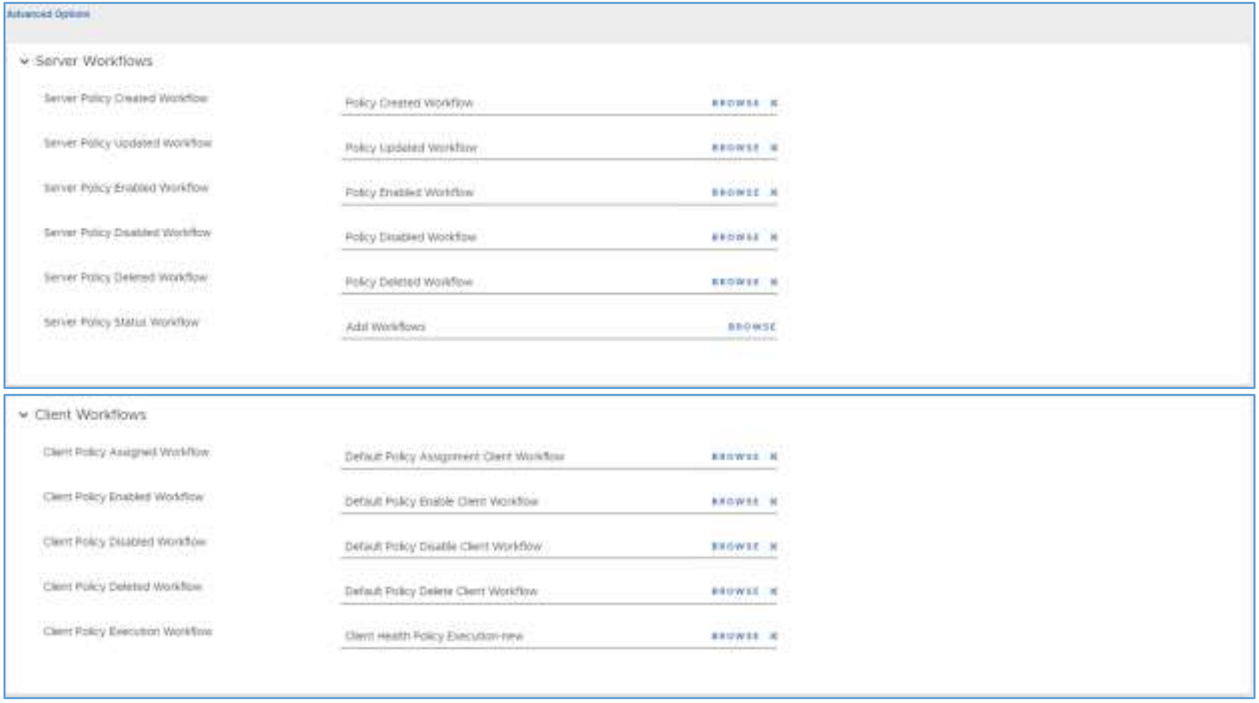
   ⤒ Move Health Check to the Top

   ↑ Move Health Check Up

   ↓ Move Health Check Down

   ⤓ Move Health Check to the Bottom

8. (Optional) **Advanced Options**.
   Select Advanced Options to change the way the policy will execute and inject different logic into the process. In most cases, these settings should be left as is.



Advanced Options

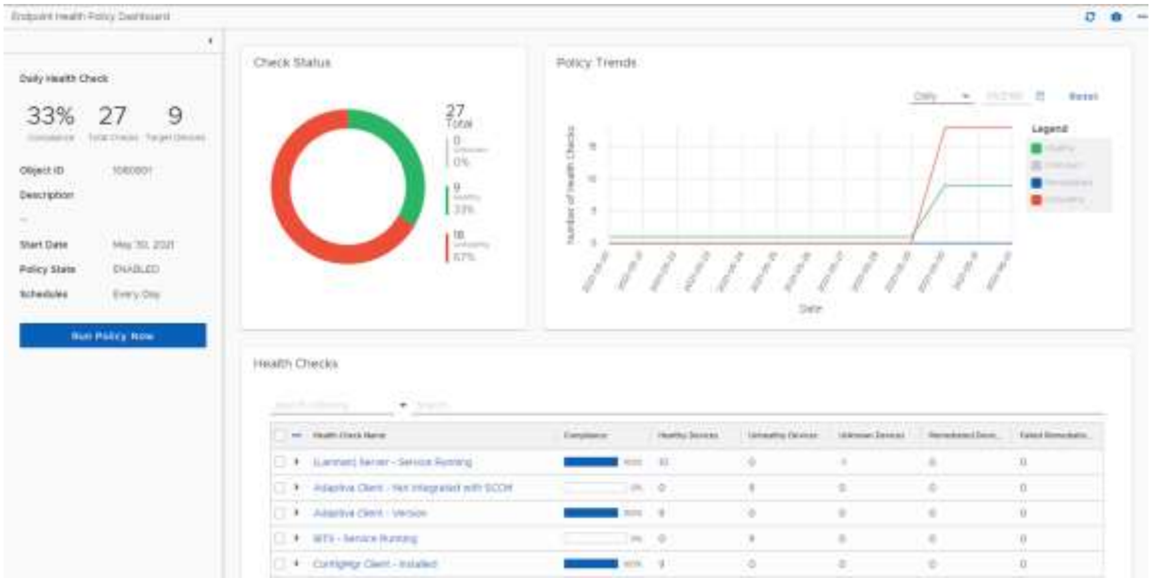
Server Workflows

Server Policy Created Workflow	Policy Created Workflow
Server Policy Updated Workflow	Policy Updated Workflow
Server Policy Enabled Workflow	Policy Enabled Workflow
Server Policy Disabled Workflow	Policy Disabled Workflow
Server Policy Deleted Workflow	Policy Deleted Workflow
Server Policy Status Workflow	Add Workflows

Client Workflows

Client Policy Assigned Workflow	Default Policy Assignment Client Workflow
Client Policy Enabled Workflow	Default Policy Enable Client Workflow
Client Policy Disabled Workflow	Default Policy Disable Client Workflow
Client Policy Deleted Workflow	Default Policy Delete Client Workflow
Client Policy Execution Workflow	Client Health Policy Execution-new

9. After every Health Check has been reviewed, click on **Save** or **Save & Run**. When Save & Run is selected the Dashboard Policy Results page will be displayed.

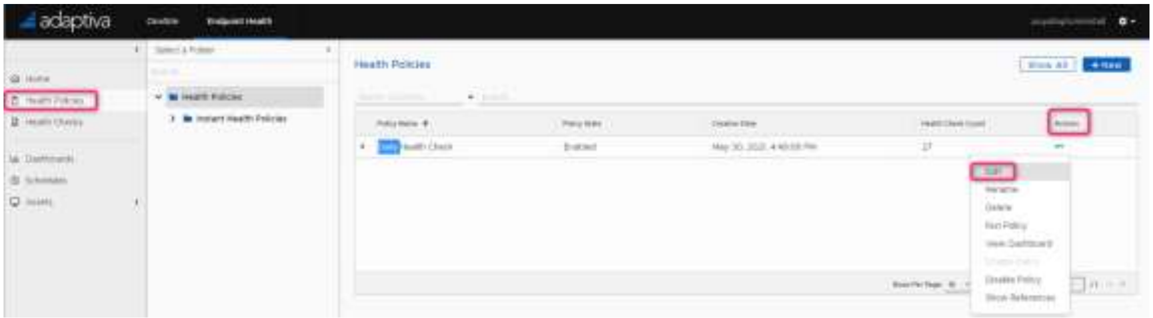


Changing a Health Policy

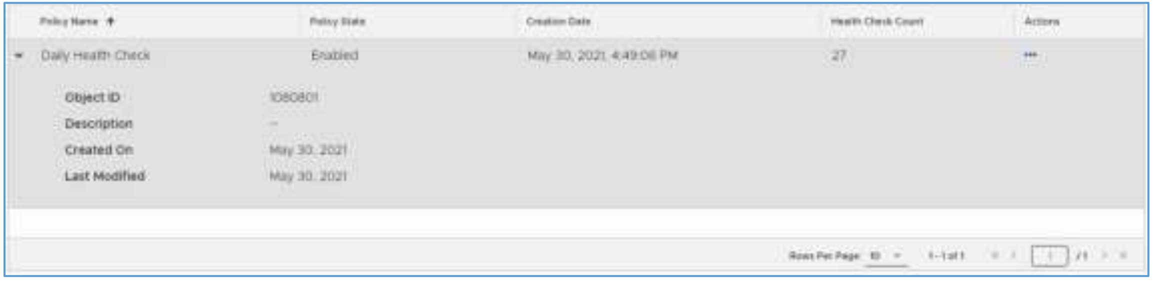
When a Scheduled or an Instant Health policy has been created use the following steps to make changes to the policy

Edit

1. From the Health Polices page, hover over the health policy. Click the ellipses (…) under the **Actions** menu and click on **Edit**



Use the **>** next to the Health Policy to display the Health Policy object ID and information as to when the policy was created and last modified. You can also see how many Health Checks have been added to this policy



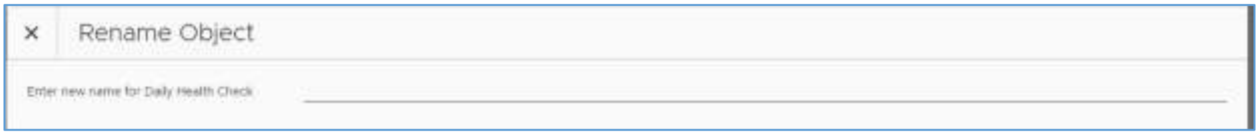
Policy Name	Policy State	Creation Date	Health Check Count	Actions
Daily Health Check	Enabled	May 30, 2021, 4:49:08 PM	27	•••

Object ID 1080801
Description --
Created On May 30, 2021
Last Modified May 30, 2021

2. Make the appropriate changes and select **Save** or **Save & Run**

Rename

This action will rename the Health Policy



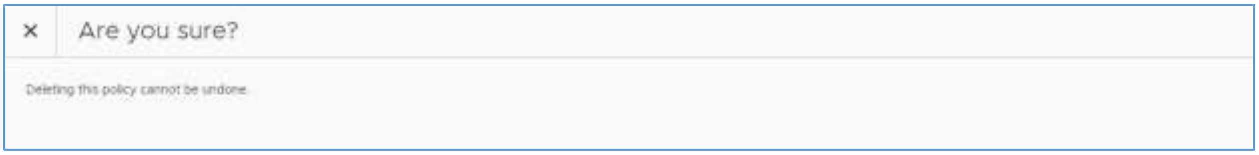
× Rename Object

Enter new name for Daily Health Check

Enter the new name and click **OK**

Delete

This action will delete the Health Policy



× Are you sure?

