

---

# Adaptiva OneSite User Guide

Updated: September 1, 2022

## OneSite Anywhere

- Configuration Manager
- Intune
- VMware Workspace ONE

# Table of Contents

What is Adaptiva OneSite? .....	5
Adaptiva OneSite Benefits .....	5
What Does OneSite Anywhere Add? .....	5
Please Read First.....	6
How Adaptiva OneSite Anywhere Applies to the New Normal .....	7
The Situation .....	7
The Problem.....	7
The Solution .....	7
Navigating the Adaptiva Web Portal .....	9
User Authentication .....	9
Licensing Adaptiva .....	9
Web Page Orientation .....	10
Navigating the Adaptiva Workbench .....	13
User Authentication .....	13
Licensing Adaptiva .....	13
Perspectives, Views, and Editors .....	14
Security and Access Control .....	15
Security Manager Perspective .....	21
Defining Network Topology .....	27
Topology Planning.....	27
Using the Adaptiva Web Portal .....	27
Using the Adaptiva Workbench.....	36
Importing the Network Topology Information .....	43
Configuring OneSite Anywhere.....	47
Upgrading to use OneSite Anywhere.....	47
Publish Content to the CDN-based Content Library .....	47
(Optional) Manage Client Authorization .....	47
Configuring OneSite for Intune .....	50
Using the Adaptiva Web Portal .....	50
Using the Adaptiva Workbench.....	50
Configuring OneSite for VMware .....	51
Health Check.....	51
Content Publication Settings.....	52
ConfigMgr Content .....	52

Intune Content .....	60
Workspace ONE Content .....	61
Adaptiva Content .....	61
Scenario: Zero Day Exploit – Using Content Priority to Distribute Faster .....	62
Content Creation and Publication .....	64
Adaptiva Web Portal Content Publishing Icons .....	64
Adaptiva Workbench Content Download Icons .....	65
ConfigMgr Content .....	65
Intune Content .....	71
Workspace ONE Content .....	80
Adaptiva Content .....	88
Content Push .....	95
Introduction .....	95
Overview .....	95
Features .....	95
Using the Adaptiva Web Portal .....	96
Using the Adaptiva Workbench .....	104
Distribution Status .....	112
LiveFlow Content Transmission .....	112
Content Distribution Status .....	126
Additional Settings for ConfigMgr Environments .....	128
Linked Servers and Object Export .....	128
Microsoft App-V Perspective .....	131
Client Data Upload Bandwidth Management .....	133
Content AutoStage .....	137
DP Bypass and DP Fallback .....	138
Peer-to-Peer PXE .....	143
Policy Bandwidth Management .....	148
Virtual SMP .....	152
Client Settings .....	154
Using the Adaptiva Web Portal .....	154
Using the Adaptiva Workbench .....	157
Dashboards .....	160
Using the Content Download Details Dashboard .....	161
Schedules .....	164
Creating a Custom Schedule .....	164
Adaptiva Groups .....	171

Using the Adaptiva Web Portal .....	171
Using the Adaptiva Workbench .....	174
(Optional) Post Installation Activities .....	179
Cache Migration Tool .....	180
Overview .....	180
How It Works .....	180
Prerequisites .....	180
Tool Location .....	180
Using the Cache Migration Tool .....	180
Appendix A: Adaptiva Logs .....	183
Server Logs .....	183
Client Logs .....	183
Appendix B: Installing the App – What Does the User See? .....	186
ConfigMgr .....	186
Intune .....	192
Workspace ONE .....	197
Adaptiva Content .....	206

# What is Adaptiva OneSite?

Adaptiva OneSite allows you to reduce your Microsoft Endpoint Manager - Configuration Manager (ConfigMgr) server hierarchy and improve bandwidth utilization. It allows you to remove ConfigMgr Secondary sites, all but one Distribution Point, and eliminates your reliance on Background Intelligent Transfer Service (BITS) and throttling. Companies are able to save on hardware costs, server OS licenses, as well as drastically reduce the cost of managing these servers. This is made possible through an enterprise peer-to-peer system, a distributed virtual cache, and advanced network protocols.

## Adaptiva OneSite Benefits

- Roll-out ConfigMgr infrastructure in weeks rather than months
- Simplify operations: no system design or operational maintenance
- Lower costs: Reduce server cost and maximize bandwidth utilization
- Dramatically faster package downloads
- Secure software distribution
- No need for Delivery Optimization configuration, Connected Cache Servers, or scheduled distributions to reduce bandwidth utilized

## What Does OneSite Anywhere Add?

With Adaptiva OneSite Anywhere, there is integration with VMware's Workspace ONE, Microsoft Intune, and Azure to enable endpoints to get content no matter where they are, and at the same time reducing VPN traffic by leveraging consumer internet links. Remote Offices with dedicated internet connections would also benefit by the removal of content downloads across their corporate WAN connection. Adaptiva OneSite Anywhere provides internet-based peer-to-peer (IP2P) to reduce congestion on the VPN and remote office connections.

- OneSite Anywhere alleviates the strain on VPNs by offloading endpoint content updates such as software and patching, enabling endpoints to get content directly from Adaptiva's own CDN, Azure, Workspace ONE CDN or from other endpoints
- OneSite Anywhere adds internet P2P capabilities to extend endpoint management and software delivery to endpoints no matter where they are. No longer do endpoints need to be on the corporate network; remote workforces will be managed just like onsite staff
- Ability to perform single CDN download from the Adaptiva CDN, Azure or Workspace ONE CDN to entire corporate network and then distribute content peer to peer.

## Please Read First

To ensure most productive experience using OneSite. Please review this guide in its entirety and consider the following points before beginning your installation:

- **There are NEW exclusions with version 8.0 and later.** Ensure the required Anti-Virus exclusions are added for all clients and server as detailed in the Installation Guide. In build 8.3 and later it will be necessary to ensure additional exclusions are added for new binaries included with the **Adaptiva Endpoint Patch** product.
- The Adaptiva Client must be installed on all machines to which the administrator wishes to download content.
- Verify no client or server firewalls restrict the port communication required for normal operation. Port information can be found in the installation guide.
- Your network topology must be properly defined in Adaptiva before your content distribution is optimized. Auto network detection is done automatically based on the different subnets in your network.
- Devices must be able to communicate with the Adaptiva Server on the corporate network or the Adaptiva Cloud Relay Service on the public internet in order to receive policy and communicate status.
- The Adaptiva Server must be able to communicate with Adaptiva clients. Clients using Network Address Translation (NAT) or ipv6 are not supported.

# How Adaptiva OneSite Anywhere Applies to the New Normal

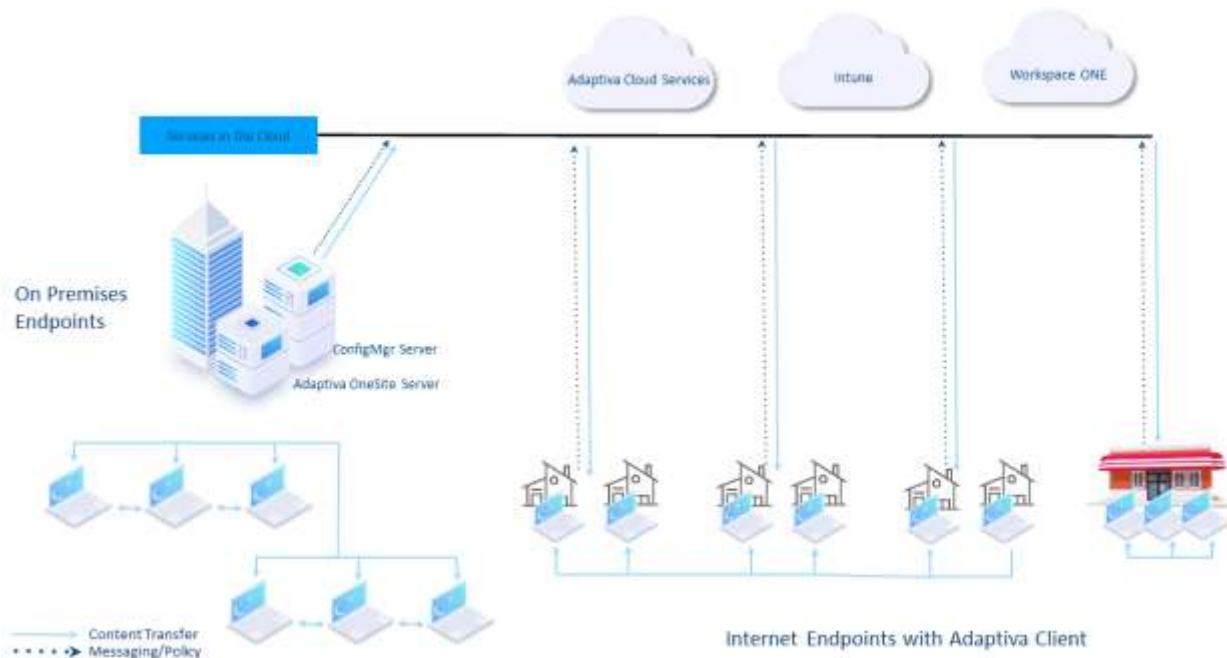
## The Situation

A large organization will typically have one or more main offices but could potentially have a large number of satellite or branch offices. Clients are also moving more frequently between on-premises connections and internet-based connections. More client computers are working from home or public Wi-Fi connections. These computers are connecting back to the corporate network using a VPN and saturating that VPN with application downloads and software update patching. This is slowing down the VPN, slowing down delivery of the applications and software updates but more importantly, slowing down the business applications that are not yet cloud-enabled.

## The Problem

Organizations will typically have a single access point to the internet via a proxy server or similar. When multiple, on-premises, clients are downloading the same content from the internet, that duplicated content is taking up additional bandwidth on the internet connection. VPN connections are also overloaded as more clients are working from home. If the VPN solution does not allow split tunneling all traffic must traverse the VPN. Some computers may never connect to the VPN and thus disappear from the ability to manage the device and support the user. In addition, AD Sites may be setup corresponding to AD Domain Controller locations, not the physical locations of routers or individual subnets. This makes peer to peer communication across an AD Site undesirable. Wireless networks and subnets dedicated to VPN clients also create additional administration requiring GPOs to enforce special configurations.

## The Solution



Adaptiva OneSite Anywhere now allows client computers to receive content, from the internet, when they are not on the corporate network or connected to the VPN. VPN connections that allow split-tunneling can eliminate all application download and software update patching content from traversing the VPN. This will allow the business applications to fully utilize the VPN for business traffic, while at the same time

decreasing the time it takes to deliver software and software updates to all remote devices. For those devices without split tunneling VPNs, OneSite will optimize the connection so that business traffic is prioritized over system management communications.

Using Adaptiva OneSite Anywhere will reduce, potentially to one, all downloads from the CDN. This will immediately reduce Azure costs. OneSite can also be configured to allow specific offices to download once from the internet and then share the content locally using Peer to Peer technologies. OneSite clients on the internet can also use Peer to Peer to share content. Clients will use an IP Geo-location system to find the closest peer across the internet. This will remove content downloads from the Content Delivery Network (CDN) and DP configured with the CMG.

Adaptiva OneSite uses a proprietary technology for avoiding congestion and delivering content at speed and scale without impacting the network or other business traffic.

OneSite's Predictive Bandwidth Harvesting technology will correctly detect the slowness of the link and any high latency. It will then automatically adapt itself to harvest only that amount of bandwidth which is not actually being used at that instant. Because this technology is fundamentally real-time in its nature, it adapts very rapidly, even when network utilization swings up and down every few milliseconds. OneSite's Flow Equalizer ensures that higher priority distributions occur first and then evenly allocates the available WAN bandwidth amongst multiple concurrent flows when multiple downloads of the same priority occur; this is similar to how an operating system distributes CPUs between multiple applications. OneSite does this by time-slicing the use of the network equally between peers, which prevents multiple concurrent WAN transfers from ever taking place.

The overall result of this combination of technologies is that there is always only one extremely well-behaved WAN transfer in progress to any given location. This allows for a completely hands-off approach to content delivery whereby any content of any size can be transferred over any link speed at any time of the day, with administrators safe in the knowledge that the network and user experience will be completely unaffected by it.

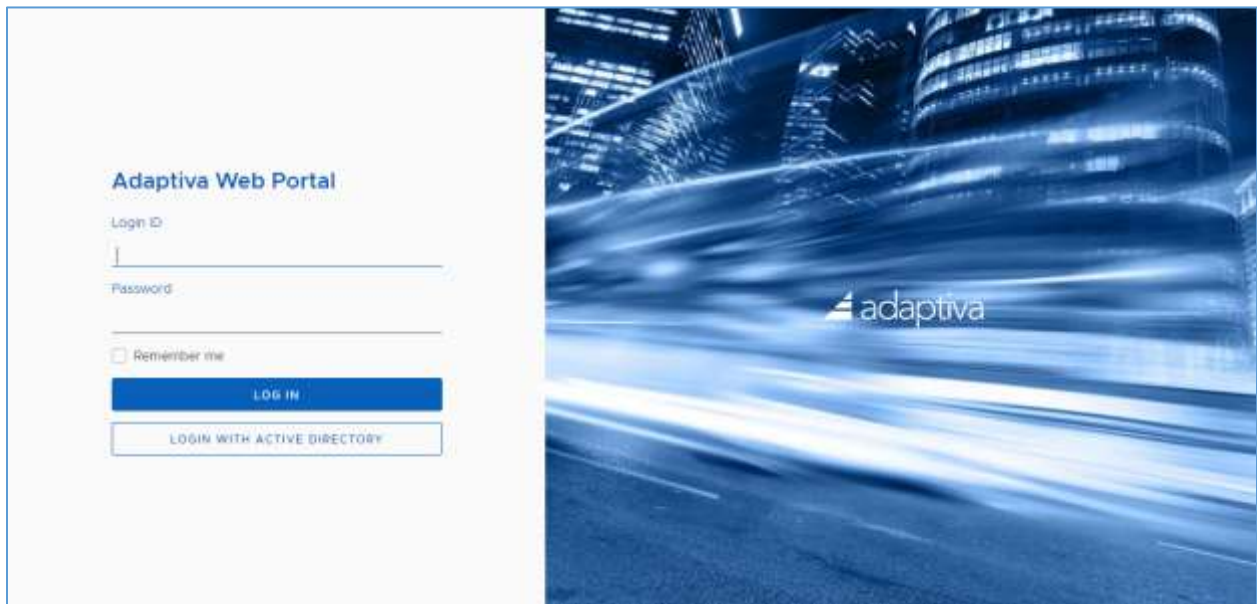
When used with Microsoft Configuration Manager, Adaptiva OneSite Anywhere does not require additional on-premises servers while providing an optimal alternative to remote distribution points. The need for a Microsoft Connected Cache server is replaced by a virtual cache. Our Virtual SAN technology combines all unused storage on clients into a collective file store. For example, if you have 100 clients, and each has 20GB of free space, that space is combined into a 2TB drive. The users are unaware their hard disk is being used for storage as we do not report this back to the OS. As they use up more of their disk space, cached content is intelligently and automatically purged based on content that is present throughout the location. As a result, each location has a nearly unlimited file store to cache all distributions. Each content item such as a package, or OS image only needs to be transported over the WAN once, and then the content is cached locally in that office.



# 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[s]://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. There are two separate options on how to log in


- **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 Super Admin or creates an Adaptiva login which is used as the Super Admin. 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.

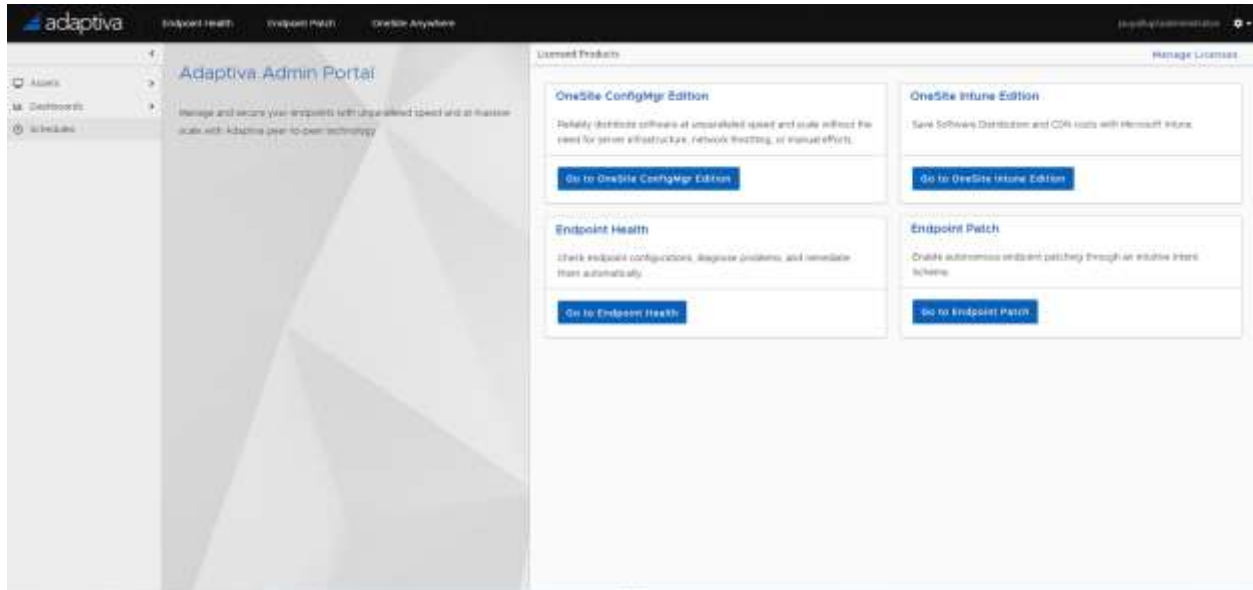
The license key will contain the licensed Company name and client count. The license key needs to be entered using the Adaptiva Web Portal or Adaptiva Workbench.

- 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[s]://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](mailto: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 ConfigMgr, OneSite Intune, OneSite VMWare, and Endpoint Health.



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.

### Pull-out Menus

Some Activity pane items have pull-out menus. These will be shown with  on the menu selection. To display the pull-out menu, click the menu item 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.

### Search and Sort

Many pages will include the ability to search the returned results. Select the **Search Columns...** drop down to select what to search for. Typically, the left-most column is always the default column to search.

Click on  to complete the search.

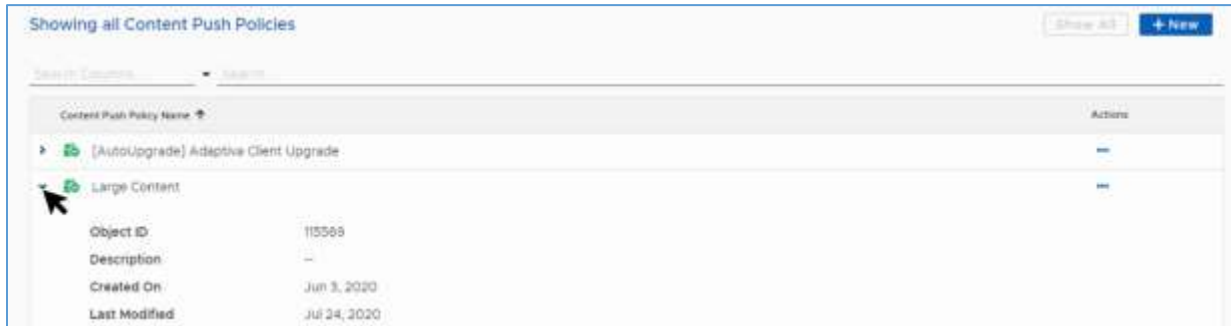
Many of the columns will be sortable, just click on the column name. The sort order will be displayed next

to the column name using  or . Non-sortable columns will not change the pointer to  and will


remain the default pointer .