Deleting this policy cannot be undone.

Click **OK** to delete the policy

Enable / Disable Policy

This action will enable or disable the policy. When a policy is disabled, the policy will stop executing on the defined schedule. This action is immediate.

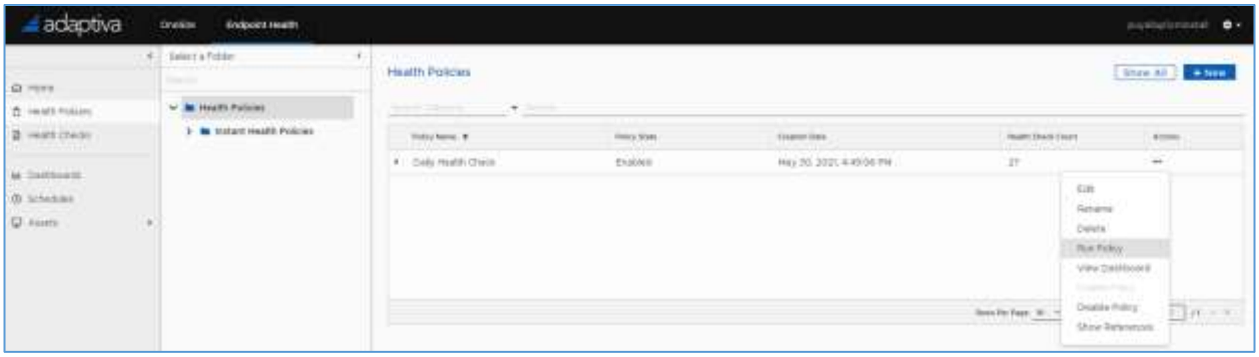
> ***NOTE: Any changes made to the policy even though it is disabled will be sent to the targeted devices***

Show References

This action shows the areas within Adaptiva where the Health Policy is referenced. Click **OK** to return to the list of Health Policies

Running the Policy

1. From the Health Polices page, hover over the health policy. Click the ellipses (…) under the **Actions** menu and click on **Run Policy**



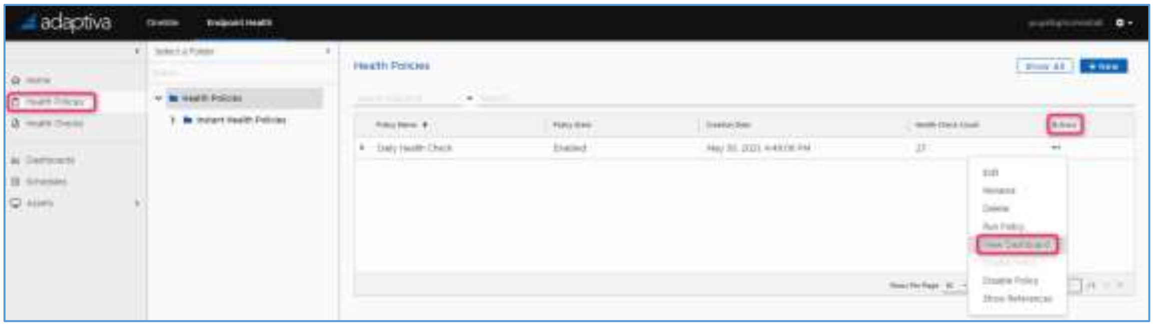
Health Policies

Policy Name	Policy State	Creation Date	Health Check Count	Actions
Daily Health Check	Enabled	May 20, 2021 4:49:06 PM	27	•••

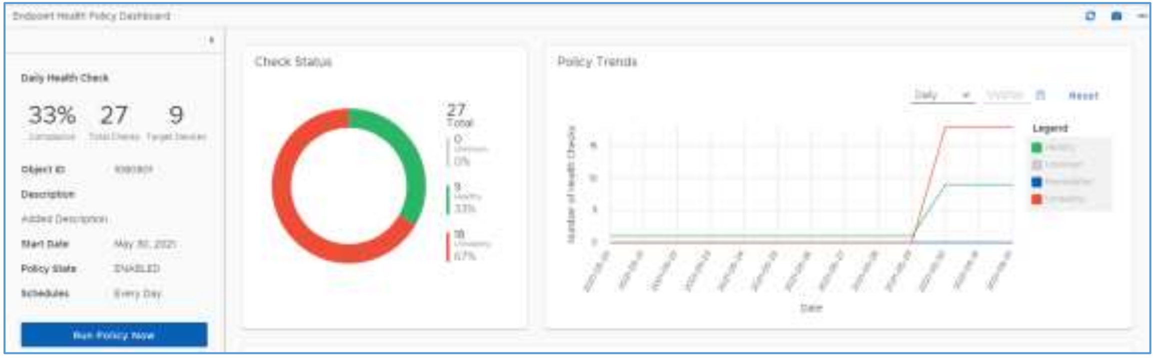
This will execute the policy on all targeted devices.

Viewing the Results

1. From the Health Polices page, hover over the health policy. Click the ellipses (…) under the **Actions** menu and click on **View Dashboard**



2. The dashboard will be displayed



Click on **Run Policy Now** to force re-execution of the Health Policy to the target devices

🔄 will refresh the results

••• will change the default refresh period. Default is 30 seconds

📷 will create a screen shot (in PNG format) of the results

> ***NOTE: This will only screen shot what is seen on the screen. If there are pages of Health Check results, only what is visible on the screen will be included in the screen shot.***

Endpoint Health Dashboards

SQL Server Reporting Services (SSRS) reports have been replaced with real-time dashboards.

The following table lists the Dashboards that can be used

1. In a web browser connect to the Adaptiva Web Portal (except Internet Explorer) – http://AdaptivaServerFQDN[:port]
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click **Go to Endpoint Health** or click **Endpoint Health** from the Solution list across the top
4. Select **Dashboards** from the Activity workspace on the left

Dashboard	Description
Endpoint Health	This is the Endpoint Health home page. This dashboard shows the overall summary of all scheduled health policies.
Endpoint Health Device Dashboard	This dashboard displays information about a specific device. Health trends, Blind Spots and lists all Health Checks targeted to the device
Endpoint Health Group Dashboard	This dashboard displays information from a specific group or collection of devices. Overall Device status, Group trends and compliance by device
Endpoint Health Location Dashboard	This dashboard displays information from a specific location. Overall Device status, Location trends and compliance by device
Endpoint Health Policy Dashboard	This dashboard displays information from a specific Health Policy. Overall Health Check status, Policy trends and compliance by Health Check
Endpoint Health Product Impact	This is also available from the Endpoint Health home page. This dashboard shows the total number of Health Check executions. It shows trends over time as well as the number of successful remediations. It will show the most remediated Health Checks as well as an estimate to number of hours saved if these health checks and remediation would have been completed manually.
Health Check Dashboard	This dashboard displays information about a specific Health Check. It provides trends for the health check, any blind spots (computers not targeted) and a list of targeted devices with check status
Health Overview	This dashboard displays summary info of all Health Checks

Integrating with ConfigMgr

Target Collections

Several health checks will create a ConfigMgr deployment to a target collection. These collections must be specified in the registry before using the Health Check.

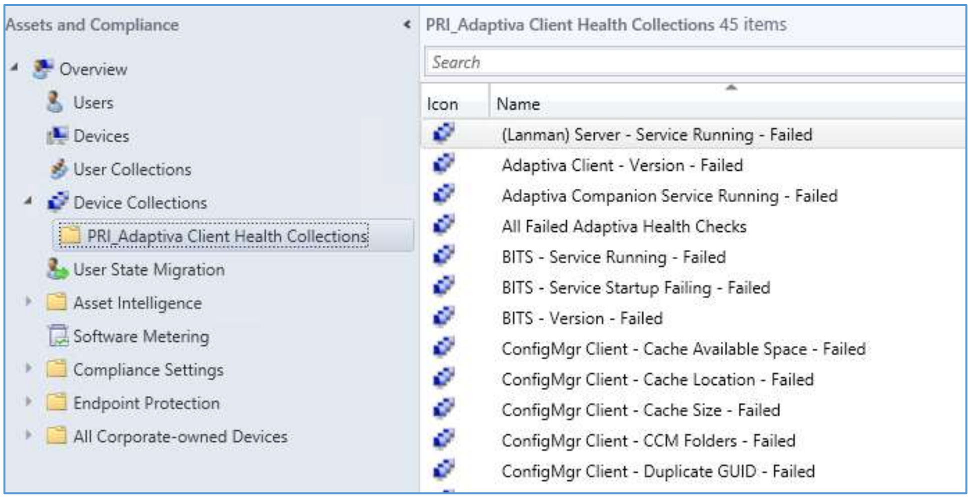
Before using the following Health Checks, modify the listed registry value and enter the collection id of the collection to be targeted for this Health Check

Health Check	Registry Modification required
ConfigMgr Client Status – Package Ping	chs.pkg_ping_sms_target_collection_id
ConfigMgr Client Status – Software Distribution	chs.softdist_ping_sms_package_id

Failed Health Check Collections

When Adaptiva OneSite is integrated with ConfigMgr, a client that fails a Health Check can be automatically added to a collection corresponding to that Health Check. This allows the administrator to easily evaluate and provide additional remediation or simply report on the failed devices.

The Failed Health Check Collections are viewable in ConfigMgr or in the Adaptiva Workbench in the SCCM Collections Explorer. The Health Check specific collections are located in a sub-folder named <sitecode>_Adaptiva Client Health Collections



(Lanman) Server - Service Running - Failed
Adaptiva Client - Version - Failed
Adaptiva Companion Service Running - Failed
All Failed Adaptiva Health Checks
BITS - Service Running - Failed
BITS - Service Startup Failing - Failed
BITS - Version - Failed
ConfigMgr Client - Cache Available Space - Failed
ConfigMgr Client - Cache Location - Failed
ConfigMgr Client - Cache Size - Failed
ConfigMgr Client - CCM Folders - Failed
ConfigMgr Client - Duplicate GUID - Failed

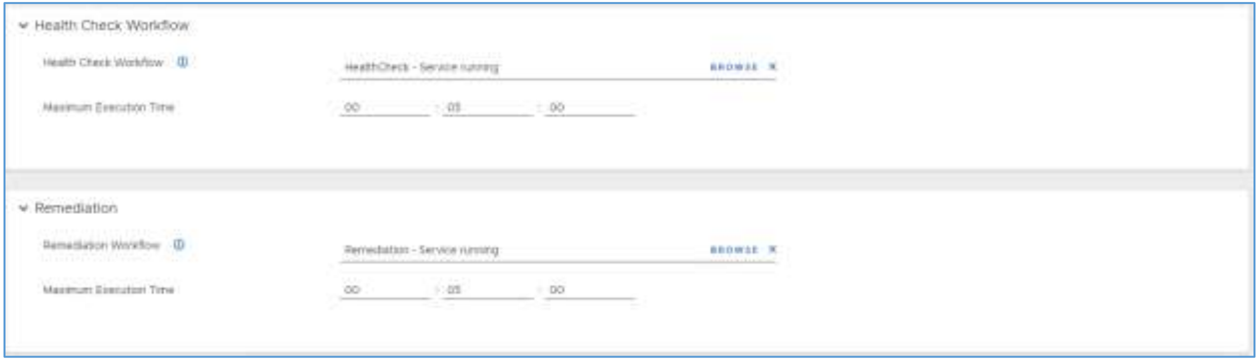
This is disabled by default. To enable these collections, do the following:

1. On the Adaptiva server, open Regedit.exe
2. Browse to HKLM\Software\Adaptiva\Server
3. Find the key: chs.turn_off_collection_updates and change the value to false
4. Restart the Adaptiva server service

Health Check Overview

A Health Check executes a defined workflow on a client and determines whether that client meets the defined criteria. If it fails to meet the criteria, a remediation workflow can be executed automatically. More information about Workflows is available in the **Workflows** section

There are two forms of workflows for Health Checks. The Health Check workflow determines whether or not the client is Healthy. The Remediation workflow attempts to repair an unhealthy client



Health Check Workflow

Health Check Workflow: HealthCheck - Service running

Maximum Execution Time: 00 : 05 : 00

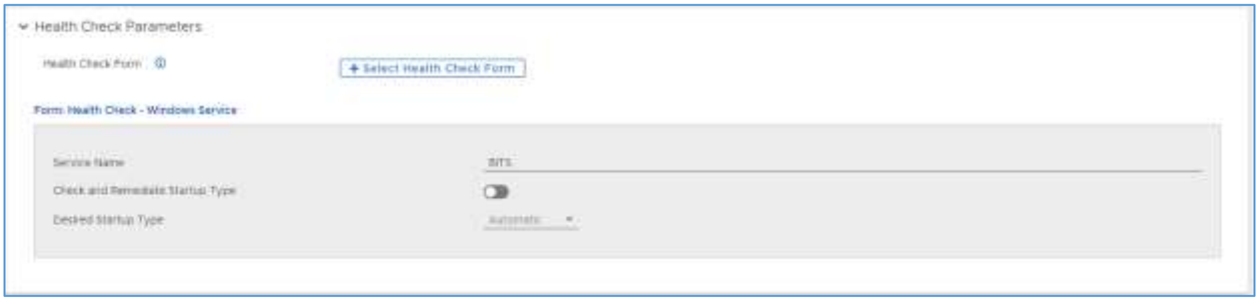
Remediation

Remediation Workflow: Remediation - Service running

Maximum Execution Time: 00 : 05 : 00

Parameters

Health Checks are executed as part of a scheduled Health Policy,. However, you may want to have some behavior of the health check change when it is run in different policies. For example, it might be important that all machines maintain a certain amount of disk space, but different offices have different requirements for the amount of disk space. It would be tedious to create a new Health Check for every different requirement. You would like to specify this in the policy. This functionality is provided by **Health Check Parameters**. Health Checks can accept input when they are added to a policy to define their behavior. It is also possible for the Health Check to contain default values, which are specified in the **Default Health Check Parameters Section**.



Health Check Parameters

Health Check Form

Form: Health Check - Windows Service

Service Name: BITS

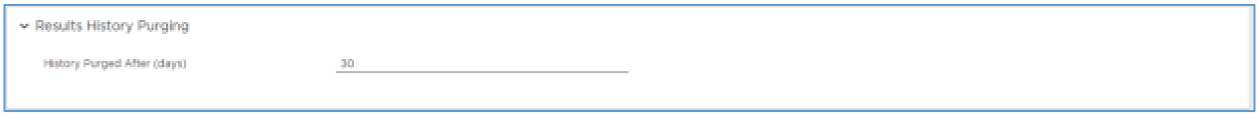
Check and Remediate Startup Type

Desired Startup Type: Automatic

In order to author a completely new Health Check from scratch, it is important to understand the purpose of a Health Check, as well as how to create Workflows and Forms/Screens.

History Purging

The most recent result of a health check execution on a client is always available. We also keep the history of health check execution, so that an administrator can view a particular client’s history. The administrator can specify how far back they would like to keep this history available before it is purged to clear space.



Results History Purging

History Purged After (days): 30

Workflows

NOTE: Creating, editing or viewing Workflows is not available in the Adaptiva Web Portal. The Adaptiva Workbench must be used

Workflows represent an execution of logic that is performed. A workflow is composed of a number of activities. These activities are the tools that the administrator can use to create health checks for their common IT scenarios. The Workflow Designer Perspective gives the administrator the ability to edit existing workflows or create their own.

Workflows are created and edited using the Workflow Designer Perspective. This perspective consists of the following views.

Workflow Explorer – allows the administrator to view existing workflows or create a new workflow.

Workflow Designer Palette – displays all activities which can be used in workflows. Activities can be dragged from the palette directly into the workflow.

Workflow Errors - the Workflow Errors View at the bottom of the workbench informs you of any problems with your workflow.

Workflow Designer Outline – Provides an overview of the workflow. This can be used to search for all used activities.

Workflow Designer Properties – Displays the properties associated with an activity.

Workflow Management Task Navigator – Allows the administrator to perform various tasks regarding workflows. This is hidden by default and is not needed for creating or modifying workflows.

Getting Started

Client Workflows – There are three types of workflows: **Client**, **Server** and **Business** Workflows. When creating Health Check and Remediation workflows, you should create a Client Workflow. Right-click **Workflows** -> **New Workflow** -> **Client**. Clicking the green plus will, by default create a Client Workflow.

Start1 Node – The start node contains a property **Workflow Name** which stores the name of the workflow.

End1 Node – The end node contains the result of the workflow. When the workflow terminates, the values held by the end node will be used to report success/failure, error description, error codes, etc. These fields can be set by any activity in the workflow using the **External node property setter** in the **Workflow Designer Properties View** while the activity is selected.

Use the **Workflow Designer Palette** to add various activities and flow to create the logic of the workflow.

Review the **Workflow Errors** to determine if there are any errors in the activities added.

Right-click on the white-space in the center pane and select **Save** to save the workflow. Select **Save and deploy** to save it and distribute the workflow policy to all clients. This does not execute the workflow; it makes the clients aware of the workflow, so they know to about if they are targeted to receive it. The workflow can also be deployed by right-clicking the workflow in the left pane and selecting **Deploy**.

When deploying a workflow, you will be prompted to define the **Execution Settings**. Here you can enable (or disable) Logging. Logs will be created on the client in the default path c:\program files (x86)\Adaptiva\AdaptivaClient\logs\WorkflowLogs. Workflow logs are automatically deleted after 5 hours.

Forms

Forms are groups of UI elements. The Workbench Form Designer allows for rapid creation of a custom UI. The administrator uses forms to create custom windows for entering Health Check Parameters. Many complex UI Components are available, but in most cases the administrator will only need the simplest UI elements like text boxes and buttons.