## Object Information

If there is a > to the left of the row additional information is available and can be found by expanding the item by clicking on the >.



## Reorganizing Objects

Some objects can be ordered manually. When  is to the left of the row clicking and dragging that as a handle will allow you to change the order of the returned rows or move objects to a different folder. If

reordering is not available, you will see the following: 

## Selecting Objects

When a row has  on the far left, check one or more boxes to select the rows. Multi-select is not always available. At the top and bottom of the results will also be additional context menus. A check box to select All, if available, and ellipses for additional actions on the selected rows.

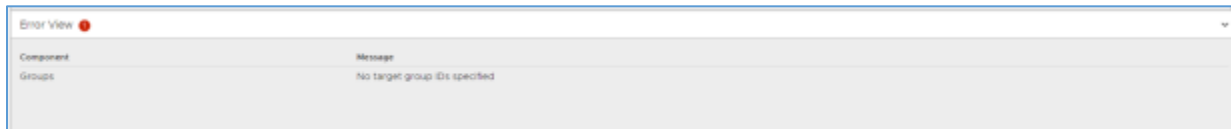
## Displaying All Rows

When results are returned, they will default to be displayed in 10 rows per page. This can be changed by select the drop down and select 10, 25, 50 or 100. Use the |<, <, >, or >| buttons to move forward and backward through the pages.



## Errors

At the bottom of Editor pages will be a collapsed section named **Error View**. This may display errors found when saving a form. Clicking on Error View will expand the section and show any relevant errors for that Editor.



The error will also be displayed in the form.

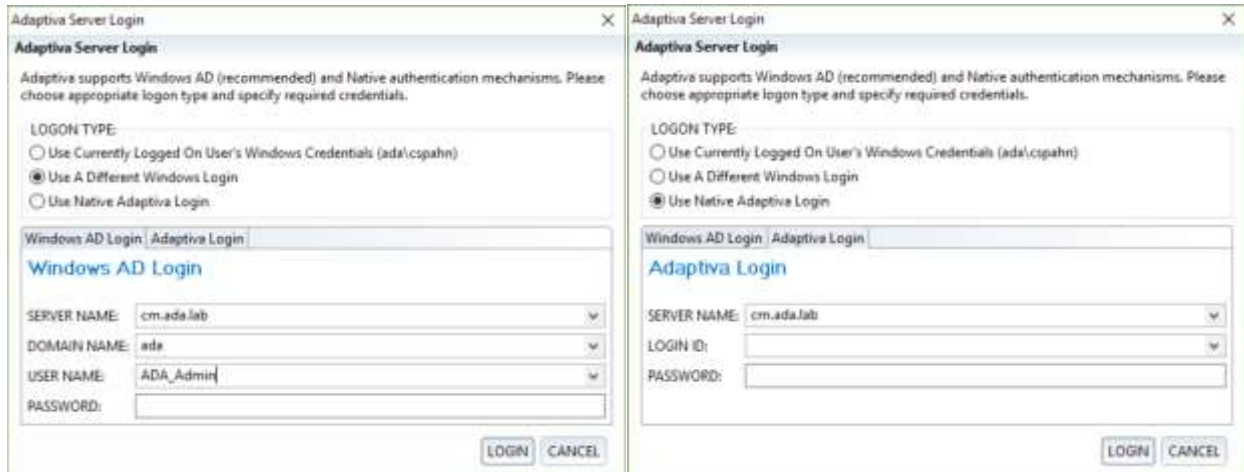
▼ General Settings

Name	<input type="text" value="Test Client Setting"/>
Description	<input type="text"/>
Priority	<input type="text" value="1"/>
 No target group IDs specified	<input type="button" value="Dismiss"/>
Target Groups	<input type="text" value="Add Groups"/> <input type="button" value="Browse"/>

# Navigating the Adaptiva Workbench

To launch the Adaptiva Workbench, click **Start -> Adaptiva -> AdaptivaWorkbench**. Alternatively, navigate to the Adaptiva Workbench installation directory (default is **C:\Program Files (x86)\Adaptiva\AdaptivaWorkbench**). Run the application **AdaptivaWorkbench.exe**.

## User Authentication



The Adaptiva Server Login dialog will open, first select your logon type:

- **Use Currently Logged on User's Windows Credentials** – this option will allow the user to login using their current login token.
- **Use a Different Windows Login** – this option allows a user to enter an AD domain name, AD user account, and password.
- **Use Native Adaptiva Login** – this option allows a user to login with an Adaptiva user name and password.

Then, on the appropriate tab (Windows AD Login or Adaptiva Login)

1. Enter the host name of the machine where Adaptiva Server is installed.
2. If using a Windows AD Login, enter the domain name.

**NOTE: For the Domain Name field, a FQDN or NETBIOS name can be used, but must match the format used for domain name when the user was created in the Workbench.**

3. Enter a user account that has been granted permissions in the Workbench.
4. Enter the password.

By default, when you install Adaptiva Server, the person installing either selects a Windows AD account to be used as the Super Admin or creates an Adaptiva login which is used as the Super Admin. 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 Workbench.

- If you are starting the workbench for the first time or your key has expired, you will be prompted for a key at startup.
- In the workbench, you can view keys or add more by expanding the **Misc** folder and selecting the **Product Licensing Perspective**.

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](mailto:ticket@adaptiva.com).

## Perspectives, Views, and Editors

The Adaptiva Workbench is used to configure Adaptiva OneSite and is customizable in nature. The three main components to the Workbench are perspectives, views, and editors.

- A View provides information for a given task. A view is typically used to navigate a hierarchy of information, open an editor, or display properties for the active editor. The two most common views in the Adaptiva Workbench are Explorers and Task Navigators.
- An Editor is a page that displays information or allows the user to edit a configuration.
- A Perspective is a combination of views and editors that perform a particular set of tasks. Use of perspectives allows the administrator to see all relevant information and hide the rest.
- Explorers are used to display objects. These could be objects created by Adaptiva, ConfigMgr, or the administrator. Right click on an object in an explorer to view operations which can be performed on that object.
- Task Navigators display a list of tasks which may be performed. Selecting an item from a task navigator will open any views, perspectives, or editors needed to perform the task.

### Working with Perspectives

To change perspective, click on **Perspective->Manage Perspectives**. The **Workbench Perspectives** dialog box will appear, allowing you to select any perspective. When you change perspective, the current perspective is maintained, and all open views and editors will be available when you return to the previous perspective.

You can quickly navigate between open perspectives using the **Ctrl+F8** and **Ctrl+Shift+F8** hotkeys.

### Working with Views

To open a view, click on **View->Manage Views**. The **Workbench Views** dialog box will appear, allowing you to select any view. Once opened, views can be moved and placed anywhere on the workbench for convenience.

The position of views within a perspective is always maintained. To reset a perspective back to the previous layout, select **Perspective->Reset Perspective**. To restore a perspective to the original layout, select **Perspective->Restore Perspective**.

# 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

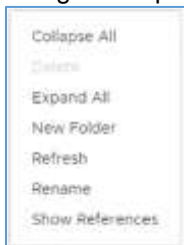
During the installation of the Adaptiva Server, the installer allows the administrator to create an Adaptiva User ID or specify an AD user account as SuperAdmin. The SuperAdmin account has the maximum permissions in the Adaptiva environment.

Security can only be managed using either the Adaptiva Web Portal or the Adaptiva Workbench.

## Using the Adaptiva Web Portal

The preferred method of managing security is through the Adaptiva Web Portal.

1. Connect to the Adaptiva Web Portal using a web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on the gear, , **Settings**, then select **Security**
4. The Settings workspace will open to the Security:Administrators view. At this screen there are several components:
  - Administrators and Roles tabs – Used to switch between Administrator management view and Roles management view
  - Folders – The default Administrator's folders are Root and Windows Administrators. There is only the Root folder for Roles. Other folders may exist depending on which solutions have been licensed, e.g. OneSite Admins, Advanced Endpoint Health Roles, Basic Endpoint Health Roles.
    - Using the ellipses additional actions can be taken on a selected Folder

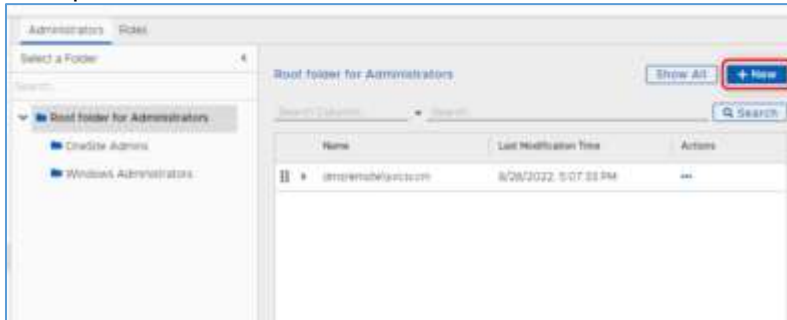


Collapse All	Collapses all folders to the root folder
Delete	Deletes a folder. Built-in folders cannot be deleted
Expand All	Expands all sub-folders below the selected folder
New Folder	Creates a New Folder as a sub-folder of the selected folder
Refresh	Refreshes the folder structure Use this after creating a new folder
Rename	Allows a Folder to be renamed
Show References	Shows where the folder object is being used

- The right-most pane will show the members of the selected folder.
  -

## Adding New Administrators

1. To create a new administrator, click the **+New** button in the upper right of the Administrators workspace.



2. The Administrator editor will appear. Complete the following sections:

### Administrator Details

The screenshot shows the 'Administrator Details' form. It includes fields for 'Admin Type' (with radio buttons for 'Administrator' and 'Windows AD Login'), 'Email Address', 'Password', and 'Confirm Password'.

**Admin type** – Specify if this is an Adaptiva login or a Windows AD login. It is recommended to use Windows AD logins to maximize security.

#### Adaptiva Login

**Email Address** – Specify email address of administrator. This is a required field. The email address does not have to be a real or valid email address. It will become the account's username and will be required when using the Adaptiva login

**Password** – Specify a password for the new account. The password must be at least 10 characters long and include at least one uppercase letter, one lowercase letter, and one numeric character. Enter the same password in the Confirm Password box.

#### Windows AD Login

**Windows Domain** – Enter the NETBIOS domain name of the account domain

**Windows User Name** – Enter the SAMAccountName of the user's domain account that will be created as an Adaptiva Administrator

### User Details

The screenshot shows the 'User Details' form. It includes fields for 'First Name', 'Last Name', 'Work Phone Number', 'After Office Phone Number', and 'Cell Phone Number'.



**First Name** – Enter the user’s First name. This is required.

**Last Name** – Enter the user’s Last name. This is required

The following are optional

**Voice Phone Number**

**After Office Phone Number**

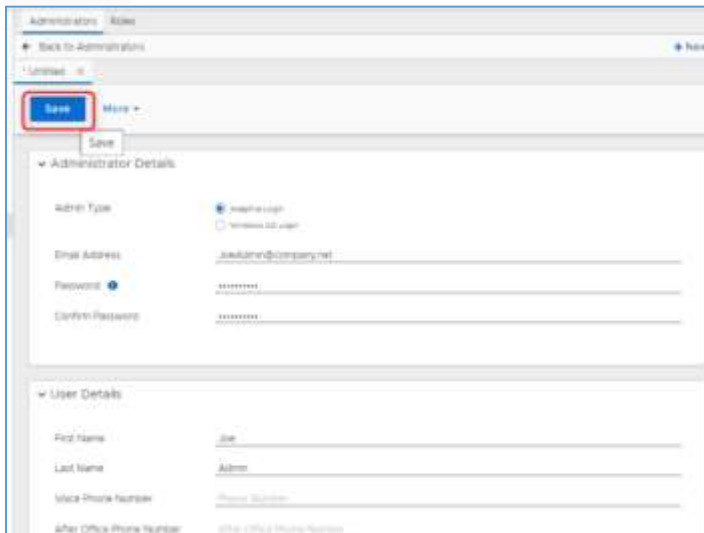
**SMS Phone Number**

### Direct Roles

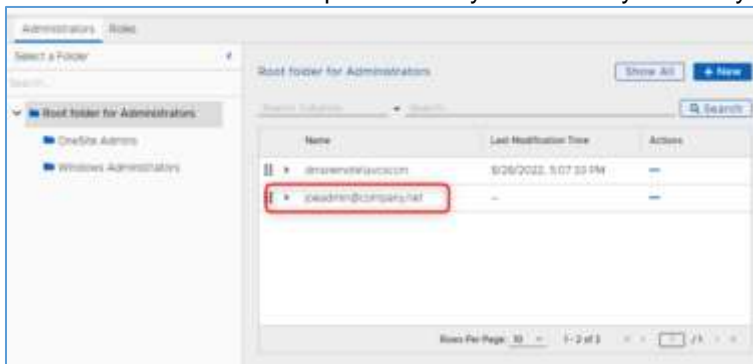


**Roles** - This list represents all roles to which the administrator has been added directly. For existing administrators, changes to this list will save immediately. You can use the **Browse** button to open the Role selection screen. See the section **Assigning Roles to Administrators**.

- Once you’ve completed the required fields, scroll back to the top of the Administrator editor and click Save.



- After saving the new login, you can use the **← Back to Administrators** button to navigate back to the Administrators workspace. Here you can find your newly created login.

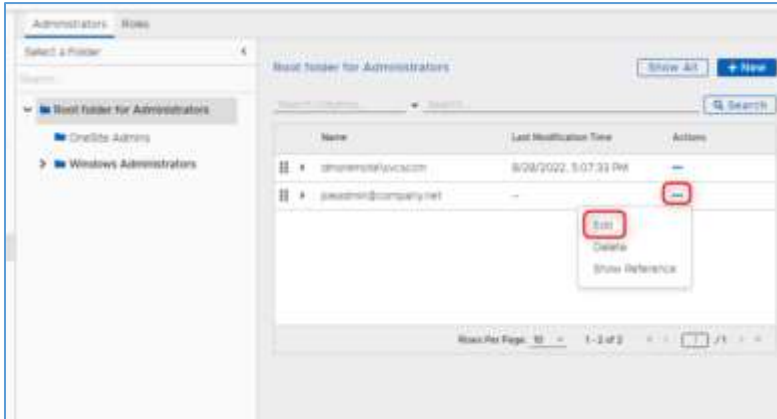


**NOTE: Adaptiva logins will be created in the selected folder. Windows AD Logins will be created in the Windows Administrators folder**

## Assigning Roles to Administrators

By default, all newly created users are added to the **All Admin** role. This role has limited access. To manage roles for an Administrator account, follow these steps:

1. On the Administrators tab, locate and click on the Administrator you wish to manage. Alternatively, you can use the ellipsis, ..., in the Actions column and select **Edit**.



2. The Administrator editor will display. Scroll to the bottom of the editor to the Direct Roles section. Displayed here are any roles already assigned to this login. Click the Browse button to add a new role.



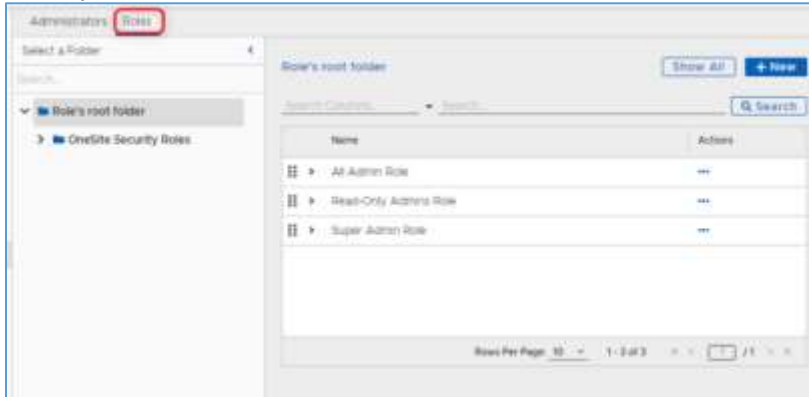
3. The Manage Roles screen will display. This view allows you to navigate the Roles folder structure and search for specific roles. The Roles root folder will contain roles that are universal to all Adaptiva products that are installed. Check the box next to one or more roles to assign to the Administrator account. To remove a role, uncheck the box next to the role.
4. Click the **Manage Roles** button
5. You'll return to the Administrators editor. The new role assignment will appear in the Direct Roles section. Also, you can remove a role by clicking the **X** next to the role name.

**NOTE: When you add or remove a role on an existing Administrator, saving the Administrator object is not necessary. The new role assignment is applied immediately.**

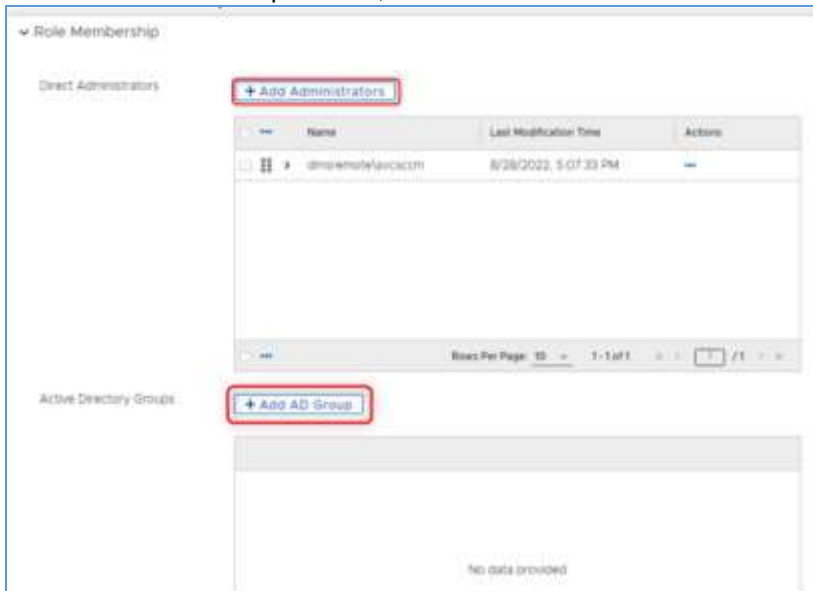
## Manage Role Assignments

To add Administrator accounts, including AD Groups, to a specific role, follow these steps:

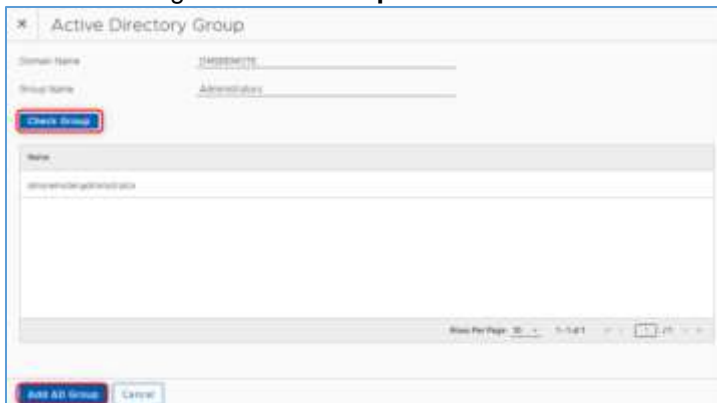
1. On the Roles tab, locate and click on the Role you wish to manage. Alternatively, you can use the ellipsis, ..., in the Actions column and select **Edit**.