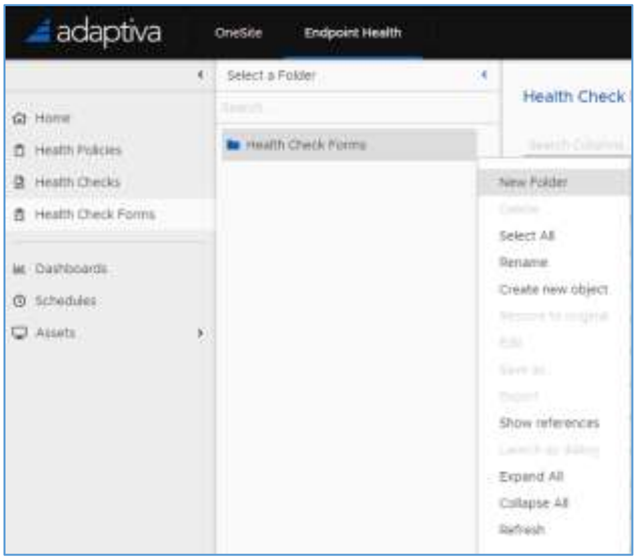
IMPORTANT: Forms should not be created in the Workbench when using Endpoint Health with release 8.1 or later.

NOTE: To create a form, users must be a member of the SuperAdmin role

Use the following instructions to create a custom form for use with your Health Check.

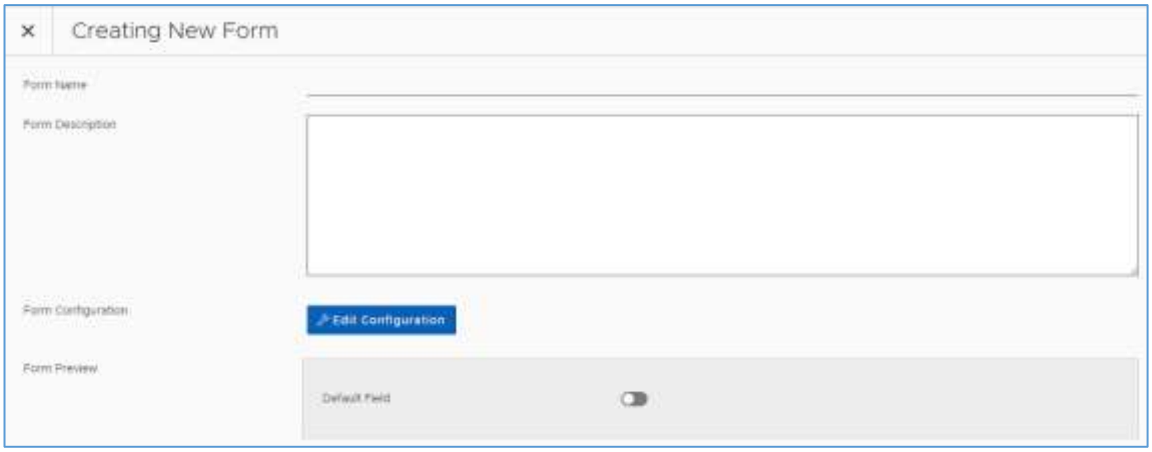
Scenario. We need a form to pass a text field to the workflow

1. In a web browser connect to the Adaptiva Web Portal (except Internet Explorer) – http://AdaptivaServerFQDN[:port]
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click **Go to Endpoint Health** or click **Endpoint Health** from the Solution list across the top
4. Select **Health Check Forms** from the Activity workspace on the left
5. The list of forms in the folder Health Check Forms is displayed.
6. In the Select a Folder pane, new folders can be created by clicking on the ellipses (…) next to the folder Health Check Folder



7. Select **New Folder** and enter the name: Custom Health Check Forms and click **Save**
8. Refresh the page (press F5) and select the Custom Health Checks Forms folder

9. Click on **+New** to create a new Form



Creating New Form

Form Name

Form Description

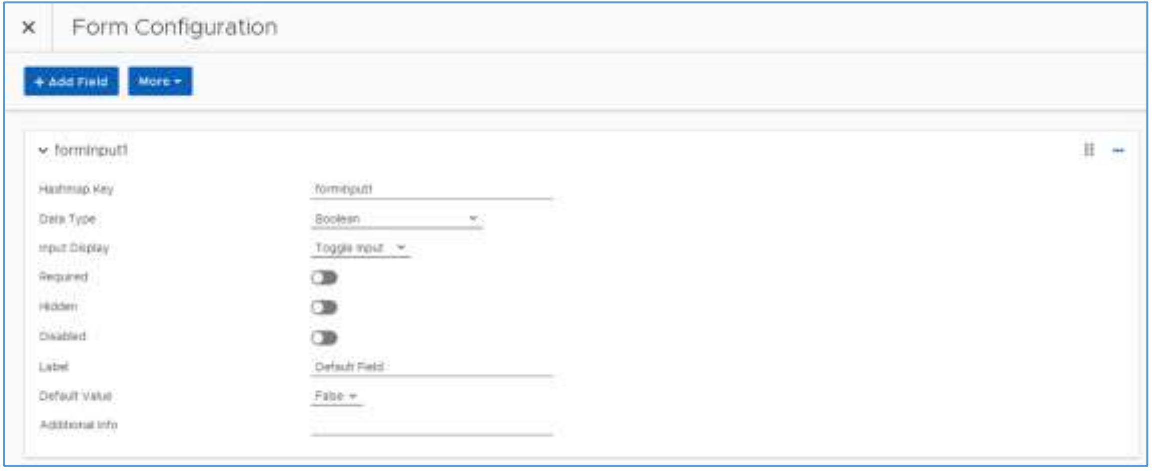
Form Configuration

Form Preview

Default Field

Form Name: Enter a descriptive Form Name
Form Description: Enter a description of the form
Form Configuration: This button will allow you to add fields to the form
Form Preview: This will preview how the form will look on the Health Check and Health Policy pages

10. Enter a Name and click on **Edit Configuration**



Form Configuration

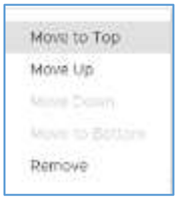
forminput1

Hashmap Key: forminput1
Data Type: Boolean
Input Display: Toggle Input
Required
Hidden
Disabled
Label: Default Field
Default Value: False
Additional Info

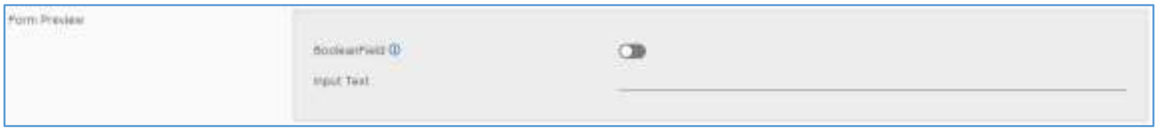
Hashmap Key: Enter the field name. This will be used to reference the input in the workflow. Do not use spaces
Data Type: Select the type of data that is to be entered: Boolean (on / off), Text, Whole Number, Fractional number (decimal value), Datetime, or a list (array) of each of the data types.
Input Display: This will change depending on the Data Type selected. For example, if a Data Type of Boolean is selected, Input Display can be Toggle Input, Checkbox, Radio Buttons or Dropdown. These allow you to change the look and how data is entered on the form.
Required: Denotes this field is required and must be entered
Hidden: Hides the field on the form
Disabled: Field is visible on the form, but cannot be changed
Label: This is the text label to preface the input field with
Default Value: The default value to display when the form is opened
Additional Info:

11. If there are more fields to add to the form, click **+Add Field**, otherwise click **OK**
Additional fields will be listed in order

12. Use the ⠿ to change the order of the fields using drag and drop or use the ellipsis menu and select one of the choices there.



13. When finished creating all of the fields, click OK
14. The fields will now be shown in the Form Preview field



15. Click Save to save the form
16. This form can now be used in your Health Check

Schedules

Schedules are used to automate the execution of Content Push policies, Business/Server workflows or update custom groups. The following default schedules have been created for you to use.

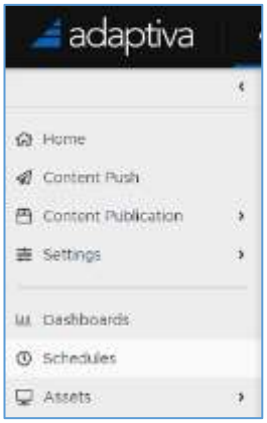
ASAP
Daily AT 2AM
Every 12 Hours
Every 15 Minutes
Every Day
Every Hour
Every Month
Every Sunday At 1 AM
Every Week
Last Saturday Of Every Month

If you want to create your own Schedule, follow the steps below

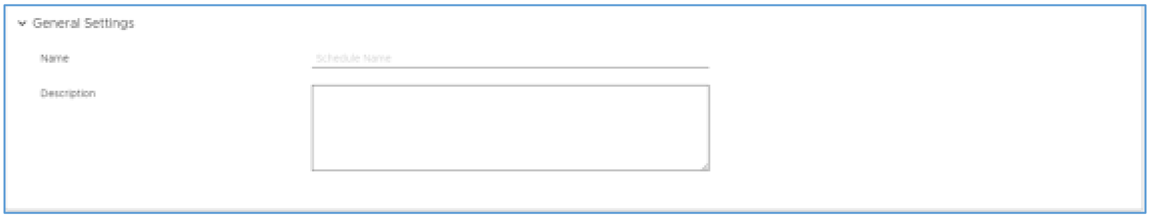
Creating a Custom Schedule

Using the Adaptiva Web Portal

1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – http://AdaptivaServerFQDN[:port]
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Schedules**

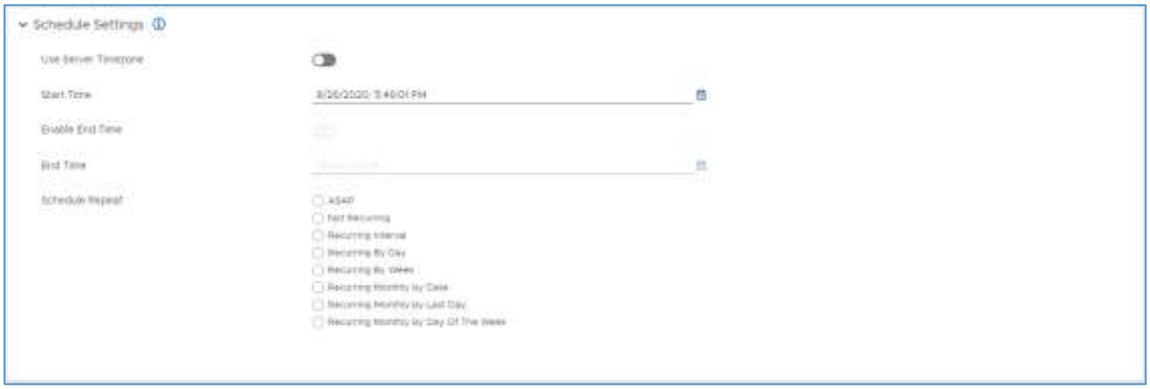


4. To create a new schedule, click on **+New**
   General Settings



Name – Enter a descriptive name for the new schedule
Description – Enter a description

Schedule Settings



Schedule Settings

Use Server Timezone

Start Time 8/26/2020 5:40:01 PM

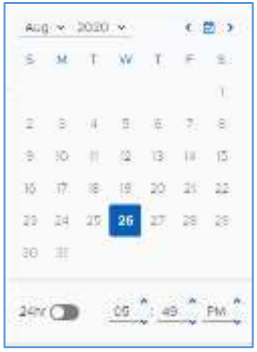
Enable End Time

End Time

Schedule Repeat

○ ASAP
○ Not Recurring
○ Recurring Interval
○ Recurring By Day
○ Recurring By Week
○ Recurring Monthly by Date
○ Recurring Monthly by Last Day
○ Recurring Monthly by Day Of The Week

Use Server TimeZone – Toggle this button to the right to use the time zone of the Adaptiva server
Start/End Time – The Start and optional End of the schedule
Enable End Time – Check this box, if available, to end the schedule on this date
Select the month, day and time using calendar control



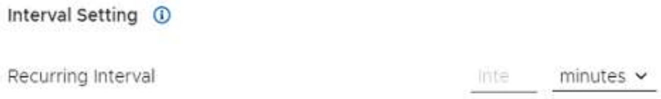
Aug 2020

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

24hr 05 : 49 PM

Schedule Repeat – Select a Schedule Repeat type. Each of these will display additional options

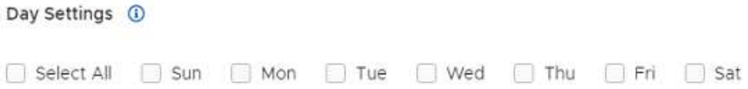
ASAP – You will not be able to select a Start or End Time
Non Recurring – You will not be able to select an End Time
Recurring Interval – Enter the specific interval in days, hours or minutes



Interval Setting

Recurring Interval Inte minutes

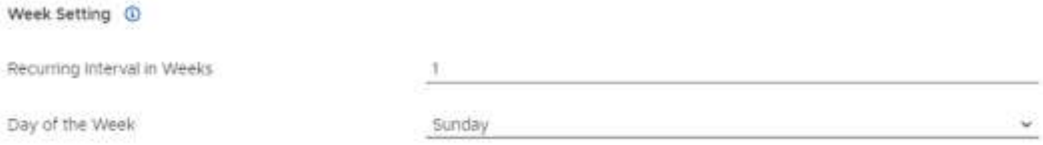
Recurring By Day – Check the day of the week



Day Settings

□ Select All □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Recurring By Week – Enter the Weekly interval for a specific day of the week

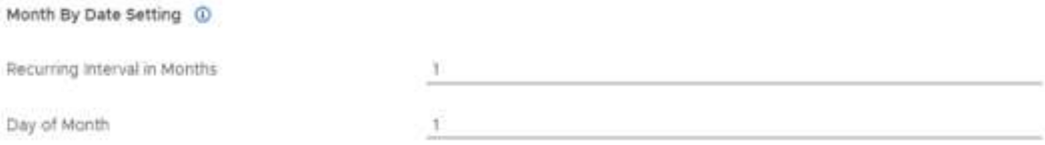


Week Setting

Recurring Interval in Weeks 1

Day of the Week Sunday

Recurring Monthly By Date – Enter the Month interval for a specific day of the month

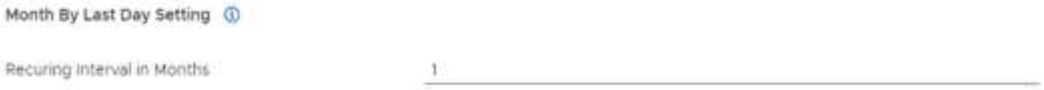


Month By Date Setting

Recurring Interval in Months 1

Day of Month 1

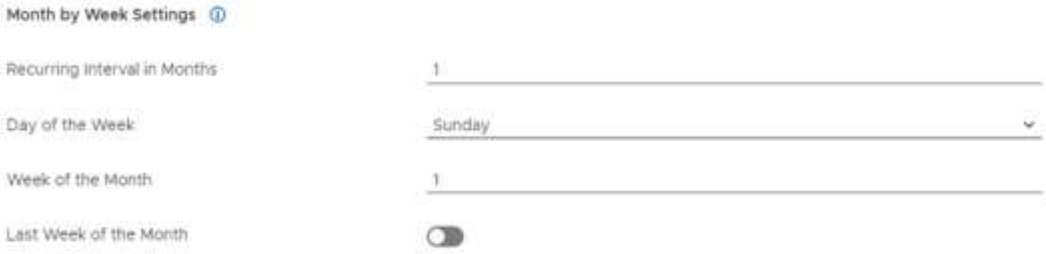
Recurring Monthly By Last Day – Enter the Month interval



Month By Last Day Setting ⓘ

Recuring Interval in Months: 1

Recurring Monthly By Day Of The Week – Enter the Month interval for a specific day and week of the month. Toggle the button **Last week of the month** to run the schedule on a specific day of the week on the last week of the month.



Month by Week Settings ⓘ

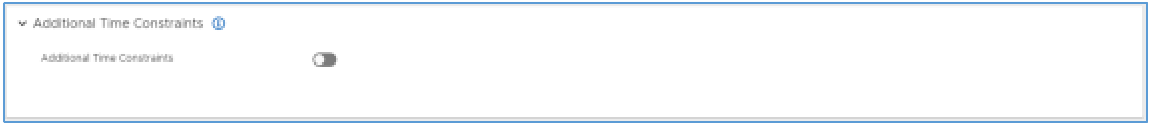
Recurring Interval in Months: 1

Day of the Week: Sunday

Week of the Month: 1

Last Week of the Month: ○

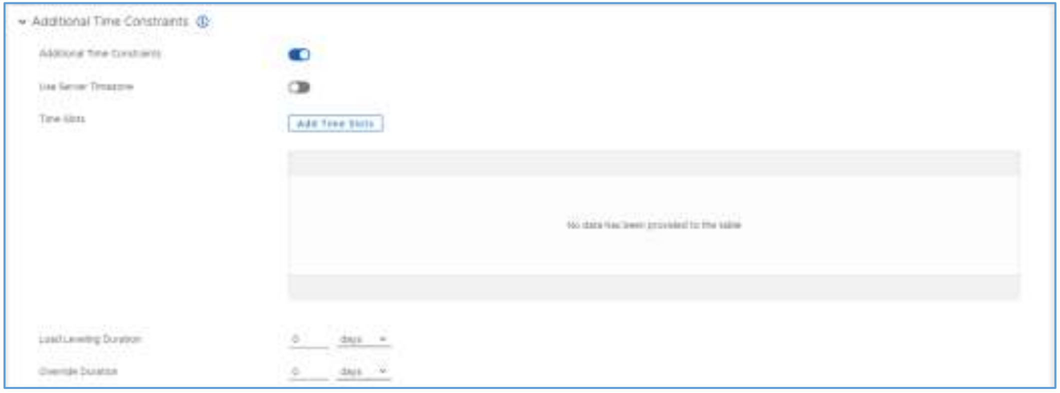
Additional Time Constraints – Create additional constraints for this schedule, including load leveling



Additional Time Constraints ⓘ

Additional Time Constraints: ○

This is disabled (slid to left) by default. Click on the button to enable



Additional Time Constraints ⓘ

Additional Time Constraints: ●

Use Server Timezone: ○

Time Slots: Add Time Slots

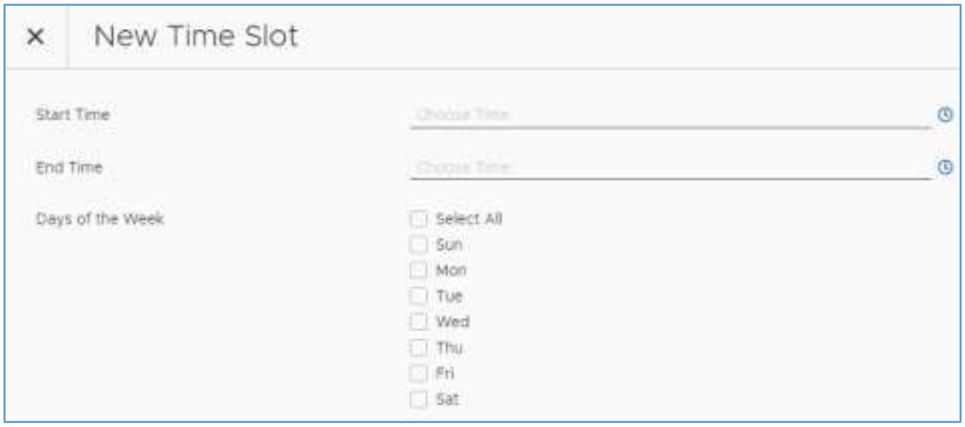
No data has been provided to the table

Load Leveling Duration: 0 days

Override Duration: 0 days

Use Server Timezone: Disabled by default. When enabled, the schedule will run based on the time on the Adaptiva Server.