2. In the Role Membership section, select either **+ Add Administrators** or **+ Add AD Group**



3. When selecting **+ Add Administrators** the Administrators root folder will be displayed. Check the box for one or more Administrator accounts and click on **Add Administrators**.
4. When selecting **+Add AD Group**



Enter the following:

**Domain Name:** Enter the NETBIOS Domain name

**Group Name:** Enter the Domain Local or Domain Global Group name

Click on **Check Group**

**NOTE: The group must have members. Also, nested group membership is not supported, only direct members will be returned. Universal Groups are not supported.**

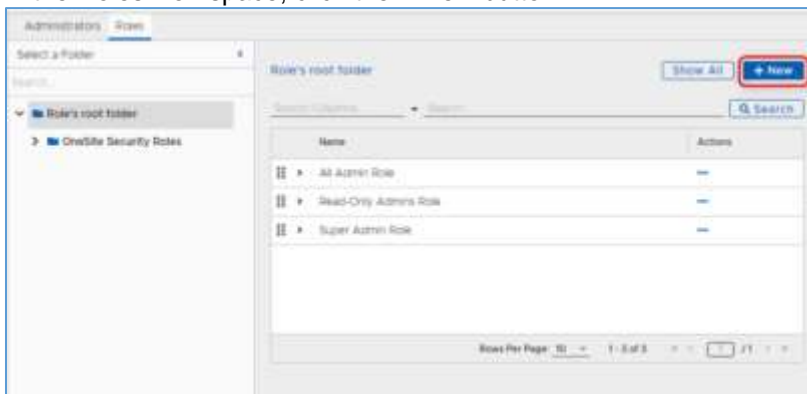
5. Click on **Add AD Group**
6. Click on **Save**

**NOTE: Members of the AD Group will automatically be created as Adaptiva Administrators and added to the All Admins Role**

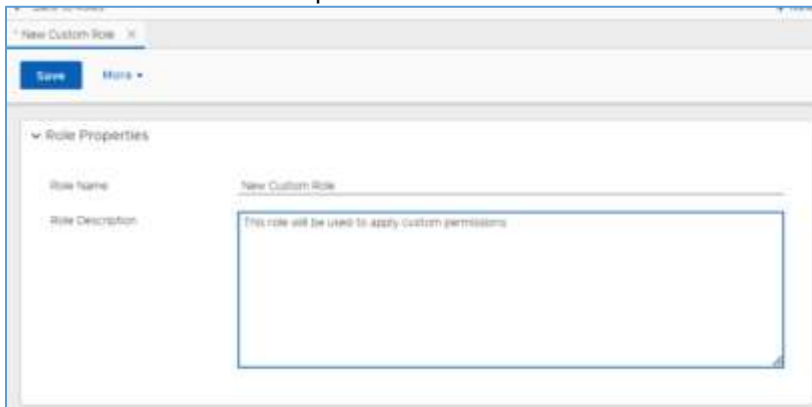
## Creating New Roles

Some organizations may want to create custom roles to control access to what some administrators can view or change. Roles can be created in the Web Portal, but at this time, Folder-level and Class permissions can only be assigned using the Adaptiva Workbench. Follow the steps below to create a new Role:

1. In the Roles workspace, click the + New button.



2. The New Role Editor will open



Complete the following sections:

### Role Properties

**Role Name** – Give the role a descriptive name

**Role Description** - A detailed description of what the roles purpose is

**Role Membership** – Add Administrators and AD Groups to the role. See the section Manage Role Assignments

**Direct Administrators** – Use the **+ Add Administrators** button to browse and add Adaptiva local logins and AD user accounts to the role

**Active Directory Groups** – Use the **+ Add AD Group** button to add AD domain groups to the role.

3. At the top of the Role editor screen, click the **Save** button.

## Assigning Permissions to a Role

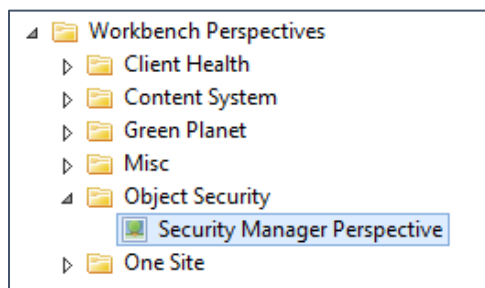
At this time the Adaptiva Workbench must be used to assign specific Class or Folder level permissions to a role.

## Using the Adaptiva Workbench

### Security Manager Perspective

OneSite's security model is administered from the **Security Manager Perspective** when using the Adaptiva Workbench.

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



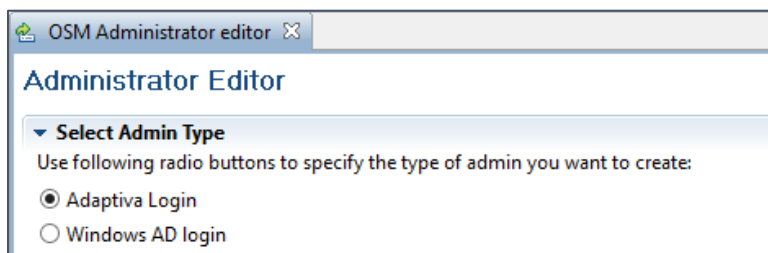
In the **OSM Task Navigator** pane, the following **Tasks** are available:

- 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**.



- 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	<input type="text" value="newadmin@company.com"/>
Email address	<input type="text" value="newadmin@company.com"/>
Password	<input type="password" value="••••••"/>
Confirm Password	<input type="password" value="••••••"/>
Windows Domain	<input type="text"/>
Windows User Name	<input type="text"/>
First Name	<input type="text" value="New"/>
Last Name	<input type="text" value="Admin"/>
Voice Phone Number	<input type="text"/>
After Office Phone Number	<input type="text"/>
SMS Phone Number	<input type="text"/>

**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.

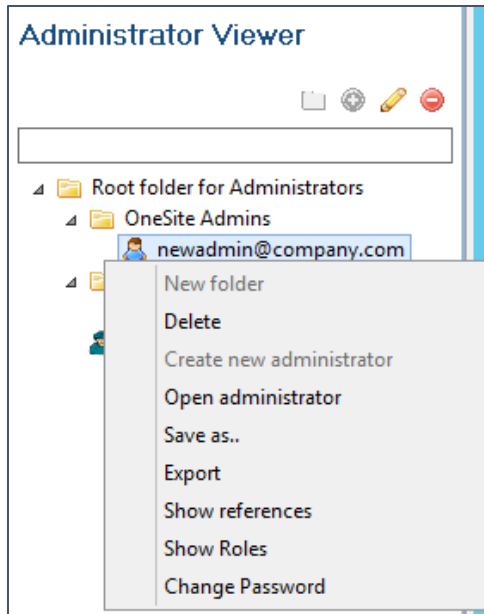
**Details**

Please fill the details of the administrator

LoginId	<input type="text" value="company.com\adaptivaAdmin"/>
Email address	<input type="text" value="adaptivaAdmin@company.com"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Windows Domain	<input type="text" value="company.com"/>
Windows User Name	<input type="text" value="adaptivaAdmin"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
Voice Phone Number	<input type="text"/>
After Office Phone Number	<input type="text"/>
SMS Phone Number	<input type="text"/>

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

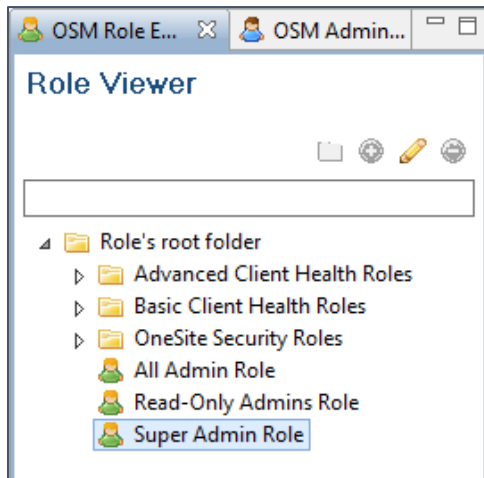
- On the right of the workbench, in the **Administrator Viewer** pane, the new administrative accounts will appear. For example, to edit or delete an account, simply right-click the account and select the appropriate option in the context menu.



### 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**.

- 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 SuperAdmin rights, open the **Super Admin Role**.



- In the center of the workbench, the **Role Editor** will appear. In the **Role Properties** section, the name and group can be customized.
- 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.

**Active Directory Groups** Reload Membership

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

Add AD Group

Remove

Remove All

**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

Group Name

Show Members

OK Cancel

**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.

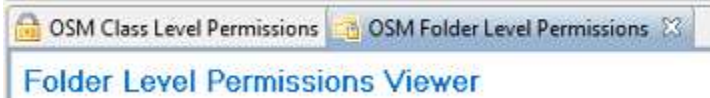
1. To create a new custom role, in the **Security Manager Perspective**, select **Create new Role**.
2. In the **Role Editor**, enter a **Name** for the new role and optionally provide a description.
3. Click **Add an Administrator** or **Add an AD Group** to add the respective accounts. Repeat for all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

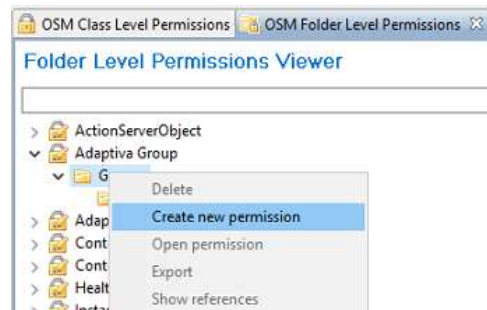
## Assigning Permissions to a Role

1. In the Workbench, under the editor are two views which are used to manage permissions:  
 OSM Class Level Permissions – Manages access to the different classes within OneSite  
 OSM Folder Level Permissions – Manages access to different folders within OneSite



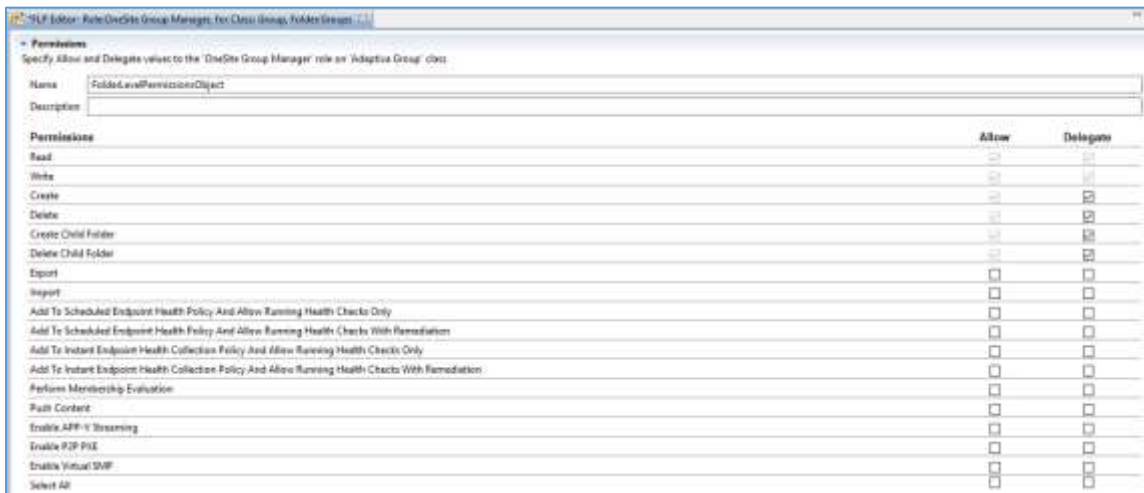
For example, if a role was created named OneSite Group Manager where they will be granted access to create and manage Adaptiva groups. Select the **OSM Folder Level Permissions** tab.

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**.

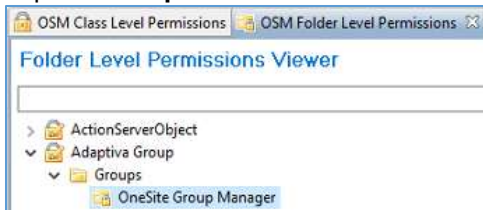


3. In the **Select the role...** dialog, select the role the permissions should be applied to. In this example, select the **Adaptiva Group Manager** role and then click **OK**.

4. In the editor, use the **Allow** checkboxes to grant granular access (permission will be denied, if left unchecked).  
Use the **Delegate** checkboxes to allow this user to granularly assign permissions to other user accounts. Click **Save** to apply the permissions.



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



# Defining Network Topology

## Topology Planning

Proper planning of your Network Topology is a crucial step in the deployment of OneSite. Some key points to keep in mind are:

- An office is defined by one or more IP ranges intended to identify machines that are connected over a LAN.
- Clients in the same office will discover and download content from peers in the same office, if available (Local Discovery).
- If content is not available in the office, the Parent office will be queried and content downloaded, if available (Remote Discovery).

**NOTE: An office can also be configured to download directly from the internet-based Content Delivery Network (CDN) location.**

- Offices will continue up one level in the hierarchy, all the way up to the Central Office to discover and acquire content.
- A particular piece of content will only be distributed from a parent to child office once, thus reducing data sent across WAN links.
- Data transport between offices uses the Background Adaptive Transport. This is the Adaptive Protocol which is designed to protect bandwidth availability by using our Predictive Bandwidth Harvesting, NetBoost, and Flow Equalizer technologies on WAN links.
- Data transport within offices uses the Foreground Adaptive Transport, which accelerates the distribution to all machines that need the content using the Memory Pipeline Architecture.
- IP Ranges separated by a WAN link should be defined as separate offices. If offices are misconfigured, the Foreground protocol might be used over a WAN link, causing saturation of the WAN, or the Background protocol might be used over a LAN, slowing the distribution of content.
- The Adaptiva Server must reside in one of the subnets in the top-tier Central Office (see note below).
- We provide a workflow that allows the Network Topology to be managed via a Microsoft Excel spreadsheet and imported into OneSite.

**NOTE: Upon installation, the Adaptiva Server automatically generates the Central Office with the complete IP address range (the entire subnet) of the Adaptiva server IP address. In all future additions/deletions of Central Office IP address ranges, it is imperative that the Adaptiva server itself falls within one of the valid IP address ranges.**

**The exception to this is when the Adaptiva Server is installed in the internet (Azure, AWS, etc.) as the expectation is there will be reduced clients and limited broadcast capabilities on that subnet. It is recommended to add subnets with Adaptiva clients where the remote offices egress.**

## Using the Adaptiva Web Portal

### Overview

The list of Locations (aka Offices) is available in the Web Portal: **Assets, Locations**.

From this page an administrator can create and view the Location hierarchy structure of the computers in their organization.

## Table view (Default)

Location Name	Location ID	Type	Last Modified	App Location	Actions
Central office	10	Default	4/2/2022 3:41:07 PM	-	...
EU DataCenter	11	Default	4/2/2022 3:40:53 PM	Central office	...
Frankfurt	12	Default	4/2/2022 3:40:48 PM	EU DataCenter	...
London	13	Default	4/2/2022 3:40:53 PM	EU DataCenter	...
Seattle-Wifi	14	Wi-Fi	4/2/2022 3:41:07 PM	US DataCenter	...
Seattle-VPN	15	VPN	4/2/2022 3:41:07 PM	US DataCenter	...
US DataCenter	16	Default	4/2/2022 3:41:07 PM	Central office	...

## Tree View

```

graph TD
    Root[Central office [10]]
    Root --- EU[EU DataCenter [11]]
    Root --- Frankfurt[Frankfurt [12]]
    Root --- London[London [13]]
    Root --- US[US DataCenter [14]]
    US --- SeattleWifi[Seattle-Wifi [14]]
    US --- SeattleVPN[Seattle-VPN [15]]
  
```

The Locations page allows the Administrator to:

- View the hierarchical representation of all locations in the system. They can also be listed in a table view.
- Create a new child location
- Merge one location with another
- Delete an existing location
- View a location
- Edit a location
- Move a location from one place in the hierarchy to another
- Set location type to Default, VPN, or Wi-Fi and other settings
- Show the No Office Clients
- Configure Auto Location Creation

## Search Bar

The Locations page has a convenient search bar which allows you to search for the Locations that you have created. Select Search Column drop down to select what to search for. By default, Search will match the location name. Other options include Location ID and Description among others. Click on [Search](#) to complete the search.

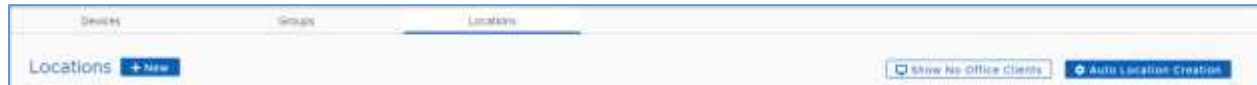
## Show No Office Clients

To view devices which are not associated with any Location click on Show No Office Clients. This will only have clients if Auto Location Creation has been disabled and clients are communicating to the Adaptiva Server.

## Auto Location Creation Settings

When an Adaptiva client registers with the server for the first time, the server looks for an existing location with an IP range that fits that client. If such a location does not exist, the server can automatically create a location using the IP address and subnet mask provided by the client. This is the purpose of the **Auto Location Creation** feature in the Locations page.

By default, Auto Location Creation is enabled. Click **Auto Location Creation** to change these settings.



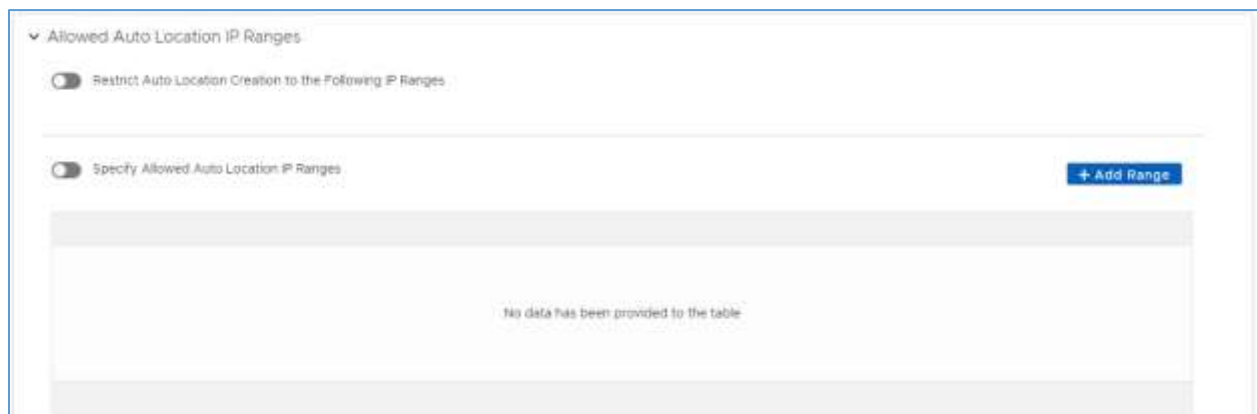
In the **Auto Location Creation Settings** page, Auto Location Creation can be turned **ON** or **OFF**. This can be useful when manually reorganizing subnets to different offices and not wanting them Auto-created when a client on that subnet communicates with the server.

Click the button to toggle to the left to disable Auto Location Creation.



## Allowed Auto Location IP Ranges

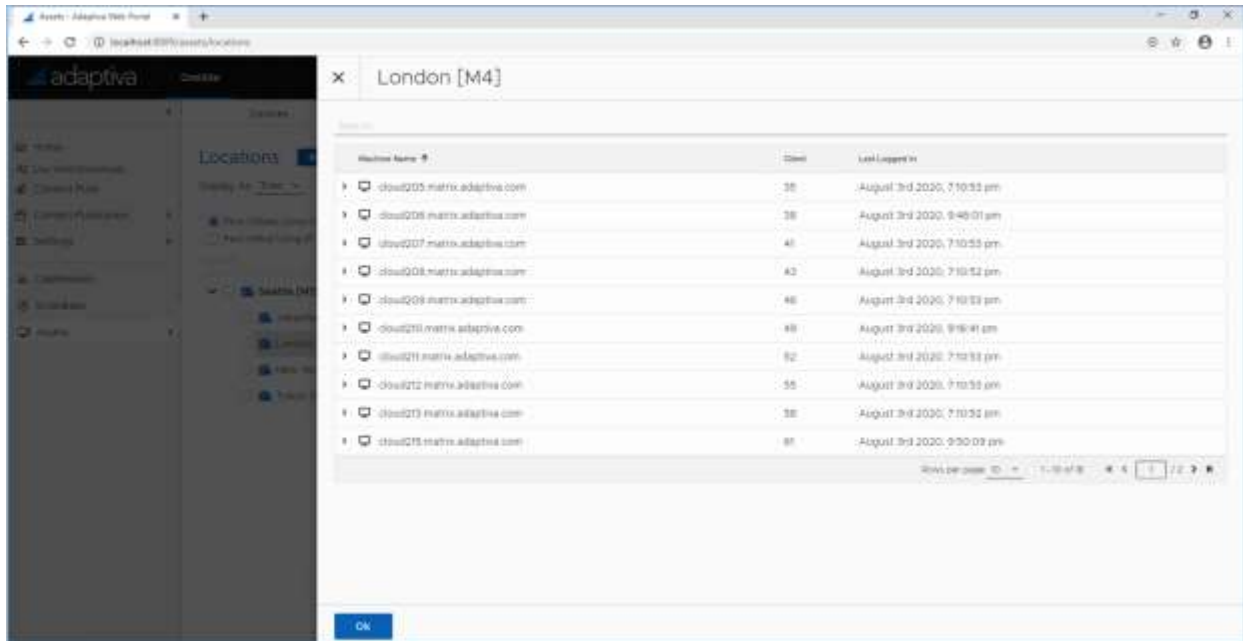
When Auto Location Creation is enabled, IP ranges can be specified that are allowed to create an Auto Location. To enable this feature, toggle the button to the right: **Restrict Auto Location Creation To The Following IP Ranges**. Check the box, **Specify Allowed Auto Location IP Ranges**, then use the **+Add Range** to add subnet ranges.



**NOTE:** If Auto Location is disabled, and clients are communicating outside of a defined location, they are considered a No Office client. A No Office client will always communicate directly to the Central Office and will not share content with other No Office clients. If this issue is detected, an office should be created with the IP range that includes the IP address of the No Office clients.

## Viewing Location Devices

To view devices which have checked into a Location: on the **Assets, Locations** page select a location.



The **Device viewer** page will be displayed to the right and will list the machine names associated within the selected Location. To display a list of No Office clients, select **Show NO OFFICE clients**.

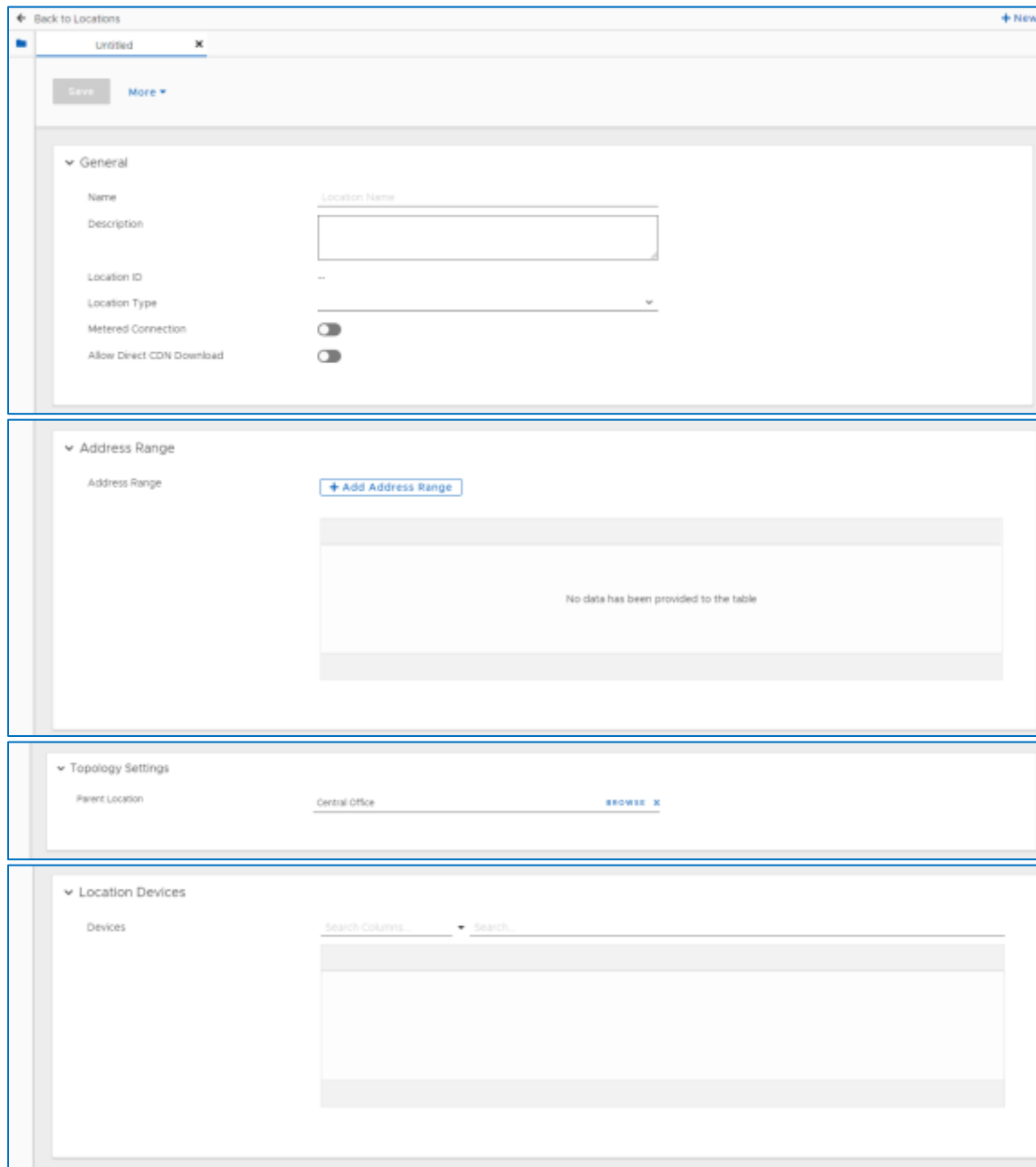
**NOTE: There is no visible Location for internet clients. They exist in a hidden Location named InternetOffice. To see those clients, select Assets, Devices and scan for devices with a Public IP value**

## Creating a Location

As mentioned earlier, the Adaptiva Server creates a default **Central Office** which consists of the subnet belonging to the IP address of the Adaptiva server. All other Locations are created as children of either the Central Office or other Locations.

To create a new Location, click on **+New**

When you have completed the entries, click on **Save**



The screenshot displays the 'Locations' configuration page in the Adaptiva web interface. The page is titled 'Untitled' and has a 'Back to Locations' link on the top left and a '+ New' link on the top right. Below the title bar, there are 'Save' and 'More' buttons. The main content area is divided into four sections:

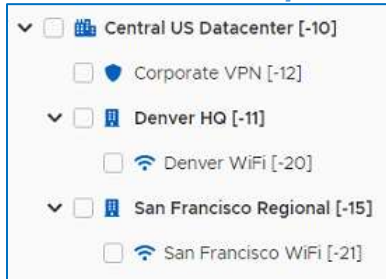
- General:** Contains fields for 'Name' (with a placeholder 'Location Name'), 'Description', 'Location ID' (showing '--'), 'Location Type' (a dropdown menu), 'Metered Connection' (a toggle switch), and 'Allow Direct CDN Download' (a toggle switch).
- Address Range:** Features an 'Add Address Range' button and a table with the message 'No data has been provided to the table'.
- Topology Settings:** Includes a 'Parent Location' dropdown menu currently set to 'Central Office' with a 'Browse' link.
- Location Devices:** Contains a search bar with 'Search Columns' and 'Search' labels, and an empty table below it.

Complete the following entries:

- **Name** – This text field allows you to specify a name for the Location
- **Description** – This text field allows you to optionally add a description for the Location.
- **Location ID** – This is assigned to the Location dynamically by the Adaptiva Server. When creating a new Location, this shows a value of --, however when saving and processing the user action, the Adaptiva Server allocates a unique ID to it.
- **Location Type** – This setting allows you to specify the type of Location which effects the behavior of how Adaptiva clients communicate within the Location. The options for this setting are as follows:
  - **Default** – Used to define a standard wired Local Area Network.

- **VPN** – Used to define a Location and IP range(s) allocated for clients connecting via VPN. Clients within a VPN Location will not attempt to share content amongst one another.
- **WiFi** – Used to define a Location and IP range(s) allocated to clients connected over Wi-Fi. Clients within a Wi-Fi Location are able to share content amongst one another but will use unicast communications rather than send broadcasts.

**NOTE: When there is a physical location that has both a wired subnet and a wireless subnet, a separate office should be created for each. The wireless office should be set to WiFi and made a child of the wired office so that content is retrieved from the parent.**

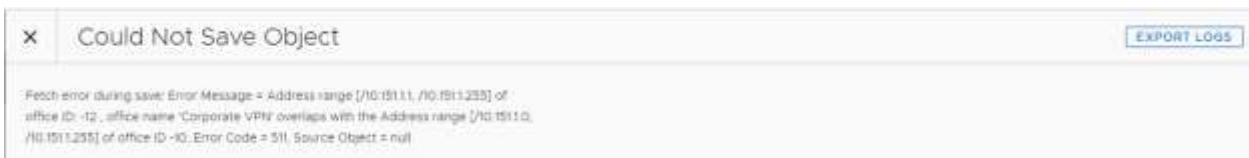


- **Metered Connection** – Used to define a Location and subnet range(s) as metered. This setting allows administrators to set policies to restrict WAN downloads from clients that are on metered connections. This policy setting can be configured within the System Configuration Perspective within the policy set: **Contentsystem / No wan download on metered connection.**
  - **Allow Direct CDN Download** – This setting, when an appropriate license is present, OneSite ConfigMgr Edition, OneSite Intune Edition or OneSite VMWare Edition licenses, allows an office to exit the hierarchy and go directly to the internet to download content. This may come from the Content Delivery Network (CDN) or from another client on the internet. Clients in this office will not be able to get content from a parent office or the Central Office *unless the content is not available on the Internet or Adaptiva CDN.*
- **Address Range** – This is a table of IP address ranges, denoted by starting IP address and ending IP address. Click **+ Add Address Range** to add a new address range.

Click **OK** when complete

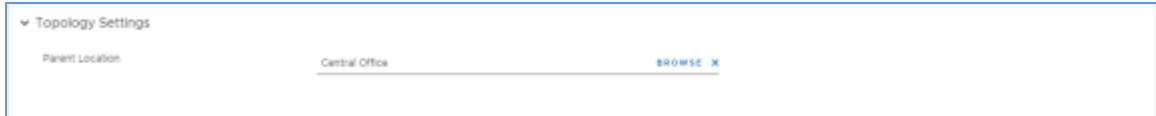
Using the ellipses, ..., at the far right under **Actions** will allow the entry to be **Updated** or **Removed**

**NOTE: If the subnet range entered overlaps a range from another Location, an error will occur when clicking Save and the Location will not be saved.**



- **Topology Settings** – This allows you place the new Location in the hierarchy.



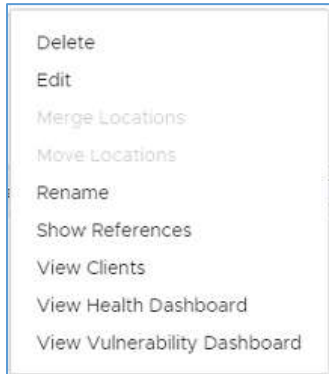


On the **Parent Location** line, select **Browse** to select the Parent location

- **Location Devices** – When you are editing an existing Location, this will show the clients that are associated with that location.

## Editing/Renaming/Moving a Location

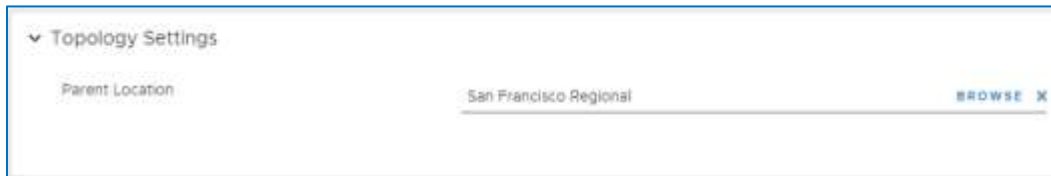
When you hover the mouse over a Location, or check the box next to its name, on the far right will be an ellipsis, ..., in the Actions column. Click the ellipses, ..., to view a context menu:



Selecting **Edit** from the context menu will let you change various settings for the Location. Please note that you cannot change the Location ID, which is the object ID in the database and was generated upon creation.

The Location name can be renamed.

The Parent Location can be changed to move the Location within the hierarchy.



To move the location, click on **Browse** and check the box next to the new parent location and click on **Add To List**. A new Location can be created by clicking on **+Create Server Object**

## Deleting a Location

Selecting **Delete** from the Action menu will allow you to delete the selected Location. Once a Location is deleted, the IP range(s) defined within the Location are also deleted. Any clients which were reporting from the Location will become **No Office** clients if Auto-Office creation is turned off or a new Office will be auto-created the next time the client checks in if Auto-Office creation is turned on.

**IMPORTANT: ALL child locations of this Location will ALSO be deleted**

## Merging a Location

To enable the Merge Locations Action item you must check the box on the left-hand side of the table.

Selecting **Merge Locations** from the context menu will prompt for which Location to merge the IP Address Ranges of the selected Location into. The Location type (Default, VPN, WiFi) will remain as that of the target Location.

## Move a Location

To enable the Move Locations Action item you must check the box on the left-hand side of the table.

Selecting **Move Locations** from the Action menu will prompt for which Location to be the new Parent Location of the selected Location. Alternatively, when in Tree view, drag and drop a location onto a new parent in the hierarchy.

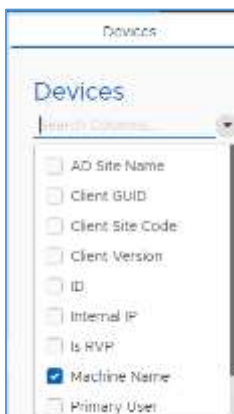
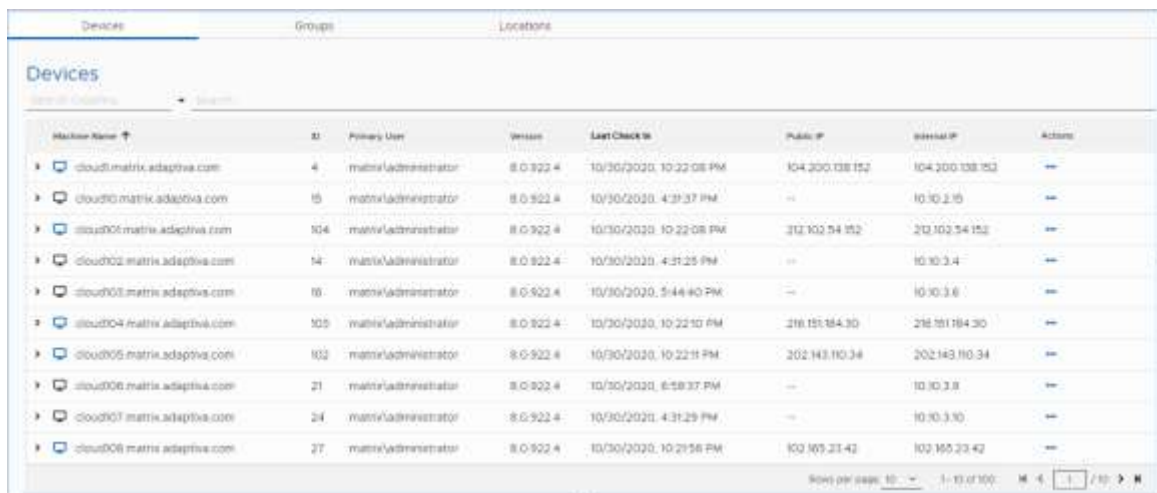
## Client Management in the Web Portal

### How to Search for and Manage Adaptiva Clients

Select **Assets, Devices** to view all Adaptiva clients reporting into the Adaptiva Server.

- There is a Search bar that can be used to search Device list

Select the Search Columns drop down and select what to search. Then enter the value to search for in the Search... box

Machine Name ↑	ID	Primary User	Version	Last Check In	Public IP	Internal IP	Actions
cloud1.matrix.adaptiva.com	4	matrix/administrator	8.0.922.4	10/30/2020, 10:22:08 PM	104.200.138.152	104.200.138.152	...
cloud10.matrix.adaptiva.com	15	matrix/administrator	8.0.922.4	10/30/2020, 4:31:37 PM	--	10.30.2.15	...
cloud101.matrix.adaptiva.com	104	matrix/administrator	8.0.922.4	10/30/2020, 10:22:08 PM	312.102.54.152	312.102.54.152	...
cloud102.matrix.adaptiva.com	14	matrix/administrator	8.0.922.4	10/30/2020, 4:31:25 PM	--	10.30.3.4	...
cloud103.matrix.adaptiva.com	16	matrix/administrator	8.0.922.4	10/30/2020, 5:44:40 PM	--	10.30.3.6	...
cloud104.matrix.adaptiva.com	105	matrix/administrator	8.0.922.4	10/30/2020, 10:22:10 PM	218.151.184.30	218.151.184.30	...
cloud105.matrix.adaptiva.com	102	matrix/administrator	8.0.922.4	10/30/2020, 10:22:11 PM	202.143.110.34	202.143.110.34	...
cloud106.matrix.adaptiva.com	21	matrix/administrator	8.0.922.4	10/30/2020, 6:58:37 PM	--	10.30.3.8	...
cloud107.matrix.adaptiva.com	24	matrix/administrator	8.0.922.4	10/30/2020, 4:31:29 PM	--	10.30.3.10	...
cloud108.matrix.adaptiva.com	27	matrix/administrator	8.0.922.4	10/30/2020, 10:21:58 PM	102.169.21.42	102.169.21.42	...

- The list can be sorted by clicking on the column header (columns Last Check In and Public IP are not sortable)
- To view additional information about a specific Device, client on the > next to the device name. This will expand the line to show the Client ID and Version
- When an Adaptiva client is no longer valid, select the ellipses, ..., under the **Actions** column and select **Remove Device** to remove the device from the Adaptiva database. This is useful when a machine is reimaged, the name is changed, and the record of the old client is still listed. By

default, inactive client records are purged after 21 days, but until the purge occurs the old record will consume a license.

Device Name	Last Check-in	IP Address	Actions
cloud1.matrix.adaptiva.com	8/4/2020, 12:12:54 AM	104.200.136.152	...
cloud10.matrix.adaptiva.com	8/4/2020, 12:04:03 AM	10.10.2.15	Remove Device
cloud101.matrix.adaptiva.com	8/4/2020, 12:13:50 AM	212.102.54.152	...
cloud102.matrix.adaptiva.com	8/4/2020, 12:04:03 AM	10.10.3.4	...