Time Slots: Click on **Add Time Slots** to create a time slot when this schedule is allowed to run.



× New Time Slot

Start Time: Choose Time

End Time: Choose Time

Days of the Week:
- □ Select All
- □ Sun
- □ Mon
- □ Tue
- □ Wed
- □ Thu
- □ Fri
- □ Sat

Start/End Time: The Start and End time of the constraint time slot. Click on **24 hour** to select the time using the 24 hour clock

Select the **Days of the Week**

Click **OK**

Load Leveling Duration: Select the Load level duration in days, hours, or minutes. The target list of devices will be balanced across the time interval

Override Duration: Select the Override duration in days, hours, or minutes. Schedules will run ASAP after the override duration

5. Click **Save**

List of Health Checks

The following section lists the health checks that are provided. For a table of remediation details for various checks, see section: **Appendix A: Health Check Remediation Details.**

Account Checks

Health Check	Description	Supports Remediation
User Account – Running Service	Verifies that a specific user account is running a specific service on the device	Yes

Adaptiva Client Checks

Health Check	Description	Supports Remediation
Adaptiva Client – Not Integrated with SCCM	Verifies that the Adaptiva Client is successfully integrated with the Configuration Manager client.	Yes
Adaptiva Client - Version	Verifies whether Adaptiva client version is equal to desired Adaptiva client version	No

Background Intelligent Transfer Service (BITS) Health Checks

Health Check	Description	Supports Remediation
BITS – Service Running	Checks and Remediates: The BITS service is running, and its start mode is set to desired type	Yes
BITS – Service Startup Failing	Checks and Remediates: Detects whether BITS startup is failing (it might be possible that BITS has become corrupted)	Yes
BITS - Version	Checks and Remediates: Ensure SCCM Clients have a recent version of BITS	Yes

ConfigMgr Client Configuration Checks

Health Check	Description	Supports Remediation
ConfigMgr Client - Cache Available Space	Checks and Remediates: The specified amount of space is available in the client cache	Yes
ConfigMgr Client - Cache Location	Checks and Remediates: The client cache location is correctly set	Yes
ConfigMgr Client - Site Assignment	Checks and Remediates: The client is assigned to the specified site	Yes

ConfigMgr Client - Site Auto Discovery	Verifies: Site auto discovery is working on the client	No

ConfigMgr Client Health Checks

Health Check	Description	Supports Remediation
ConfigMgr Client – Cache Size	Checks and Remediates: The client cache size is set to desired value, or more	Yes
ConfigMgr Client – CCM Folders	Checks and Remediates: There is no file named CCM in the Windows system32 folder, and there is no file named CCMSETUP in the Windows system32 folder	Yes
ConfigMgr Client - Download Provider	Verifies whether the specified download provider is present in the CCM_DownloadProvider class in WMI	No
ConfigMgr Client – Duplicate GUID	Verifies: The client does not have a duplicate SMS GUID	No
ConfigMgr Client – Installed	Checks and Remediates: The SCCM client agent is installed	Yes
ConfigMgr Client – Management Point Location	Verifies: The client can correctly determine the location of the management point	No
ConfigMgr Client - Orphaned Cache Folders	Verifies whether there are any folders in the ccmcache that the ConfigMgr client is not aware of. Remediation removes any that exist.	Yes
ConfigMgr Client – Provisioning Mode	Checks and Remediates: Cases where the Task Sequence Manager leaves software distribution disabled even after it has exited	Yes
ConfigMgr Client – Service Running	Checks and Remediates: The SCCM client agent service is running, and its start mode is set to automatic	Yes
ConfigMgr Client - Version	Checks and Remediates: The specified version or later of SCCM agent is installed	Yes

ConfigMgr Client Installation Checks

Health Check	Description	Supports Remediation
CCMSetup – DiscoveryStatus MOF	Checks and Remediates: If the event logs contain entries indicating CCMSetup failed due to a DiscoveryStatus MOF compile issue; compiles the MOF automatically if so	Yes
CCMSetup – StatusAgentProxy DLL	Detects if the event logs contain entries indicating CCMSetup failed due to a StatusAgentProxy DLL issue	No

CCMSetup – Visual C++ DLL	Checks and Remediates: If the size of the Visual C++ DLL is incorrect, the correct DLL is copied from the specified path	Yes

ConfigMgr Client Status Checks

Health Check	Description	Supports Remediation
ConfigMgr Client Status – Hardware Inventory	Checks and Remediates: whether hardware inventory is working	Yes
ConfigMgr Client Status – Heartbeat Discovery	Checks and Remediates: whether heartbeat discovery is working	Yes
ConfigMgr Client Status – Management Point Ping	Checks and Remediates: The management point location can be detected, and management point can be pinged using ICMP echo	No
ConfigMgr Client Status – Package Ping	Checks and Remediates: whether package download is working or not	Yes
ConfigMgr Client Status – Policy Retrieval	Checks and Remediates: a recently updated policy can be downloaded successfully by the client	Yes
ConfigMgr Client Status – Software Distribution	Checks and Remediates: whether software distribution is working or not	Yes
ConfigMgr Client Status – Software Inventory	Checks and Remediates: whether software inventory is working or not	Yes
ConfigMgr Client Status – Status Message Submission	Checks and Remediates: whether status messages are being reported	Yes

Data Execution Prevention Checks

Health Check	Description	Supports Remediation
DEP - Policy	Verifies that the Data Execution Prevention Policy is set to a specific setting.	Yes

DCOM Checks

Health Check	Description	Supports Remediation
DCOM – Remote Connection Enabled	Checks and Remediates: Whether remote connection is enabled or not	Yes

Instant Inventory Checks

Health Check	Description	Supports Remediation

Instant Inventory - Disk Space	Returns any machines that have below the specified amount of available disk space	No
Instant Inventory - File Contains Text	Returns any machines that have the specified text in a specified file	No
Instant Inventory – File Exists	Returns any machines that have a specified file	No
Instant Inventory – Folder Exists	Returns any machines that have a specified folder	No
Instant Inventory – Process Running	Returns any machines that have a specified process running	No
Instant Inventory – Service Started	Returns any machines that have a specified service that is in the started state	No
Instant Inventory – Service Stopped	Returns any machines that have a specified service that is in the stopped state	No

IP Address Scope Checks

Health Check	Description	Supports Remediation
IP – Permitted Scope	Verifies: Client's IP address is within the specified permitted IP address scopes	No
IP – Prohibited Scope	Verifies: Client's IP address is not within the specified prohibited IP address scopes	No

Network Checks

Health Check	Description	Supports Remediation
(Lanman) Server - Service Running	Verifies: The lanmanserver service is running, and its start mode is set to automatic	Yes
Network - DNS Name Resolution	Verifies whether the local hostname resolves to the correct IP address in DNS. Remediation registers the current IP in DNS.	Yes
Network – DNS Settings	Checks and Remediates: If the Primary DNS suffix, Sync Domain with Membership, the Primary DNS Domain, the NIC DNS Domain and Enable Dynamic DNS Registration settings are set correctly; sets to the desired state if incorrect	Yes
Network – Hosts file entries present	Checks and Remediates: If the hosts file contains the specified entries; if any specified hosts entry is not present, it is appended	Yes

Operating System (OS) Health Checks

Health Check	Description	Supports Remediation
OS – Admin Share Available	Checks and Remediates: The admin$ share is published on the client	Yes

OS – Clear Windows print queues	Clears the Windows printer queues	Yes
OS – Computer Naming Convention	Detects whether the computer naming convention matches the specified regular expression	No
OS – Delete Temp Folder Contents	Deletes all content from Temp folders	No
OS – File Associations	Checks and Remediates: That a list of file extensions is present and match. Corrects any that are incorrect and adds any that are missing	Yes
OS - Group Policy Processing Errors	Verifies whether any errors are shown within the specified number of days when attempting to process Group Policy.	No
OS – Logon Server Correct	Detects whether the current Logon Server matches the desired name	No
OS – Remote Desktop Settings	Checks and Remediates: Remote Desktop, Remote Assistance and Secure connection (Network Level Authentication) and sets if any are incorrect	Yes
OS – Run Key Entries	Checks and Remediates: Both the x86 and x64 Run Key entries are in an allowed list; removes any that are not	Yes
OS – Screen Saver Settings	Checks and Remediates: For each user, whether the screen saver is configured, whether it is set to password protected, the timeout and the path; if any are incorrect, they are corrected	Yes
OS – Security Group Presence	Checks and Remediates: Local group membership for a specified local group to ensure that a specified member exists; if it does not exist, it is added	Yes
OS - Version	Verifies that the client operating system version is one of the specified versions.	No
OS – Windows Explorer Settings	Checks and Remediates: The following - Show Hidden Files, Show Protected System Files, Hide File Extensions for Known File Types, Compressed Files in a different color, Show Run on Start Menu, Hide Empty Drives; corrects any that are incorrect	Yes
OS – Windows Licensing Compliance	Detects the current Windows licensing state	No
Remote Registry Service Running (OS Specific)	Checks and Remediates: The Remote Registry service is running based on operating system, and its start mode is set to desired type	Yes