## How to View Clients Reporting from a Specific Location

1. In **Assets, Locations**, click any location.
2. The Device Viewer will open showing the list of machine names associated at the Location. The devices can be sorted by clicking the column header (columns Last Logged In and Public IP are not sortable)

× Johannesburg [M6] Clients

Showing Clients for Johannesburg [M6]

Search Columns: + Search

Machine Name	ID	Primary User	Version	Last Check-in	Public IP	Internal IP
cloud425.matrix.adaptiva.com	12	matrix/administrator	8.0.922.4	10/30/2020, 4:31:24 PM	--	10.10.6.17
cloud424.matrix.adaptiva.com	101	matrix/administrator	8.0.922.4	10/30/2020, 6:41:40 PM	--	10.10.6.36
cloud423.matrix.adaptiva.com	100	matrix/administrator	8.0.922.4	10/30/2020, 4:31:45 PM	--	10.10.6.35
cloud422.matrix.adaptiva.com	99	matrix/administrator	8.0.922.4	10/30/2020, 8:36:06 PM	--	10.10.6.34
cloud421.matrix.adaptiva.com	98	matrix/administrator	8.0.922.4	10/30/2020, 4:31:25 PM	--	10.10.6.33
cloud420.matrix.adaptiva.com	87	matrix/administrator	8.0.922.4	10/30/2020, 6:30:31 PM	--	10.10.6.31
cloud419.matrix.adaptiva.com	96	matrix/administrator	8.0.922.4	10/30/2020, 10:28:40 PM	--	10.10.6.32
cloud418.matrix.adaptiva.com	95	matrix/administrator	8.0.922.4	10/30/2020, 8:24:57 PM	--	10.10.6.30
cloud416.matrix.adaptiva.com	83	matrix/administrator	8.0.922.4	10/30/2020, 4:31:29 PM	--	10.10.6.28
cloud415.matrix.adaptiva.com	82	matrix/administrator	8.0.922.4	10/30/2020, 4:31:17 PM	--	10.10.6.27

Rows per page: 10 | 1 - 10 of 18 | ⏪ 1 / 2 ⏩

OK

Click **OK** at the bottom, or the **X** at the top to return to the list of locations

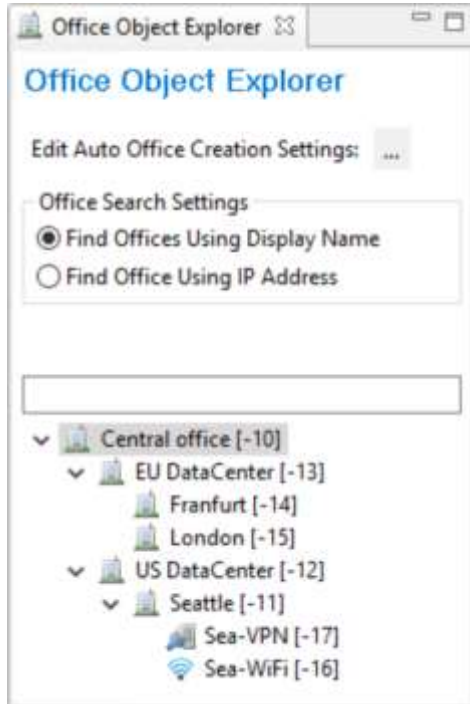
3. One important reason to visit this view is to determine which Adaptiva client is functioning as the **RVP** on a given subnet. The RVP, or RendezVous Point, can be identified by the blue computer icon

cloud422.matrix.adaptiva.com	99	August 4th 2020, 12:22:39 am
cloud423.matrix.adaptiva.com	100	August 4th 2020, 12:04:23 am
cloud424.matrix.adaptiva.com	101	August 4th 2020, 12:04:23 am
cloud425.matrix.adaptiva.com	12	August 4th 2020, 12:04:03 am

## Using the Adaptiva Workbench

### Overview

The **Office Object Explorer**, available in the **Network Topology Perspective**, allows an administrator to create and view the office hierarchy structure of the computers in their organization.



The Office Object Explorer allows the Administrator to:

- View the hierarchical representation of all offices in the system
- Create a new child office under an existing office
- Merge one office with another
- Delete an existing office
- View an office
- Edit an office
- Move an office from one place in the hierarchy to another
- Set Office Type to Default, VPN, or WiFi and other settings

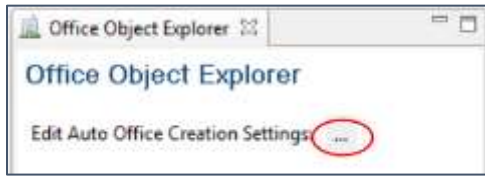
### Search Bar

The Office Object Explorer has a convenient search bar which allows you to search for offices that have been created. Directly above the search box there is the ability to search by Display Name or IP Address.

### Auto Office Creation Settings

When an Adaptiva client registers with the server for the first time, the server looks for an existing office with an IP range that fits that client. If such an office does not exist, the server can automatically create an office using the IP address and subnet mask provided by the client. This is the purpose of the **Auto Office Creation** feature in the Network Topology perspective.

By default, Auto Office Creation is enabled. Click the ellipses, ..., to change Auto Office Creation settings.



In the **Auto Office Creation Settings Editor**, Auto Office Creation can be turned **ON** or **OFF**. This can be useful when manually reorganizing subnets to different offices and not wanting them Auto-created when a client on that subnet communicates with the server.

### Allowed Auto Office IP Address Ranges

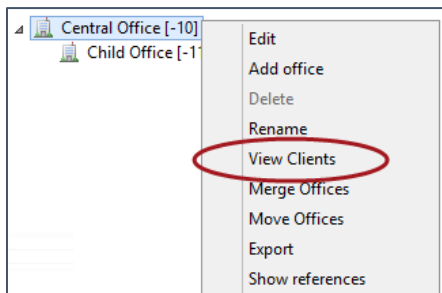
When Auto Office is enabled, IP ranges can be specified that are allowed to create an Auto Office. To enable this feature, check the box: **Restrict Auto Office Creation To The Following IP Address Ranges**. Check the box, **Specify Allowed Auto Office Ranges**, then use the **Add**, **Edit**, or **Remove** buttons to manage the allowed subnet ranges.



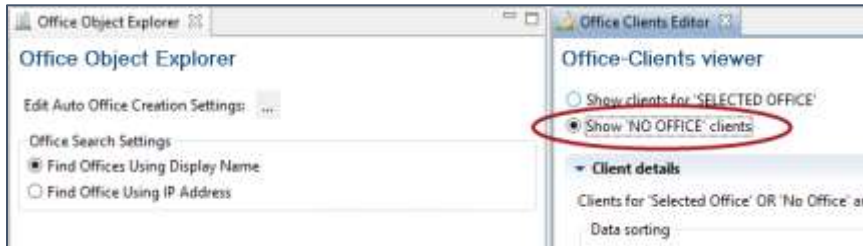
**NOTE:** If Auto Office is turned OFF, and clients are communicating outside of a defined office, they are considered a No Office client. A No Office client will always communicate directly to the Central Office and will not share content with other No Office clients. If this issue is detected, an office should be created with the IP range that includes the IP address of the No Office clients.

### Viewing Office Clients

To view machines which have checked into an office, or to check if there are any No Office clients, in the **Office Object Explorer** right-click an office and select **View Clients**.



The **Office-Clients viewer** will be displayed to the right and will list the clients located within the selected office. To display a list of No Office clients, select **Show 'NO OFFICE' clients**.

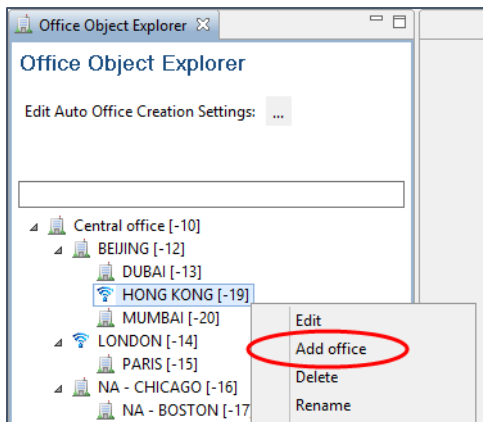


**NOTE:** *There is no visible Office for internet clients. They exist in a hidden Office named InternetOffice.*

## Creating an Office

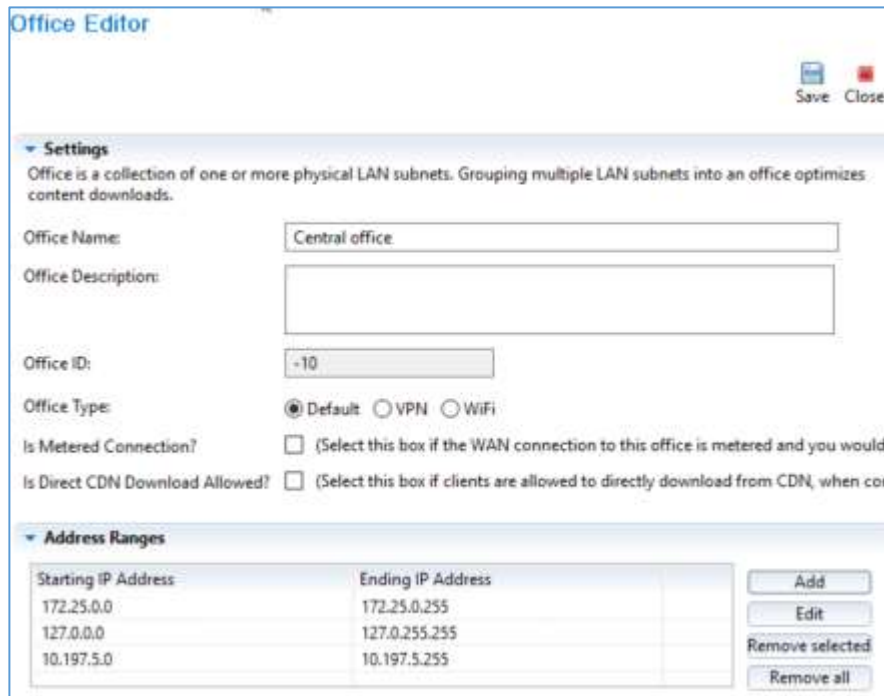
As mentioned earlier, the Adaptiva Server creates a default **Central Office** which consists of the subnet containing to the IP address of the Adaptiva server. All other offices are created as children of either this office or other offices.

To create a new office as the child of a particular office, right-click the parent office and select **Add Office**. This will open the **Office Object Editor**.



## Office Object Editor

The Office Object Editor allows the administrator to set parameters which define the particular office.



The screenshot shows the 'Office Editor' window with the following fields and options:

- Settings:**
  - Office Name: Central office
  - Office Description: (empty text area)
  - Office ID: -10
  - Office Type:  Default  VPN  WiFi
  - Is Metered Connection?  (Select this box if the WAN connection to this office is metered and you would like to limit bandwidth for this office.)
  - Is Direct CDN Download Allowed?  (Select this box if clients are allowed to directly download from CDN, when content is available.)
- Address Ranges:**

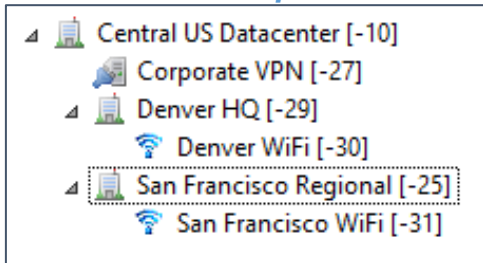
Starting IP Address	Ending IP Address
172.25.0.0	172.25.0.255
127.0.0.0	127.0.255.255
10.197.5.0	10.197.5.255

Buttons: Add, Edit, Remove selected, Remove all

### Settings:

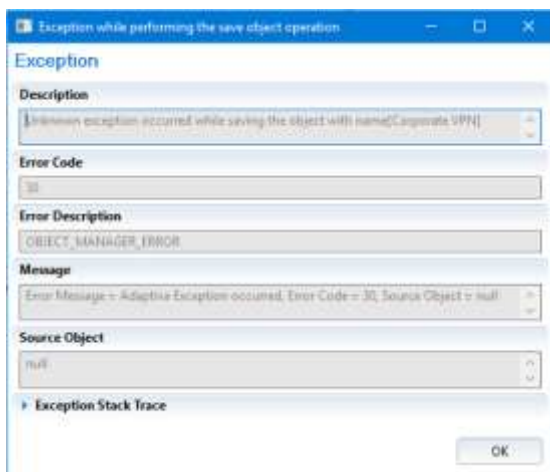
- **Office Name** – This text field allows you to specify a name for the office
- **Office Description** – This text field allows you to optionally add a description for the office.
- **Office ID** – This is assigned to the office dynamically by the Adaptiva Server. When creating a new office, this shows a value of 0, however, upon saving the new Office, the Adaptiva Server allocates a unique ID to it.
- **Office Type** – This setting allows you to specify the type of office which effects the behavior of how Adaptiva clients communicate within the office. The options for this setting are as follows:
  - **Default** – Used to define a standard wired Local Area Network.
  - **VPN** – Used to define an office and IP range(s) allocated for clients connecting via VPN. Clients within a VPN office will not attempt to share content amongst one another.
  - **WiFi** – Used to define an office and IP range(s) allocated to clients connected over Wi-Fi. Clients within a Wi-Fi office are able to share content amongst one another but will use unicast communications rather than sending broadcasts.

**NOTE:** When there is a physical location that has both a wired subnet and a wireless subnet, a separate office should be created for each. The wireless office should be set to WiFi and made a child of the wired office so that content is retrieved from the parent.



- **Is Metered Connection?** – Used to define an office and subnet range(s) as metered. This setting allows administrators to set policies to restrict WAN downloads from clients that are on metered connections. This policy setting can be configured within the System Configuration Perspective within the policy set: **Contentsystem / No wan download on metered connection**.
- **Is Direct CDN Download Allowed?** – This setting, when an appropriate license is present, OneSite ConfigMgr Edition, OneSite Intune Edition or OneSite VMWare Edition licenses, allows an office to exit the hierarchy and go directly to the internet to download content. This may come from the Content Delivery Network (CDN) or from another client on the internet. Client in this office will not be able to get content from a parent office or the Central Office.
- **Address Ranges** – This is a table of IP address ranges, denoted by starting IP address and ending IP address. The buttons to the right of the frame allow you to **Add**, **Edit**, **Remove selected** or **Remove all** table entries. If the subnet range overlaps a range from another office, an error will occur upon clicking Save and the office will not be saved.

**NOTE:** If the subnet range entered overlaps a range from another Office, an error will occur when clicking Save and the Office will not be saved.



## Editing an Office

Right-clicking an office and selecting **Edit**, or double-clicking, will allow various settings to be changed for the office via the **Office Object Editor**. Please note that the Office ID cannot be changed. This is the object ID in the database and is generated upon creation.



## Renaming an Office

Right-clicking an office and selecting **Rename** will allow the selected office to be renamed. This is a convenience provided for the administrator and this action is also possible through the Edit Office selection (via the Office Object Editor).

## Deleting an Office

Right-clicking an office and selecting **Delete** will delete the selected office. Once an office is deleted, the IP range(s) defined within the office are also deleted. Any clients which were reporting from the office will become **No Office** clients if Auto-Office creation is turned off or a new Office will be auto-created the next time the client checks in if Auto-Office creation is turned on.

**IMPORTANT: ALL Child Locations of this Location will ALSO be deleted**

## Merging an Office

Right-clicking an office and selecting **Merge Offices** will bring up the **Office Object Explorer** to select another office to merge into. The subnets in both offices will be combined into the target office and the office type (Default, VPN, WiFi) will remain as that of the target office.

## Moving an Office

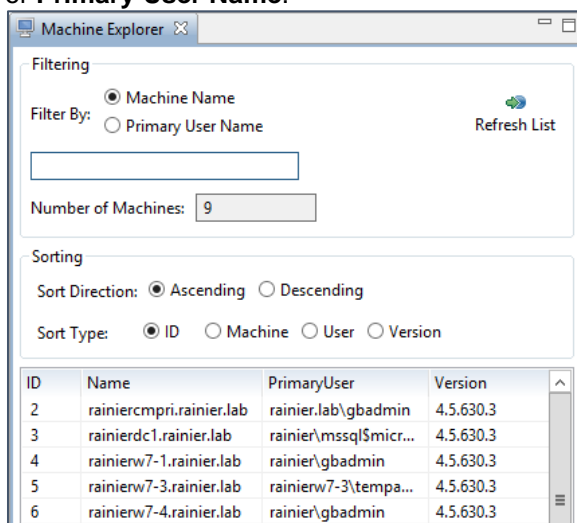
Right-clicking an office and selecting **Move Offices** will bring up the **Office Object Explorer** to choose another office to make as the parent. Alternatively, drag and drop an office onto a new parent in the hierarchy.

## Client Management in the Network Topology Perspective

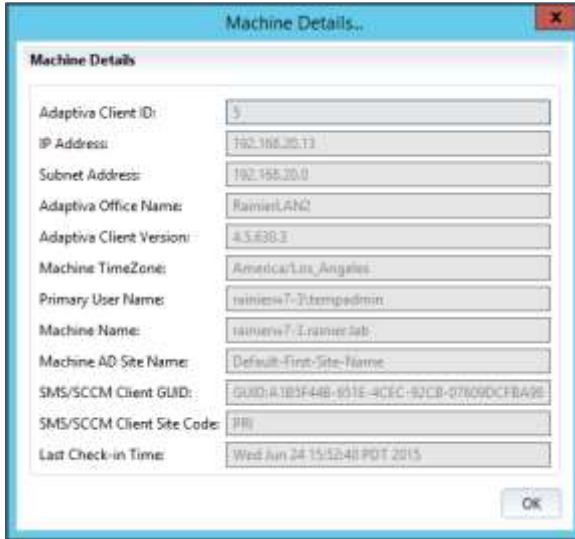
Customizing the Network Topology Perspective to optimize content flow within an organization is critical for a successful Adaptiva implementation, but the Network Topology perspective also provides the ability to search for clients, view all clients, view clients within a specific office location, or delete clients.

### How to Search for and Manage Adaptiva Clients

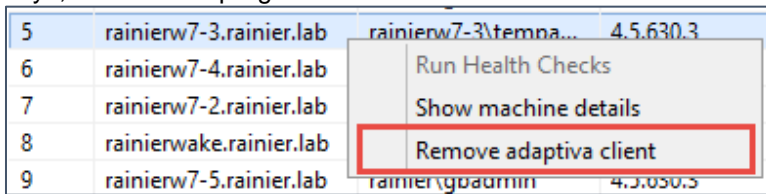
- ❑ The **Machine Explorer** view, in the **Network Topology Perspective**, allows all Adaptiva clients reporting into the Adaptiva Server to be viewed.
- ❑ In the **Machine Explorer** view, use the Filtering options to search for clients by **Machine Name** or **Primary User Name**.



- ❑ To view additional information about a specific client, right-click the client, and in the context menu, select **Show machine details** which will display the **Machine Details** dialog.

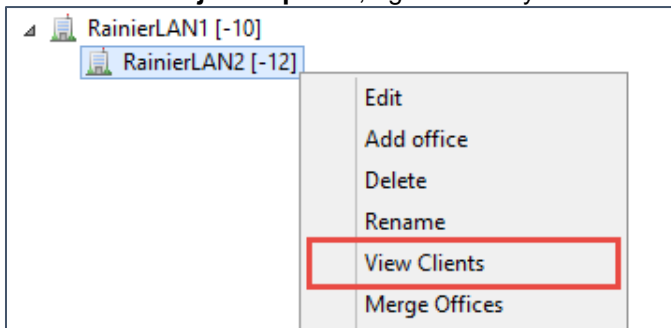


- ❑ When an Adaptiva client is no longer valid, right-click the client in the **Machine Explorer** and in the context menu select **Remove adaptiva client** to remove client from the Adaptiva database. This is useful when a machine is reimaged, and the name is changed and the record of the old client is still showing in the workbench. By default, inactive client records are purged after 21 days, but until the purge occurs the old record will consume a license.

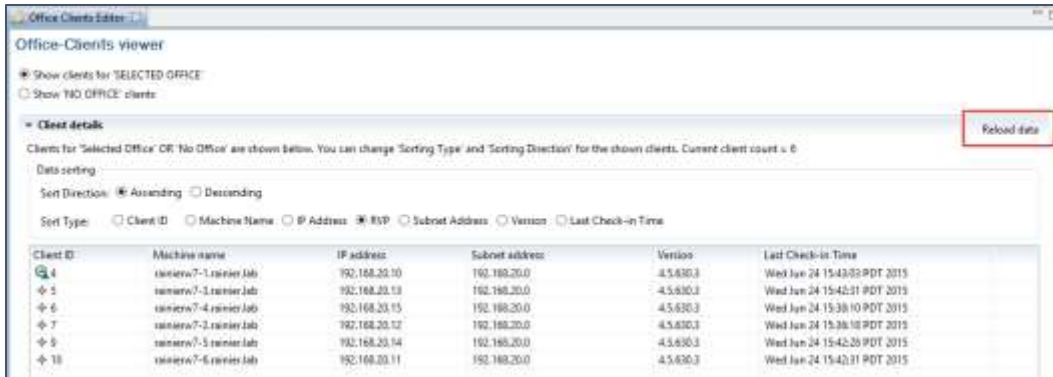


### How to View Clients Reporting from a Specific Office

- ❑ In the **Office Object Explorer**, right-click any office and in the context menu select **View Clients**.



- ❑ The **Office-Clients** viewer will open where you will see the list of machines located within the office. The clients can be sorted via various columns. At any time, click **Reload data** to refresh the view.



- ❑ One important reason to visit this view is to determine which Adaptiva client is functioning as the **RVP** on a given subnet. The RVP, or RendezVus Point, can be identified by the green icon with the blue triangle.

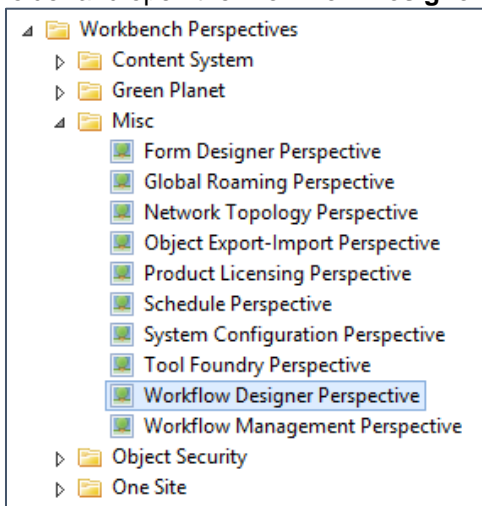
## Importing the Network Topology Information

To simplify the process of defining a complete Network Topology with office names, IP ranges, types, and hierarchy, there is an option to import this information using a spreadsheet. A sample spreadsheet is included in the OneSite product download and is named: **Sample-Input-Network-Topology-Import-Workflow.xlsx**.

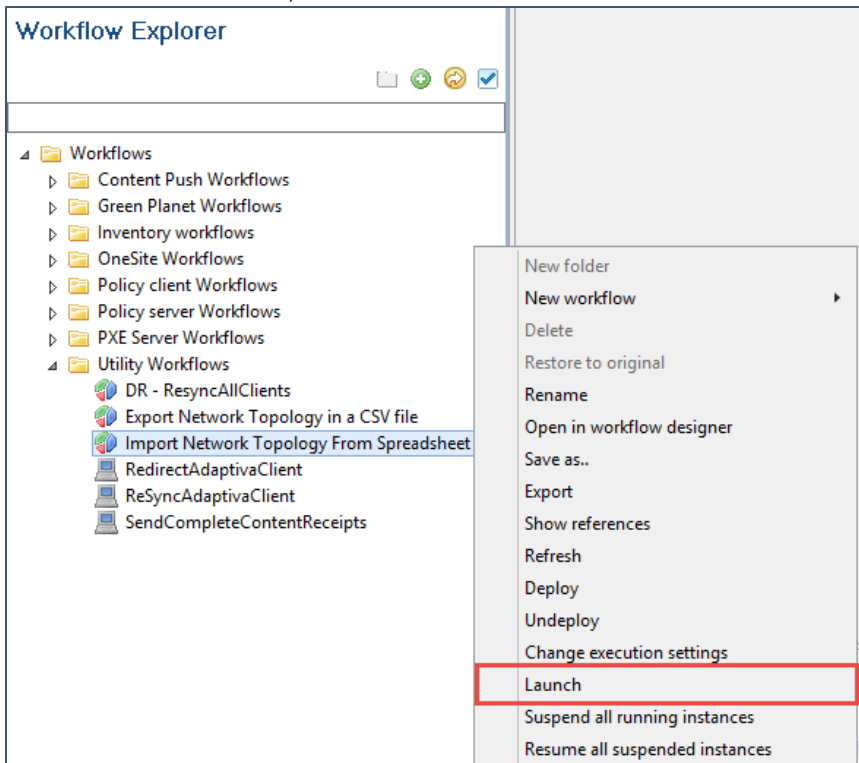
To import a Network Topology using a spreadsheet:

This is only available in the workbench

- ❑ Modify the sample spreadsheet and store it on the Adaptiva server. In this example, the file name will be C:\Adaptiva\NetworkTopology.xlsx.
- ❑ Open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **Misc** folder and open the **Workflow Designer Perspective**.



- ❑ In the **Workflow Designer Perspective**, in the **Workflow Explorer** pane, expand the **Utility Workflows** folder then right-click the **Import Network Topology From Spreadsheet** workflow and in the context menu, select **Launch**.



- ❑ The **Network Topology Generator – From Excel** form should open where the administrator should modify the fields to accommodate the data in the network topology spreadsheet.

- **Excel File Location** – Enter the path and filename for the .XLSX file which contains the network topology.
- **Initial Header Rows** – Enter the number of rows which should be ignored. Typically, this is only the first row that is used for column headers in the Excel file.
- **Office Name and Description** – Enter the column number that contains the office name and description that will be populated for each office in the Network Topology Perspective. Optionally, select the checkbox to include the IP address range for each office in the office description.

**IMPORTANT:** The row in the spreadsheet which represents the name of the Central office should match exactly what is in the Network Topology Perspective or a child office will be created.

- **Office Hierarchy** – Enter the column number which contains the name of the parent office. If it is possible that the import results in empty offices, it would be a good idea to select the checkbox **Automatically Delete Empty Offices Which Don't Have Child Offices**.
  - **IP Address Information** – First, select the layout of the spreadsheet from the three choices. Spreadsheet contains IP Address Ranges, Spreadsheet contains Subnet Addresses and subnet masks, or Spreadsheet contain CIDR. Next, enter the column numbers which contain the information for each of the items.
  - **Office Type Settings** – Enter the column numbers which contain VPN, WiFi, and Metered information.
- ❑ Once complete, click **OK** to begin the import. Depending on the amount of data, the import may take time. Open the Network Topology Perspective to view your changes.

**TIP:** After importing a Network Topology from a spreadsheet, it is recommended that you review the logs for overlapping ranges that may have been removed

*from an office in favor of another due to the same range being incorrectly identified in the spreadsheet or associated with more than one office. The log can be found in <AdaptivaServerInstallPath>\Logs\Workflowlogs. The log file name will start with Import Network Topology From Spreadsheet. When you open the log, simply search for Removed Overlapping Range to identify which offices and ranges require follow up.*

# Configuring OneSite Anywhere

Most of the following activities only need to be completed once.

## Upgrading to use OneSite Anywhere

If upgrading the existing Adaptiva environment to be able to use the Web Portal, or have clients access the Adaptiva Cloud Relay Service, a OneSite Anywhere Product license key must be added. (This will be shown as OneSite ConfigMgr Edition). This can be obtained from your Adaptiva Sales Representative.

See the **Licensing Adaptiva** section for more information on how to add a Product Key.

The Adaptiva Server must be activated to allow Adaptiva clients to communicate with the Adaptiva server via the Adaptiva Cloud Relay Services. See the **Server Activation** section in the Adaptiva Installation Guide.

## Publish Content to the CDN-based Content Library

If this is an existing environment where the Adaptiva ConfigMgr Edition license has just been enabled, refer to sections listed below to publish content to the CDN:

### Using the Adaptiva Web Portal

Solution	Section Reference
Configuration Manager	<a href="#">Content Publication Settings for each Content Type and Priority</a>
Intune	Intune Content -> <a href="#">Using the Adaptiva Web Portal</a>
Adaptiva	Adaptiva Content -> <a href="#">Using the Adaptiva Web Portal</a>

### Using the Adaptiva Workbench

Solution	Section Reference
Configuration Manager	<a href="#">Content Publication Settings for each Content Type and Priority</a>
Intune	Intune Content -> <a href="#">Using the Adaptiva Workbench</a>
Adaptiva	Adaptiva Content -> <a href="#">Using the Adaptiva Workbench</a>

## (Optional) Manage Client Authorization

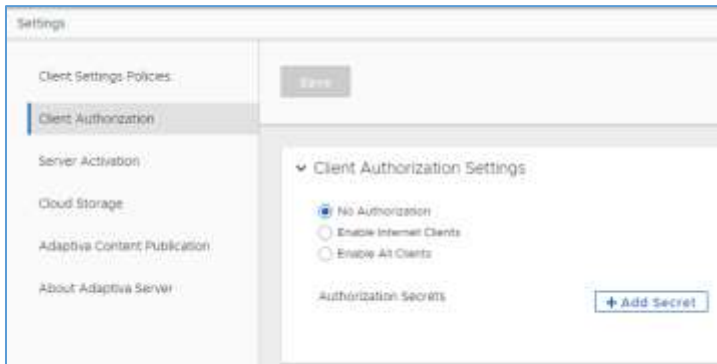
**Client Authorization** can be used to additionally protect Adaptiva client installations that are completed over the internet, when the client cannot communicate with the Adaptiva Server, but can communicate with the Adaptiva Cloud Relay Services at <http://services.adaptiva.cloud>.

When an Authorization Secret is created, a new client installation must include that Authorization Secret or password. A password is entered during the Adaptiva Client installation that ensures only clients with valid passwords can be registered with the Adaptiva Server.

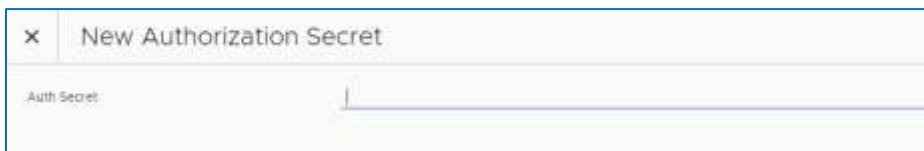
Authorization Secrets can be created and removed at any time. When removed, be sure to update any command lines that included the secret.

## Using the Adaptiva Web Portal

1. In , **Settings** ([http\[s\]://AdaptivaServerFQDN\[:port\]/settings](http[s]://AdaptivaServerFQDN[:port]/settings))
2. Select **Client Authorization**



3. Determine which client installations will require a password: **Internet Clients** registering through the Adaptiva Cloud Relay Service or **All Clients**
4. Click on **+ Add Secret**



5. Enter a password/Authorization Secret and click **OK**
6. To remove an Authorization Secret, click on the x to the right of the secret



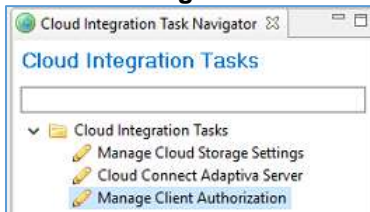
7. Click on **Save**
8. Use this password/Authorization Secret when manually installing the client or as part of the command line

**NOTE: A password is not required when upgrading clients to the latest version. They are already registered with the Adaptiva server and have received the secure tokens to connect and exchange information.**

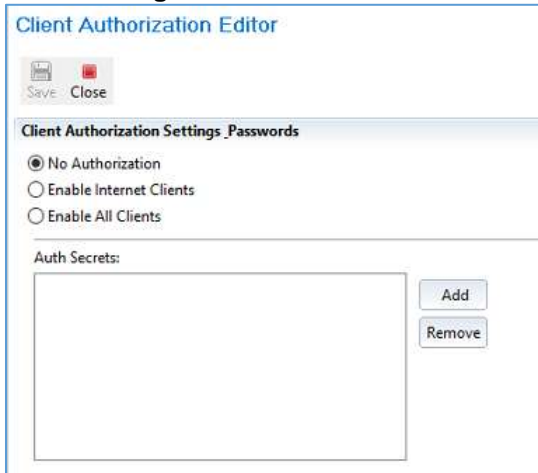


## Using the Adaptiva Workbench

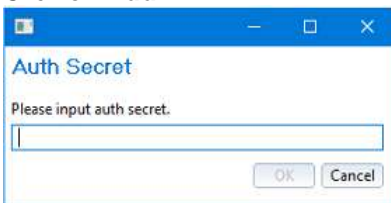
1. In the Adaptiva Workbench, expand **Misc** and select **Cloud Integrations Perspective** to open the **Cloud Integration Tasks**



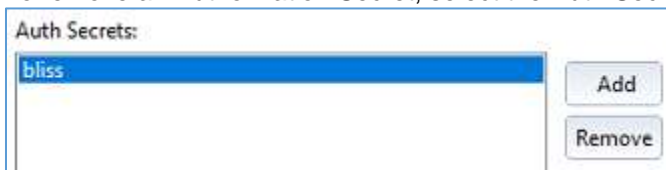
2. Select **Manage Client Authorization**



3. Determine which client installations will require a password: **Internet Clients** registering through the Adaptiva Cloud Relay service or **All Clients**
4. Click on **Add**



5. Enter a password and click **OK**
6. To remove an Authorization Secret, select the Auth Secret and click **Remove**



7. Click on **Save**
8. Use this password/Authorization Secret when manually installing the client or as part of the command line

**NOTE:** A password is not required when upgrading clients to the latest version. They are already registered with the Adaptiva server and have received the secure tokens to connect and exchange information.

# Configuring OneSite for Intune

## Using the Adaptiva Web Portal

App Registration, which allows the Adaptiva Server service to authenticate against your Azure Active Directory, must be completed prior to creating and deploying content using Adaptiva OneSite for Intune. To Create the App Registration, reference the **App Registration** sub-section in the **Installation Prerequisites** section of the **Adaptiva Installation Guide**. To Configure Adaptiva OneSite to use the App Registration reference the **(Optional) Post Installation Tasks** sub-section in the **Server Installation** section of the **Adaptiva Installation Guide**.

## Using the Adaptiva Workbench

Automation does not occur when using the Adaptiva Workbench. The app to deploy would need to be created in the workbench AND created again in Intune using the P2P App generated by the workbench. Thus, it is not recommended to use the Adaptiva Workbench to create apps for deployment with Intune. Use the Adaptiva Web Portal.

The App Registration must be created before this section can be completed. See the section App Registration in the Adaptiva Installation Guide.

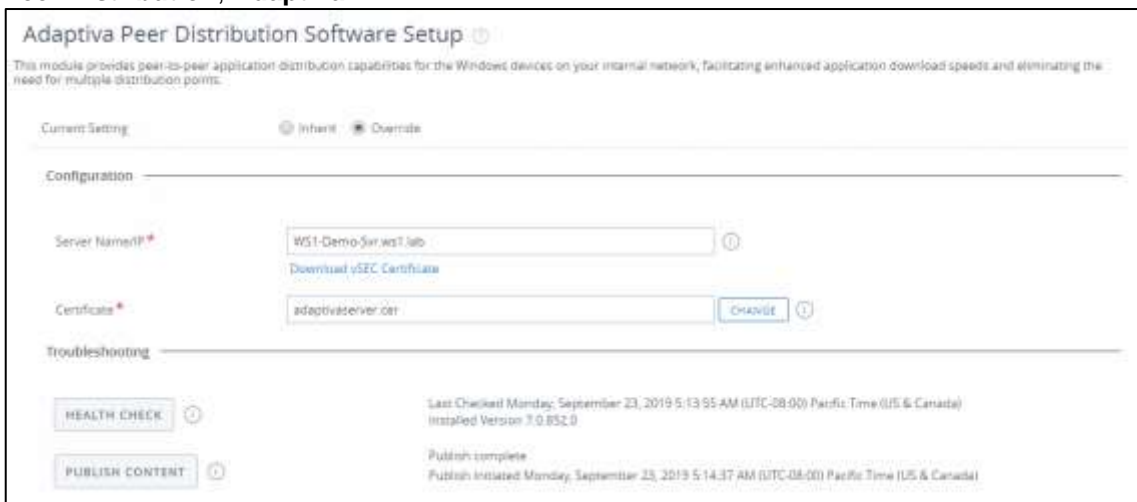
# Configuring OneSite for VMware

## Health Check

The integration between Adaptiva and Workspace ONE was handled as part of the installation – see the Adaptiva Installation Guide. This integration can be confirmed by running a Health Check to ensure Workspace ONE UEM is able to recognize and communicate with Adaptiva.

**NOTE: This next process can only be done at the level where the Adaptiva connection was created**

1. Open a web browser and connect to <https://cn800.airwatchportals.com>
2. Log in with your UEM account
3. Browse to **Groups and Settings, All Settings**, under **System**, select **Enterprise Integration, Peer Distribution, Adaptiva**



**Adaptiva Peer Distribution Software Setup**

This module provides peer-to-peer application distribution capabilities for the Windows devices on your internal network, facilitating enhanced application download speeds and eliminating the need for multiple distribution points.

Current Setting:  Inherit  Override

**Configuration**

Server Name:  Download vSEC Certificate

Certificate:  Change

**Troubleshooting**

**HEALTH CHECK** ? Last Checked: Monday, September 23, 2019 5:13:55 AM (UTC-08:00) Pacific Time (US & Canada)  
Installed Version: 7.0.852.0

**PUBLISH CONTENT** ? Publish complete  
Publish Initiated: Monday, September 23, 2019 5:14:37 AM (UTC-08:00) Pacific Time (US & Canada)

4. Click on **Health Check**  
If the Health Check button is not there, then you are in a child Organization Group. The Health Check is only available in the Organization Group where the connection to Adaptiva was created
5. The Health Check will return the results




✓ Health Check  
 Minimum Supported Server Version - 6.0.758.0  
 Last Checked - Wednesday, April 22, 2020 4:04:09 AM (UTC-08:00) Pacific Time (US & Canada)  
 Installed Version - 7.0.852.0

6. Click on the X in top right corner to return to the Groups & Settings page

# Content Publication Settings

Content Publication Settings control how content is published. There are four different sources of content and places to publish this content. Content can be published on the Adaptiva Server or on the CDN (Cloud store) or both places.