PowerShell Health Checks

Health Check	Description	Supports Remediation

PowerShell – Set PowerShell Execution Policy	Checks and Remediates: The PowerShell execution policy. Choose between Restricted, All Signed, Remote Signed, Unrestricted, Bypass or Undefined Sets to the desired state if incorrect	Yes
PowerShell - WinRM	Checks and Remediates: That WinRM is enabled or disabled on the machine. If in an incorrect state, changes it accordingly	Yes

SCCM Miscellaneous Checks

Health Check	Description	Supports Remediation
SCCM – Client Actions must be Present	Verifies specific client actions are present.	Yes

Security Health Checks

Health Check	Description	Supports Remediation
Security - Bad Rabbit Immunisation	Verifies whether a system has already been infected by the Bad Rabbit ransomware. Remediation removes the infection and immunizes against future attack.	Yes
Security – BitLocker Drive Encryption	Checks and Remediates: If BitLocker drive encryption is enabled for either the OS Drive, All Drives or a Specific drive; enables if it is not already enabled (encrypts)	Yes
Security – Secure Boot	Detects whether Secure Boot is enabled or disabled in the BIOS/UEFI	No
Security – User Access Control (UAC) Enabled	Checks and Remediates: If UAC is enabled; performed only on Windows operating systems	Yes
Security – User Local Admin	Detects whether the currently logged on user is a local administrator	No
Security - WannaCry Infection Detection	Verifies whether systems have already been infected by WannaCry by conducting a comprehensive evaluation of Indicators of Compromise (IOC) for this exploit. Machines that fail this health check are already compromised and must be immediately quarantined. The business must then evaluate whether to reimage the affected systems or pay the ransom to retrieve data.	No
Security - WannaCry Vulnerability Assessment	Verifies whether systems are vulnerable to the WannaCry attack by evaluating whether the correct patches and system updates have been applied to the system. If a machine contains none of the specified patches, it is	Yes

	vulnerable to attack by WannaCry. The patch list can be easily updated by system administrators through a simple command line user interface to add additional patches to the health check as they become available.	

Software Health Checks

Health Check	Description	Supports Remediation
Software – Illegal Software Installed	Detects whether any software specified in a named list of either software titles or software GUIDs is installed	No
Software – Internet Explorer Home Page	Checks and Remediates: Whether the Internet Explorer home page is set correctly, and if not sets it	Yes

System Performance Health Checks

Health Check	Description	Supports Remediation
System – Defrag Drive	Runs the disk defragmentation tool to reorganize and optimize the disk	No
System - Disk Cleanup	Verifies whether the device is under a specified percentage of free disk space. Remediation will run the disk cleanup utility with the specified cleanup options to safely reclaim space.	Yes
System – Free Disk Space	Verifies: The % free space on disk drives	No
System - Reboot Required	Verifies whether a reboot is required for up to four primary reboot reasons (Windows Update Installation, Windows Component Installation, File Rename Operations, SCCM Reboot Pending)	No
System - Run Check Disk	Schedules a ChkDsk to run on the next reboot	No
System – Trigger System Restore	Triggers a System Restore task so systems can be restored to a specific point in time	No
System – Uptime	Verifies whether a system has been online longer than the specified number of days	No

System Settings Checks

Health Check	Description	Supports Remediation
System – Registry Setting must Exist	Verifies that a specific registry setting exists or is set to a specific value.	Yes
Unquoted Service Binary Path	Scans for services that have spaces in their binary path, but which are not surrounded by	Yes

	double quotes. Remediates any that are found.	

Tanium Health Checks

Health Check	Description	Supports Remediation
Tanium – Verify Client Settings	Verifies that Tanium Client settings are set to a desired state.	Yes

Windows 10 Health Checks

Health Check	Description	Supports Remediation
Windows 10 - Credential Guard Active	Verifies that Credential Guard is enabled and active on the machine. If Credential Guard is not enabled, remediation will enable it	Yes
Windows 10 - Device Guard & Credential Guard Active	Verifies that both Device Guard and Credential Guard are enabled and active on the machine. If Device Guard and Credential Guard are not enabled, remediation will enable them	Yes
Windows 10 - Device Guard & Credential Guard Capable	Verifies that the device has all prerequisites and is capable of supporting both Device Guard and Credential Guard	No
Windows 10 - Device Guard HVCI Active	Verifies that Device Guard/HVCI is enabled and active on the machine. If Device Guard is not enabled remediation will enable it	Yes
Windows 10 - DG-CG - DMA Protection	Verifies that Direct Memory Access Protection is available. This advanced security feature is desirable for Device Guard/Credential Guard security	No
Windows 10 - DG-CG - NX Protection	Verifies that No-Execute (NX) Protection is available. This advanced security feature is desirable for Device Guard/Credential Guard security	No
Windows 10 - DG-CG - OS Architecture	Verifies that the Operating System is 64-bit. 64-bit virtualization is required for Device Guard/Credential Guard	No
Windows 10 - DG-CG - OS SKU	Verifies that the Operating System is a valid SKU. Supported SKUs for Device Guard/Credential Guard include Enterprise, Server, Education and IoT	No
Windows 10 - DG-CG - Secure Boot State	Verifies that Secure Boot is enabled on the device. Secure Boot is a requirement for Device Guard/Credential Guard	No
Windows 10 - DG-CG - Secure MOR	Verifies that Secure Memory Overwrite Request (MOR) Protection is available. This	No

	advanced security feature is desirable for Device Guard/Credential Guard security	
Windows 10 - DG-CG - SLAT Supported CPU	Verifies that the installed CPU supports the Second-level address translation feature desirable for Device Guard/Credential Guard	No
Windows 10 - DG-CG - SMM Protection	Verifies that System Management Mode (SMM) Protection is available. This advanced security feature is desirable for Device Guard/Credential Guard security	No
Windows 10 - DG-CG - TPM Version	Verifies that the system has a valid TPM and that it is at least version 2.0. Version 2.0 of the TPM is desirable for Device Guard/Credential Guard	No
Windows 10 - DG-CG - Virtualization Firmware	Verifies that virtualization firmware is present and available. This includes Intel Virtualization Technology, Intel VT-x, AMD-V, Virtualization Extensions or similar. Virtualization firmware is a requirement for Device Guard/Credential Guard	No
Windows 10 - DG-CG - Win10 Build Version	Verifies that the version of Windows 10 running is Redstone X or higher. Additional security options were made available after build 10586 (release 1511) that are desirable for Device Guard/Credential Guard	No
Windows 10 - Last OS Install Date-Time	Verifies that the last time the device had an OS install/reinstall was more than X days ago. This can ensure that end-users that have just been disrupted for an install are prioritized last for another install	No
Windows 10 - Microsoft Edge Version	Verifies that the installed version of Microsoft Edge meets requirements	No
Windows 10 - Minimum Hardware Requirements	Verifies that the device has the minimum required hardware specification for supporting Windows 10. Defaults are set to Microsoft hardware recommendations but can be adjusted at design time or runtime to reflect specific business requirements for upgrade	No
Windows 10 - Unified Extensible Firmware Interface (UEFI)	Verifies that the device is running the Unified Extensible Firmware Interface (UEFI) required for Secure Boot and Device Guard/Credential Guard. These security features are not supported on legacy BIOS	No

Windows Update Agent Health Checks

Health Check	Description	Supports Remediation
Windows Update - Auto Update GPO	Verifies whether the group policy settings for Windows Update configuration are set correctly.	No
Windows Update - Last Scan Cycle	Verifies whether the machine last ran the software update scan cycle within the specified number of days.	Yes
Windows Update - Metadata Version	Verifies whether the software update metadata version on the client matches the current metadata version on the server	Yes
Windows Update - Non-Compliant Assignments	Verifies whether there are any ConfigMgr software update deployments that contain updates in a non-compliant state	No
Windows Update - Software Update Scan Errors	Verifies whether any errors have been reported by the Software update scan agent and reports back up to the last 10 errors	No
WUA – Service Missing	Checks and Remediates: Whether WSUS service is present on the machine or not	Yes
WUA – Service Running	Checks and Remediates: The wuauserv service is running, and its start mode is set to desired type	Yes
WUA - Version	Checks and Remediates: The WSUS client version is current	Yes

WMI Health Checks

Health Check	Description	Supports Remediation
WMI – ConfigMgr Client Namespaces	Checks and Remediates: Connectivity to WMI namespaces used by the SCCM client	Yes
WMI – ExecMgr Connection Error	Checks and Remediates: Detects whether the SCCM client's execmgr log contains WMI connection errors	Yes
WMI – In Path	Checks and Remediates: The system32\wbem folder is included in the path variable in the environment	Yes
WMI – Repository Integrity	Checks and Remediates: The integrity of the WMI repository	Yes
WMI – Service Running	Checks and Remediates: The WinMgmt service is running, and its start mode is set to desired type	Yes

Appendix A: Health Check Remediation Details

Account Checks

Health Check	Remediation Details
User Account – Running Service	Checks a specific user account is running a specific service on the device. Stops or Stops and Disables the service if not set correctly

Adaptiva Client Checks

Health Check	Remediation Details
Adaptiva Client – Not Integrated with SCCM	Configures integration with ConfigMgr.