**NOTE: VMWare Workspace ONE content is only published on their Content Delivery Network and will not be in the Adaptiva Content Library on the Adaptiva server or Cloud store. The Adaptiva Server will receive metadata information so clients can locate the content.**

Content Source	Adaptiva Web Portal	Adaptiva Workbench
Configuration Manager	OneSite Anywhere, OneSite ConfigMgr Edition. Select Settings, Publication  Select each content type:  Packages, Software Updates, Boot Images, OS Images, OS Update Packages, Driver Packages, Applications	OneSite, One Site – Package Perspective, Default <contenttype> Settings, Edit <priority> <contenttype> Settings, <contenttype> Publication Settings tab  where <contenttype> is:  Package, Software Update, Boot Image, Operating System Image, Operating System Update Package, Driver Package, Application Package and <priority> is High, Medium or Low
Adaptiva	 Settings, Adaptiva Content Publication	Content Management, Adaptiva Content Publication Perspective, Manage System Content Publication Settings
Intune	OneSite Anywhere, OneSite Intune Edition. Select Intune Settings, Cloud Content Settings	OneSite Intune, OneSite for Intune, Manage Application Content Publication Settings
VMWare	Not Applicable – content is published on the VMWare CDN	Not Applicable – content is published on the VMWare CDN

Use the sections below to configure where Adaptiva will store content

**IMPORTANT: The section Connecting to Azure Storage in the Installation Guide MUST have been completed first.**

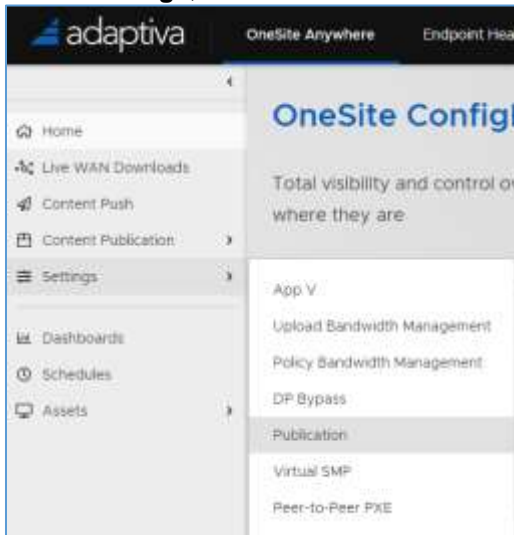
## ConfigMgr Content

It would be tedious to publish every content item manually. Most organizations will enable **Automatic Content Publication** so that when new ConfigMgr objects are created that have associated content, Adaptiva will detect and automatically publish the associated content. When a content item (package, software update, etc.) is created in ConfigMgr it will be created with the default distribution priority setting of Medium, but the priority can be set to High, Medium, or Low. The administrator can configure OneSite to automatically apply different settings for different priorities for each content type.

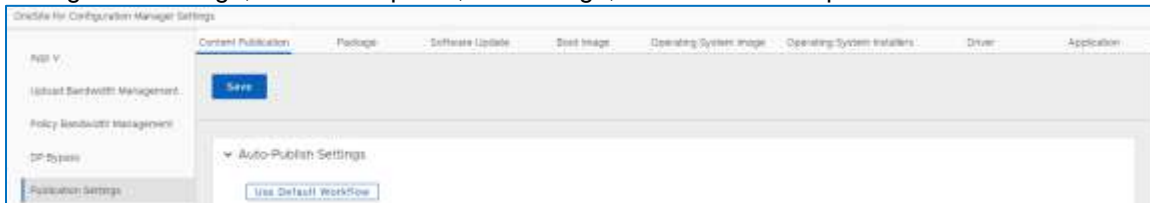
## Using the Adaptiva Web Portal

### Automatic Content Publication of ConfigMgr Content

1. Connect to the Adaptiva Web Portal using a web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Go to OneSite ConfigMgr Edition** or click **OneSite Anywhere, OneSite ConfigMgr Edition**
4. Select **Settings, Publication**



5. This will open, by default, into the **Content Publication** settings. Notice, there are additional settings for Package, Software Update, Boot Image, etc. across the top



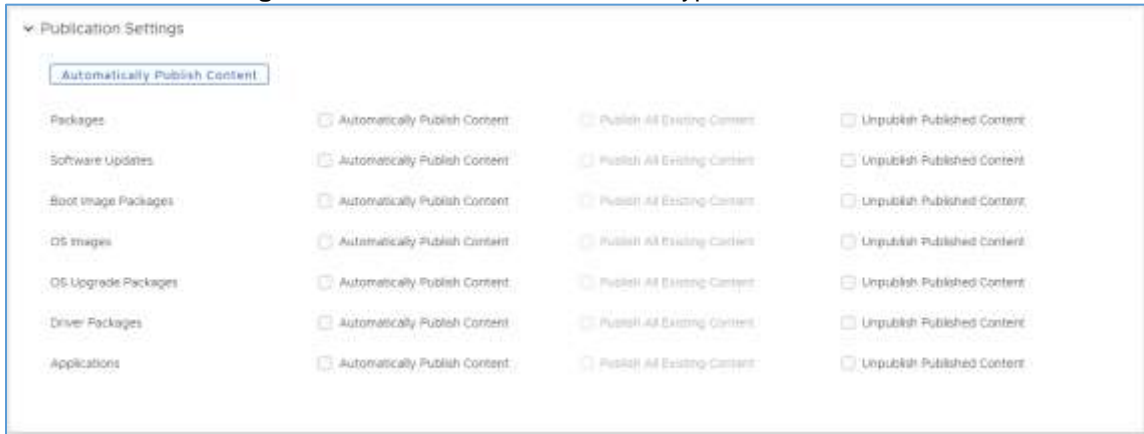
6. In **Auto-Publish Settings** the following is available



**Content Publication Workflow:** A workflow can be selected to provide additional functionality when ConfigMgr content is published, for example: to approve or deny publication. No action is required unless the default workflow will not be used.

**Publish Without Source Files:** This setting will publish ConfigMgr content without acquiring source files. This will save drive space since no content will actually be distributed from the Adaptiva Content Library on this server but should only be used when the Adaptiva Server is connected to a ConfigMgr Central Administration Site (CAS) that has no clients registered. On child Primary sites, this setting should not be enabled

- In **Publication Settings**, check the box for each content type



**Automatically Publish Content:** When selected, all new or modified items for the respective content type will be published.

If **Automatically Publish Content** is not checked, then you can select **Unpublish Published Content** – All content within that content type will be removed from OneSite

**Publish All Existing Content:** When selected, all existing content of the specified type in ConfigMgr will be published in Adaptiva. If not selected, only new content within that content type will be published.

- Click **Save**

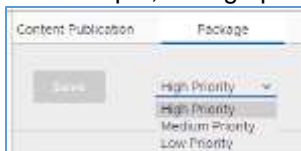
### Content Publication Settings for each Content Type and Priority

OneSite allows for a high degree of control when distributing content. Settings can also be changed for individual content items.

- Connect to the Adaptiva Web Portal using a web browser (except Internet Explorer) – [http\[s\]://AdaptivaServerFQDN\[:port\]](http[s]://AdaptivaServerFQDN[:port])
- Enter the appropriate credentials or click on **Login with Active Directory**
- Click on **Go to OneSite ConfigMgr** or click **OneSite Anywhere, OneSite ConfigMgr Edition**
- In **Settings, Publication**, select the individual content types: **Package, Software Update, Boot Image, etc.**



- Select the content type priority – the changes made below will only affect content with the same priority in ConfigMgr.  
For example, All high priority packages will be encrypted and will have a priority of 10



**General Settings** - this displays information, status, and encryption settings for a content type and priority.

**Encrypt Packages** – If the Encrypt Package setting is enabled (slid right), the content will be encrypted during publication.

**NOTE:** *Enabling this setting on an already published content item will force re-publication. Publishing encrypted content items will take longer than publishing a non-encrypted content item due to the resources needed to perform the encryption.*

**Content Publication Settings**, select the appropriate checkbox

**IMPORTANT:** *It is NOT recommended to store Software Updates in the Azure Cloud Store. These can be downloaded directly from the Windows Update CDN. The exception to this would be 3rd party software updates. For those, in ConfigMgr, change their priority to High (something different than normal Software Updates) (To change Software Update Deployment package Priority: Deployment Packages, Properties, Distribution Settings) and then in Adaptiva Web Portal configure the High Priority Software Update Publication Settings and check Publish Content on Cloud Store.*

**Package Download Settings** - This contains settings that control the download and reporting behavior of a content type and priority.

**Send Status Message On** – The content can be configured to send ConfigMgr status messages when the download starts, when it finishes, if it fails and at any **In-Progress** completion percent interval. Content download status can be reviewed in ConfigMgr reports.

**Never Download On Battery** – When enabled (slid to the right), laptops running on battery power will not attempt to download the content.

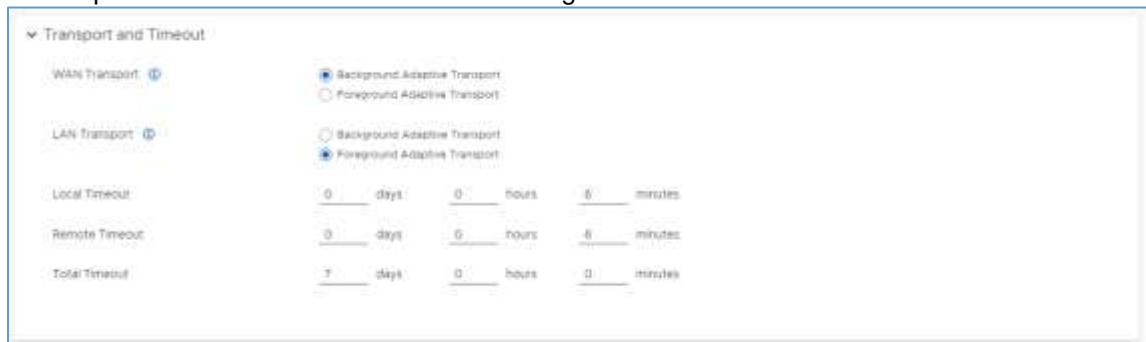
**Never Download Over WAN** – When enabled (slid to the right), the content is set to never download over the WAN or between offices.

**Priority** - ConfigMgr allows the user to specify Content Distribution Priorities for content relative to one another as High, Medium, or Low. OneSite takes this concept a step further and provides more flexibility by allowing an administrator to define 255 levels of priority (with 1 being lowest and 255 being highest priority). WAN downloads of lower priority content are automatically paused when a higher priority download starts. By specifying a priority for a content item, you are choosing which content downloads it can pre-empt, and which content can pre-empt it.

Each content type and priority have a default priority:

Content Type	Adaptiva Priority		
	ConfigMgr Priority: Low Priority	Medium Priority	High Priority
Boot Image	20	80	160
OS Image	20	80	160
OS Update Package	20	80	160
Driver	20	80	160
Package	40	100	180
Application	50	120	190
Software Update	60	110	200

**Transport and Timeout Settings** - These settings control the transport protocol which will be used while downloading content across the WAN and over the LAN. By default, WAN downloads are configured to use Background Adaptive Transport and will prevent interference with other traffic. The speed of the download will automatically adapt to the amount of actual unused bandwidth on that network. The Foreground Adaptive Transport, which is used on LAN connections by default, will still use our UDP based protocol, with checkpoint restart capability but will not perform Predictive Bandwidth Harvesting.



The screenshot shows the 'Transport and Timeout' settings interface. It includes sections for WAN transport (with Background Adaptive Transport selected), LAN transport (with Foreground Adaptive Transport selected), and three timeout settings: Local Timeout (0 days, 0 hours, 5 minutes), Remote Timeout (0 days, 0 hours, 5 minutes), and Total Timeout (7 days, 0 hours, 0 minutes).

**WAN Transport:** Select the default transport for downloads across the WAN.

**LAN Transport:** Select the default transport for downloads across the LAN

**Timeout Settings:** Determines how long clients will wait for the package before abandoning the request.

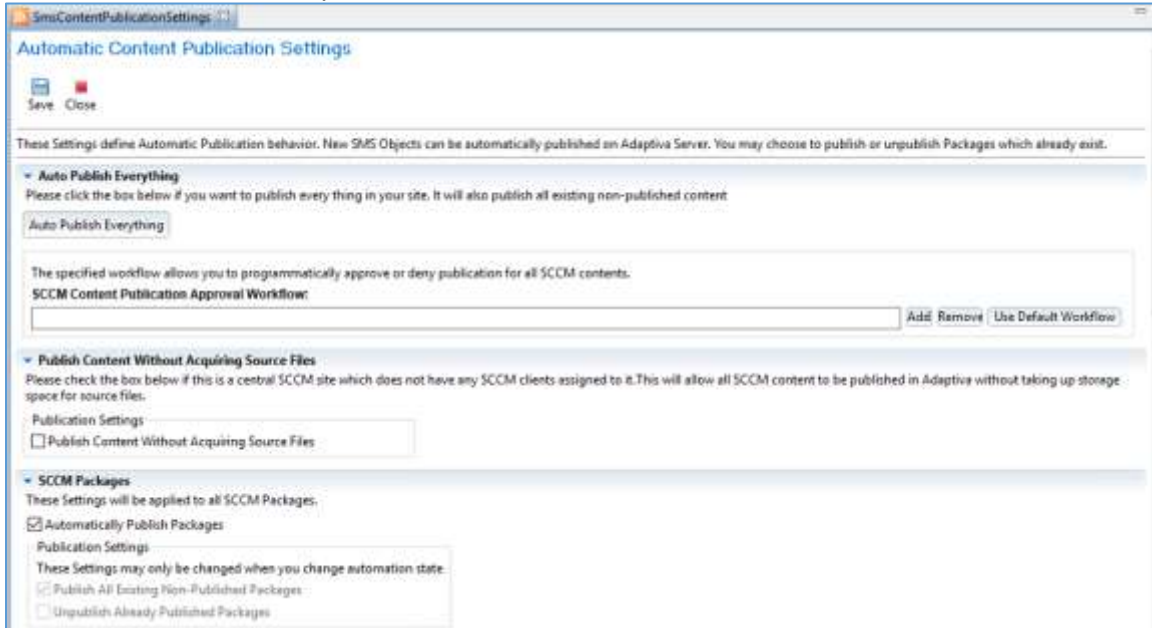
6. Click on **Save**
7. Repeat for each priority and each content type



## Using the Adaptiva Workbench

### Automatic Content Publication of ConfigMgr Content

1. In the Adaptiva Workbench, expand **OneSite** and select **OneSite – Package Perspective**
2. Select **Edit Automatic Publication Settings**. In the **Automatic Content Publication Settings** editor, review the various options:



**Auto Publish Everything:** When selected, all newly created content and existing content in ConfigMgr will be published in Adaptiva. Depending on the amount of content, this process can take time.

**SCCM Content Publication Approval Workflow:** A workflow can be selected to provide additional functionality when ConfigMgr content is published, for example: to approve or deny publication. No action is required unless the default workflow will not be used.

**Publish Content Without Acquiring Source Files:** This setting will publish ConfigMgr content without acquiring source files. This will save drive space since no content will actually be distributed from the Adaptiva Content Library on this server. This should only be used when the Adaptiva Server is connected to a ConfigMgr Central Administration Site (CAS) and the Adaptiva clients will be registered with an Adaptiva server connected to a child Primary site. When the Adaptiva clients will be registered with the Adaptiva server connected to the CAS, this setting should NOT be checked. On child Primary sites, this setting should NOT be checked.

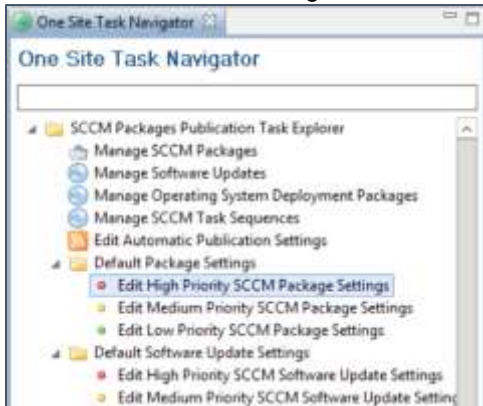
**<Content Type>** - The below settings apply to each content type and can be specified individually. Content types include Packages, Software Updates, Boot Image Packages, etc.

- **Automatically Publish Packages** – When selected, all new or modified items for the respective content type will be published. When you make a change to this property, the following options are available:
  - **Publish All Existing Non-Published Packages** – When selected, all packages existing in ConfigMgr will be published in Adaptiva. If not selected, only new content within that content type will be published.
  - **Unpublish Already Published Packages** – All content within that content type will be removed from OneSite.
3. Repeat for each content type
  4. Scroll back to the top and click **Save**, then **Close**

## Content Publication Settings for each Content Type and Priority

OneSite allows for a high degree of control when distributing content. Settings can also be changed for individual content items.

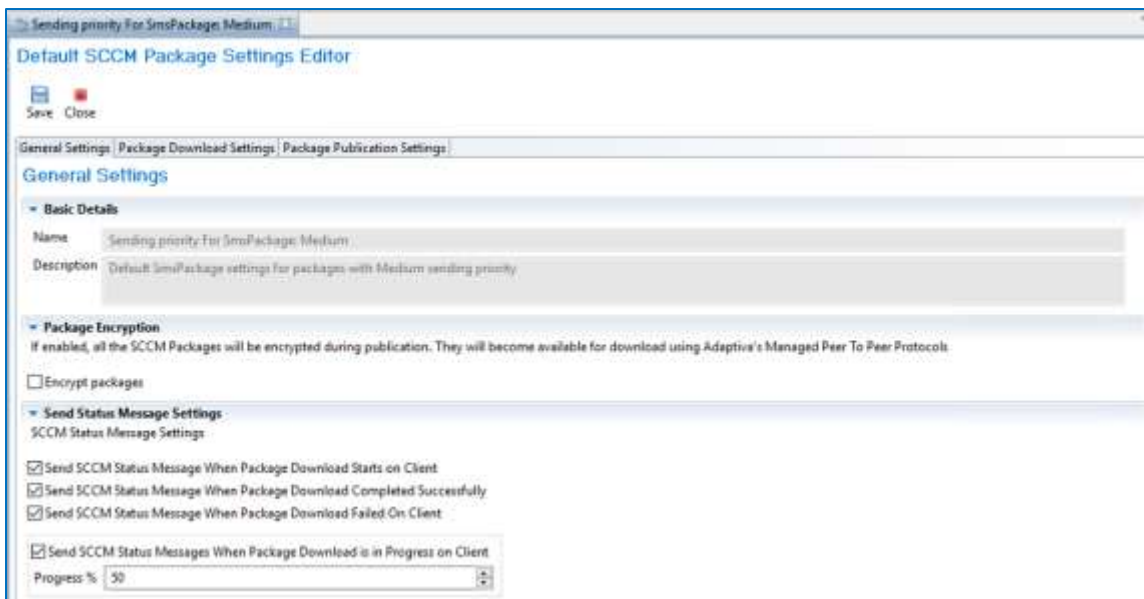
1. In the Adaptiva Workbench, expand **OneSite**, select **OneSite – Package Perspective** to open the **OneSite Task Navigator**
2. Content Publication settings are maintained for each content type and priority



For example, to tell Adaptiva to publish all medium priority packages to both the Adaptiva Server and the Cloud Store, under **Default Package Settings**, select **Edit Medium Priority SCCM Package Settings** and then click on the tab **Package Publication Settings**

### General Settings

This tab displays information, status, and encryption settings for a content type and priority.



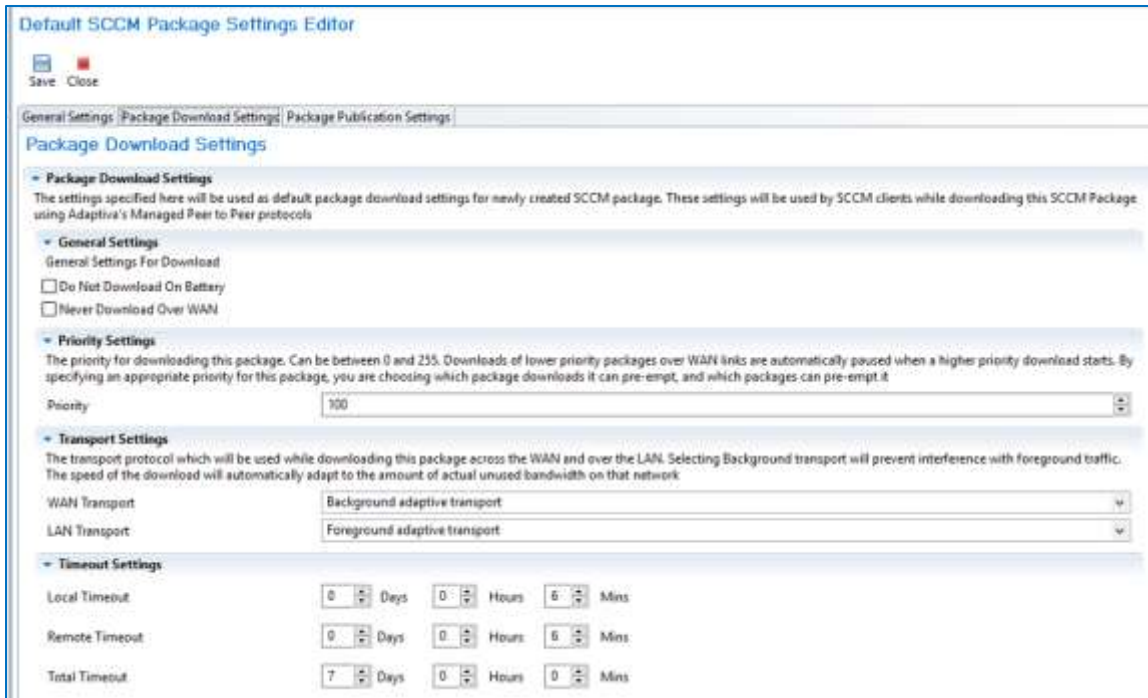
**Package Encryption:** If the Encrypt Package setting is checked, the content will be encrypted during publication.