Background Intelligent Transfer Service (BITS) Health Checks

Health Check	Remediation Details
BITS – Service Running	Start BITS service and set its start mode to automatic.
BITS – Service Startup Failing	Removes BITS DAT files from %ALLUSERSPROFILE%\ Microsoft\Network\Downloader folder.
BITS - Version	A UNC path must be provided to the BITS installation executable. A command line execute activity installs BITS, waits until the execution is complete, and determines success or failure based on the return value from the executable.

ConfigMgr Client Configuration Checks

Health Check	Remediation Details
ConfigMgr Client - Cache Available Space	Non-qualified cache elements are deleted sequentially until available space requirements are met. After deleting all elements, if the requirement is not met, Cache size is increased by the required number of bytes.
ConfigMgr Client - Cache Location	Sets the cache location to the specified path.
ConfigMgr Client - Site Assignment	If configured to perform auto site discovery, then perform auto site discovery. If a specific site is specified, the client will be assigned to the specified site.

ConfigMgr Client Health Checks

Health Check	Remediation Details

ConfigMgr Client – Cache Size	Sets the cache size to the specified value.
ConfigMgr Client – CCM Folders	Deletes the folders named ccm and ccmsetup.
ConfigMgr Client – Installed	Installs the ConfigMgr client directly using command line or by generating CCR on the site server for the client machine.
ConfigMgr Client - Orphaned Cache Folders	Deletes any orphaned folders in the ccmcache.
ConfigMgr Client – Provisioning Mode	Resets the paused registry value to 0 in [HKLM\Software\Microsoft\SMS\Mobile Client\Software Distribution\State] and restarts the SMS Agent Host Service if TSManager is not running.
ConfigMgr Client – Service Running	Starts the SMS Agent Host service and sets its start mode to automatic.
ConfigMgr Client - Version	Installs the ConfigMgr client directly using command line or by generating CCR on the site server for the client machine.

ConfigMgr Client Installation Checks

Health Check	Remediation Details
CCMSetup – DiscoveryStatus MOF	The following command is executed: MofComp.exe %SystemDrive%\Program Files\Microsoft Policy Platform\ExtendedStatus.mof.
CCMSetup – Visual C++ msvcr100 dll	If incorrect version of msvcr100.dll is detected, the correct version will be copied from the defined UNC path.

ConfigMgr Client Status Checks

Health Check	Remediation Details
ConfigMgr Client Status – Hardware Inventory	Executes a full policy reset or re-installs the ConfigMgr Client if the option is selected.
ConfigMgr Client Status – Heartbeat Discovery	Executes a full policy reset or re-installs the ConfigMgr Client if the option is selected.
ConfigMgr Client Status – Package Ping	Executes a full policy reset or re-installs the ConfigMgr Client if the option is selected.
ConfigMgr Client Status – Policy Retrieval	Executes a full policy reset or re-installs the ConfigMgr Client if the option is selected.
ConfigMgr Client Status – Software Distribution	Executes a full policy reset or re-installs the ConfigMgr Client if the option is selected.
ConfigMgr Client Status – Software Inventory	Executes a full policy reset or re-installs the ConfigMgr Client if the option is selected.
ConfigMgr Client Status – Status Message Submission	Executes a full policy reset or re-installs the ConfigMgr Client if the option is selected.

Data Execution Prevention Checks

Health Check	Remediation Details
DEP - Policy	Settings Data Execution Prevention Policy to specified setting

DCOM Checks

Health Check	Remediation Details
DCOM – Remote Connection Enabled	Writes registry value: Hive: HKLM or HKCR Key: Software\Microsoft\Ole Value Name: EnableDCOM Value: Y

Network

Health Check	Remediation Details
(Lanman) Server – Service Running	Starts the LanmanServer service and sets its start mode to automatic.
Network - DNS Name Resolution	Registers the current IP with DNS by executing the command: ipconfig /registerdns
Network – DNS Settings	Sets the provided Primary DNS suffix and/or syncs with domain membership. Sets the Primary DNS domain. Sets the NIC DNS domain and/or Enable Dynamic DNS Registration.
Network – Hosts file entries present	If specified entries in the hosts file are not present, they will be appended to the hosts file.

Operating System (OS) Health Checks

Health Check	Remediation Details
OS – Admin Share Available	The admin$ share is created and mapped to the %WINDIR% folder.
OS – Clear Windows print queues	The Windows print queues will be cleared.
OS – File Associations	File associations are defined in the format <extension>=<application>, if not present or incorrect, the file associations will be set.
OS – Remote Desktop Settings	Allows for the options: • Enable / Disable All Remote Assistance connections • Enable / Disable Remote Desktop connections • Enable / Disable Remote Desktop with NLA (Network Level Authentication)
OS – Run Key Entries	Sets 64-bit, 32-bit, or both registry run keys based on a specified list.

OS – Screen Saver Settings	Sets screen saver settings for New and Existing Users, Existing Users Only, or New Users Only for the following settings: • Enabling a screen saver • Require a password to exit screen saver • Set a specific screen saver timeout
OS – Security Group Presence	Adds a specific member to a specified local user group if the user does not exist.
OS – Windows Explorer Settings	Sets Windows Explorer settings for New and Existing Users, Existing Users Only, or New Users Only for the following settings: • Show Hidden Files • Show Protected System Files • Hide File Extensions • Compress Files in a Different Color • Show Run on Start Menu • Hide Empty Drives • Show Full Path
Remote Registry Service Running (OS Specific)	Starts the Remote Registry service and sets its start mode to automatic.

PowerShell Health Checks

Health Check	Remediation Details
PowerShell – Set PowerShell Execution Policy	Sets the PowerShell Execution Policy setting to one of the following: • Restricted: Do not load configuration files or run scripts • All Signed: Requires all scripts to be signed by a trusted publisher • Remote Signed: Requires all scripts downloaded from the Internet to be signed • Unrestricted: Runs all scripts. Unsigned scripts from the Internet will prompt for permission • Bypass: Nothing is blocked and no warnings or prompts will occur • Undefined: Removes the current execution policy form the current scope
PowerShell - WinRM	If WinRM is disabled, WinRM will be enabled.

SCCM Miscellaneous Checks

Health Check	Remediation Details
SCCM – Client Actions must be Present	Performs a machine policy refresh

Security Health Checks

Health Check	Remediation Details

Security - Bad Rabbit Immunisation	Removes the infection and immunizes against future attack
Security – BitLocker Drive Encryption	Enables BitLocker on either: • Operating System Drive Only • All Fixed Drives • Specific Drive Letter
Security – User Access Control (UAC) Enabled	UAC is enabled.
Security - WannaCry Vulnerability Assessment	Sets the following registry value and shuts down the system. Hive: HKEY_LOCAL_MACHINE Sub Key: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters Name: SMB1 Type: REG_DWORD Value: 0

Software Health Checks

Health Check	Remediation Details
Software – Internet Explorer Home Page	Sets a defined Internet Explorer Home Page for New and Existing Users, Existing Users Only, or New Users Only.

System Performance Health Checks

Health Check	Remediation Details
System - Disk Cleanup	Initiates a system disk cleanup by executing the cleanmgr built-in application.

System Settings Checks

Health Check	Remediation Details
System – Registry Setting must Exist	Sets the specific registry to the specified value
Unquoted Service Binary Path	Fixes binary path which are not surrounded by double quotes

Tanium Health Checks

Health Check	Remediation Details
Tanium – Verify Client Settings	Set the Tanium Client settings

Windows 10 Health Checks

Health Check	Remediation Details
Windows 10 - Credential Guard Active	Enables Credential Guard Feature on the system.
Windows 10 - Device Guard & Credential Guard Active	Enables Device Guard and Credential Guard features on the system.
Windows 10 - Device Guard HVCI Active	Enables Device Guard feature on the system.

Windows Update Agent (WUA) Health Checks

Health Check	Remediation Details
Windows Update - Last Scan Cycle	Initiate an SCCM Software updates scan cycle on the system.
Windows Update - Metadata Version	Initiate an SCCM Software updates scan cycle on the system to retrieve the latest update metadata.
WUA – Service Missing	The following command is executed to restore the Windows Update service: regsvr32 -s wuaueng.dll
WUA – Service Running	Starts the Windows Update service and sets its start mode to automatic.
WUA - Version	Installs the specified version of WSUS client on the client machine.

WMI Health Checks

Health Check	Remediation Details
WMI – ConfigMgr Client Namespaces	The remediation is the same as WMI – Repository Integrity remediation below, except that the execmgr.log is deleted.
WMI – ExecMgr Connection Error	The remediation is the same as WMI – Repository Integrity remediation below, except that the execmgr.log is deleted.
WMI – In Path	The System32\WBEM folder is added to the %PATH% environment variable.
WMI – Repository Integrity	The WMI repository is recreated: If pre-Windows XP SP2 OR if pre-Vista and Reset WMI Repository is selected, the following occurs: ▪ Net stop winmgmt ▪ Wait 5 seconds ▪ Delete %windir%\system32\wbem\repository folder ▪ Wait 5 seconds ▪ Re-register WMI DLLs and EXEs: cd /d %windir%\system32\wbem for %i in (*.dll) do RegSvr32 -s %i for %i in (*.exe) do %i /RegServer for %i in (*.mof) do mofcomp %i

	for %i in (*.mfl) do mofcomp %i Net start winmgmt On windows XP SP2 and later systems: rundll32 wbemupgd, UpgradeRepository On Windows 2003 Server SP1: rundll32 wbemupgd, RepairWMISetup On Vista onwards: winmgmt /salvagerepository OR winmgmt /resetrepository Net start ccmexec Wait for the input wait duration. Generally, 5 minutes
WMI – Service Running	Starts the Windows Management Instrumentation service and sets its start mode to automatic.