**NOTE:** Enabling this setting on an already published content item will force re-publication. Publishing encrypted content items will take longer than publishing a non-encrypted content item due to the resources needed to perform the encryption.

**Send Status Message Settings:** The content can be configured to send ConfigMgr status messages when the download starts, when it finishes, and at any completion percent interval. Content download status can be reviewed in ConfigMgr reports.

## Package Download Settings

This tab displays settings that control the download of a content type and priority



**Default SCCM Package Settings Editor**

Save Close

General Settings | **Package Download Settings** | Package Publication Settings

**Package Download Settings**

The settings specified here will be used as default package download settings for newly created SCCM package. These settings will be used by SCCM clients while downloading this SCCM Package using Adaptive's Managed Peer to Peer protocols

**General Settings**  
General Settings For Download

Do Not Download On Battery

Never Download Over WAN

**Priority Settings**  
The priority for downloading this package. Can be between 0 and 255. Downloads of lower priority packages over WAN links are automatically paused when a higher priority download starts. By specifying an appropriate priority for this package, you are choosing which package downloads it can pre-empt, and which packages can pre-empt it

Priority: 100

**Transport Settings**  
The transport protocol which will be used while downloading this package across the WAN and over the LAN. Selecting Background transport will prevent interference with foreground traffic. The speed of the download will automatically adapt to the amount of actual unused bandwidth on that network

WAN Transport: Background adaptive transport

LAN Transport: Foreground adaptive transport

**Timeout Settings**

Local Timeout: 0 Days 0 Hours 6 Mins

Remote Timeout: 0 Days 0 Hours 6 Mins

Total Timeout: 7 Days 0 Hours 0 Mins

**Do Not Download On Battery** – When selected, laptops running on battery power will not attempt to download the content.

**Never Download Over WAN** – When selected, the content is set to never download over the WAN or between offices.

## Priority Settings

**Priority** - ConfigMgr allows the user to specify Content Distribution Priorities for content relative to one another as High, Medium, or Low. OneSite takes this concept a step further and provides more flexibility by allowing an administrator to define 255 levels of priority (with 1 being lowest and 255 being highest priority) . WAN downloads of lower priority content are automatically paused when a higher priority download starts. By specifying a priority for a content item, you are choosing which content downloads it can pre-empt, and which content can pre-empt it.

## Transport Settings

These settings control the transport protocol which will be used while downloading content across the WAN and over the LAN. By default, WAN downloads are configured to use Background Adaptive Transport and will prevent interference with other traffic. The speed of the download will automatically adapt to the amount of actual unused bandwidth on that network. The Foreground Adaptive Transport, which is used on LAN connections by default, will still use our UDP based protocol, with checkpoint restart capability but will not perform Predictive Bandwidth Harvesting.

**Timeout Settings** - Determines how long clients will wait for the package before abandoning the request.

- **WAN Transport** – Select the default transport for downloads across the WAN.
- **LAN Transport** – Select the default transport for downloads across the LAN

- **Timeout Settings** - Determines how long clients will wait for the package before abandoning the request.

### Package Publication Settings

This tab displays settings that control how the specified content with the specific priority is published



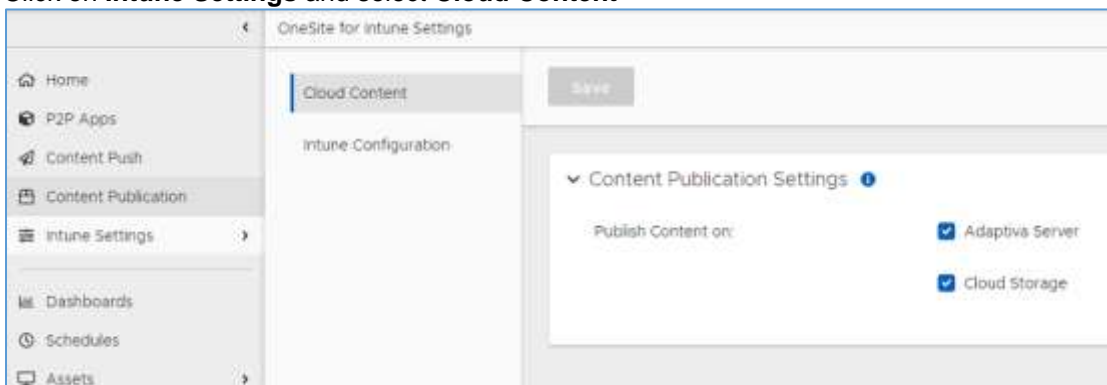
**IMPORTANT:** It is **NOT** recommended to store Software Updates in the Azure Cloud Store. These can be downloaded directly from the Windows Update CDN. The exception to this would be 3rd party software updates. For those, change their priority to High (something different than normal Software Updates) (To change Software Update package Priority: Deployment Packages, Properties, Distribution Settings) and then configure the High Priority SCCM Software Update Settings and select Publish Content on Cloud Store.

3. Click **Save**, then **Close**
4. Repeat for each content type and priority

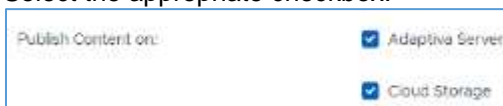
## Intune Content

### Using the Adaptiva Web Portal

1. Connect to the Adaptiva Web Portal using a web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Go to OneSite Intune Edition** or click **OneSite Anywhere, OneSite Intune Edition**
4. Click on **Intune Settings** and select **Cloud Content**



5. Select the appropriate checkbox.



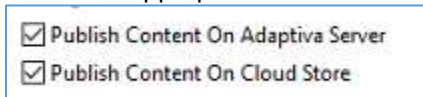
6. Click **Save**

## Using the Adaptiva Workbench

1. In the Adaptiva Workbench, expand **OneSite Intune**, select **OneSite for Intune** to open the **Intune Settings Tasks**



2. Select **Manage Application Content Publication Settings**
3. Select the appropriate check box.



4. Click **Save** and **Close**

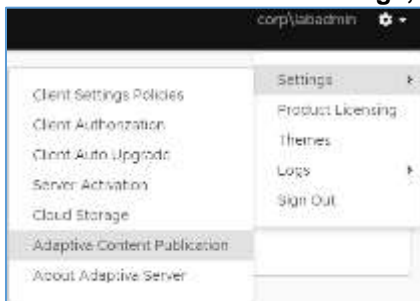
## Workspace ONE Content

At this time, the Workspace ONE app metadata is only visible in the Adaptiva Workbench. There are no content publication settings for Workspace ONE apps as the content is stored exclusively in the Workspace ONE CDN.

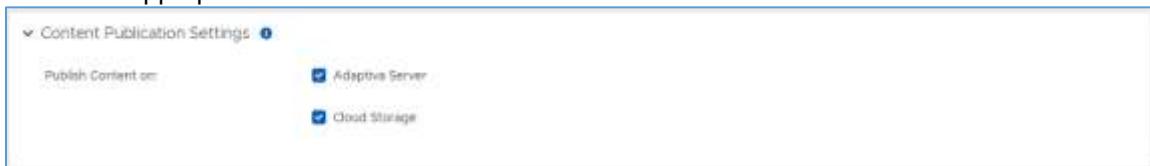
## Adaptiva Content

### Using the Adaptiva Web Portal

1. Connect to the Adaptiva Web Portal using a web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on and select **Settings**, select **Adaptiva Content Publication**



4. Select the appropriate checkbox

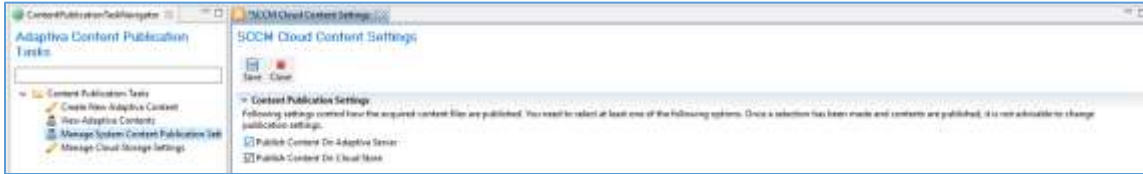


5. Click **Save**

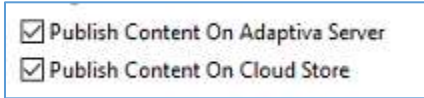
### Using the Adaptiva Workbench

1. In the Adaptiva Workbench, expand **Content Management**, select **Adaptiva Content Publication Perspective** to open the **Adaptiva Content Publication Tasks**

2. Select **Manage System Content Publication Settings**



3. Select the appropriate checkbox.

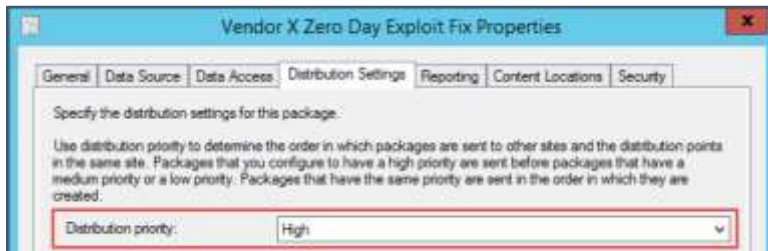


4. Click **Save** and **Close**

## Scenario: Zero Day Exploit – Using Content Priority to Distribute Faster

Consider the following scenario: An administrator has implemented ConfigMgr and Adaptiva and is in the process of deploying routine Microsoft Software Updates to all machines in the enterprise. Currently the content is being downloaded from hundreds of office locations. That afternoon, one of the company’s software vendors announces the release of a patch for their product which fixes a rapidly spreading zero day exploit. The administrator is instructed to deploy the fix immediately to all clients in the enterprise so a ConfigMgr package is created and is ready for deployment. The administrator deploys the package using ConfigMgr and notices that clients are still downloading the routine Software Update package and not the Zero Day Exploit fix.

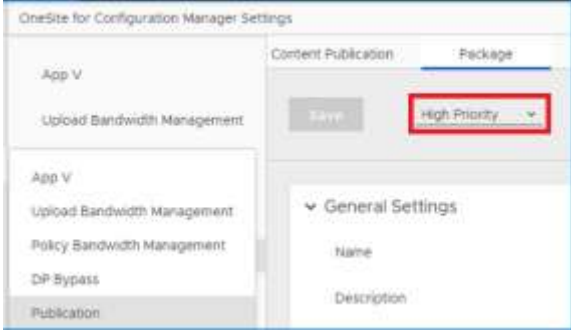
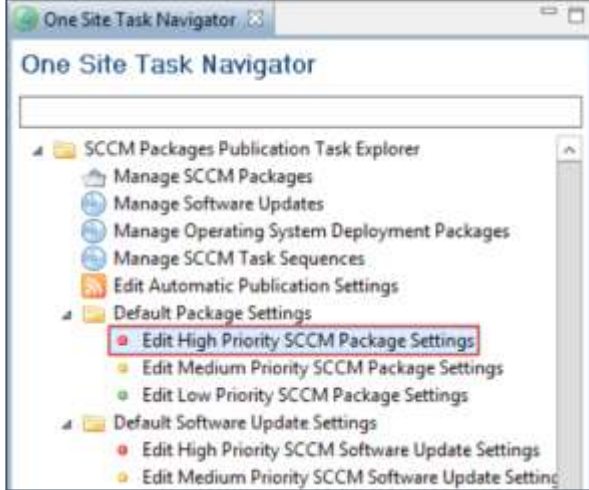
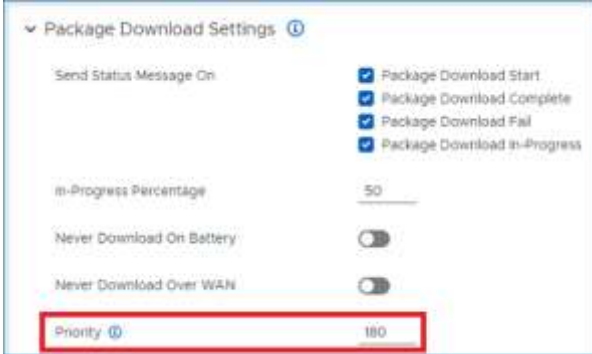

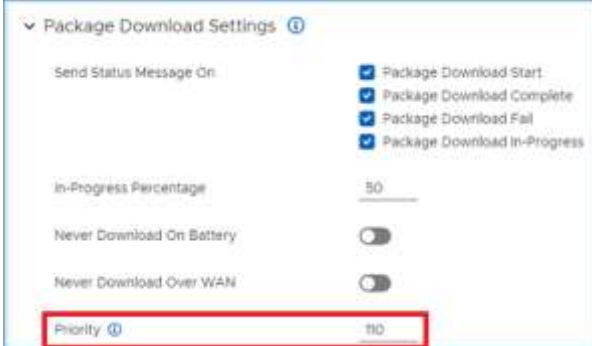

To resolve this issue, the administrator would open the ConfigMgr console, and edit the Properties of the package. Under the Distribution Settings tab, the priority is changed from Medium to High.



After applying the change, the Adaptiva Server immediately detects the change in priority and instructs the Adaptiva clients downloading the software update package to wait, and the Zero Day Exploit package begins downloading immediately.

To see why this change resolved the issue follow the steps below to review the defaults for High-priority ConfigMgr Packages and Medium priority Software Update Deployment Packages.

Using the Adaptiva Web Portal	Using the Adaptiva Workbench
<p>Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – <code>http[s]://AdaptivaServerFQDN[:port]</code></p> <p>Select <b>Go to Settings, Publication</b> or click <b>OneSite Anywhere, OneSite ConfigMgr Edition, Settings, Publication</b>.</p>	<p>In the <b>OneSite – Package Perspective</b> and in the <b>One Site Task Navigator</b>, under the <b>Default Package Settings</b>, open <b>Edit High Priority SCCM Package Settings</b>.</p>

Using the Adaptiva Web Portal	Using the Adaptiva Workbench
<p>Select <b>Package</b> and be sure <b>High Priority</b> is selected</p> 	
<p>Scroll down to the <b>Package Download Settings</b> section. Notice the priority is set to <b>180</b></p> 	<p>In the <b>Default SCCM Package Settings</b> editor, select the <b>Package Download Settings</b> tab. Notice in the <b>Priority Settings</b> section, the priority is set to <b>180</b>.</p> 
<p>Select the <b>Software Update</b> content type from the top menu, then select <b>Medium Priority</b></p> <p>Scroll down to the <b>Package Download Settings</b> section. Notice the priority is set to <b>110</b> by default</p> 	<p>Now in the <b>One Site Task Navigator</b>, under <b>Default Software Update Settings</b>, open <b>Edit Medium Priority SCCM Software Update Settings</b>. In the editor, select the <b>Software Update Settings</b> tab, in the Priority Settings section, notice the priority is set to <b>110</b> by default.</p> 

The above scenario provides an example of how settings can be applied to entire content types individually based on ConfigMgr Content Distribution priorities. This provides ConfigMgr and Adaptiva administrators granular control of how Adaptiva content is managed.

For even more granular control, the administrator can edit any package and manually set the priority in Package Download Settings to the desired setting to ensure that it has the desired priority.

# Content Creation and Publication

When content is published in Adaptiva, a package is created in Adaptiva and the source files are gathered directly from the ConfigMgr Content Library or the specified content source location for Adaptiva or Intune content. The package is compressed, optionally encrypted, and is stored on the Adaptiva server in the <AdaptivaServerInstallPath>\data\ContentLibrary folder by default.

**NOTE: The Content Library can be moved by following the instructions in this [How-To article](#).**








The content can also be stored in the internet in an Azure Storage Container where it can be accessed by either Adaptiva clients in the Central Office to distribute to on-premises clients or directly by Adaptiva clients that are on the internet. Whenever published content is referenced in an Advertisement/Deployment, it will be distributed using Adaptiva OneSite instead of ConfigMgr, Intune or Workspace ONE.

If you are updating existing content to publish to the Cloud Store be sure to update the Content Publication Settings for each content type and priority first.



**IMPORTANT: Content cannot be published to the cloud using the workbench without first unpublishing that content. When content is unpublished it will be removed from all computers. This may not be desirable. Use the Adaptiva Web Portal and the Update Publication Action to update the content into the cloud based on the Content Publication Settings defined.**

## Adaptiva Web Portal Content Publishing Icons


This is the list of Publication Status icons shown in the Adaptiva Web Portal

	Content has been published successfully to the Adaptiva Server Content Library
	Content has been published successfully to the cloud
	Content has been published successfully to both the Adaptiva Server Content Library and to the cloud
	There is an issue publishing the content. Check the Publication Status column.
	There is no content for this item
	Publication is in progress.
	Not Published




### Application Folder Icons

	All content has been published
	One or more content items has not been published

### Software Updates Folder Icons











	All content has been published
---	--------------------------------



	One or more content items has not been published
	<p>No content to publish</p> <p>NOTE: This icon will display if there are one or more individual content items that are not able to be published. Select the update in the deployment package to see the list of the individual content items. Sort descending on the column Publication Status. If a content item is removed from the update, Adaptiva will show the publication status of the content item as SMS Object Expired in SCCM and the content item will have the icon </p>

## Adaptiva Workbench Content Download Icons

This is the list of Publication Status icons in the Adaptiva Workbench

	Content has been published successfully to the Adaptiva Server Content Library
	Content has been published successfully to the cloud
	Content has been published successfully to both the Adaptiva Server Content Library and to the cloud
	Content is partially published
	Content is publishing
	Publication is in progress.
	Published without content
	There is an issue publishing the content. Check the Publication Status column.
	There is no content to publish
	Not Published

## ConfigMgr Content

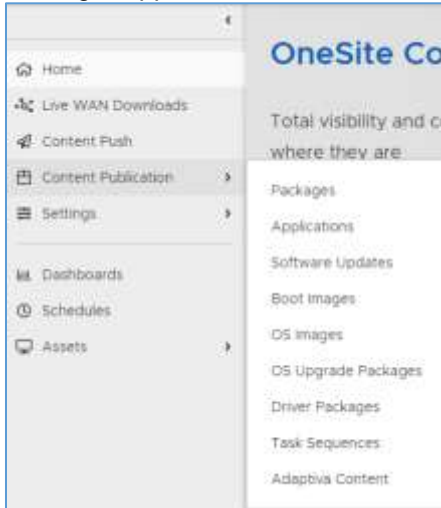
### Using the Adaptiva Web Portal

Configuration Manager content should be automatically published based on the Content Publication Settings when that content is created in Configuration Manager. Create a package, application or other content type in the ConfigMgr console, then open Web Portal to view the content in the Content Viewer page.

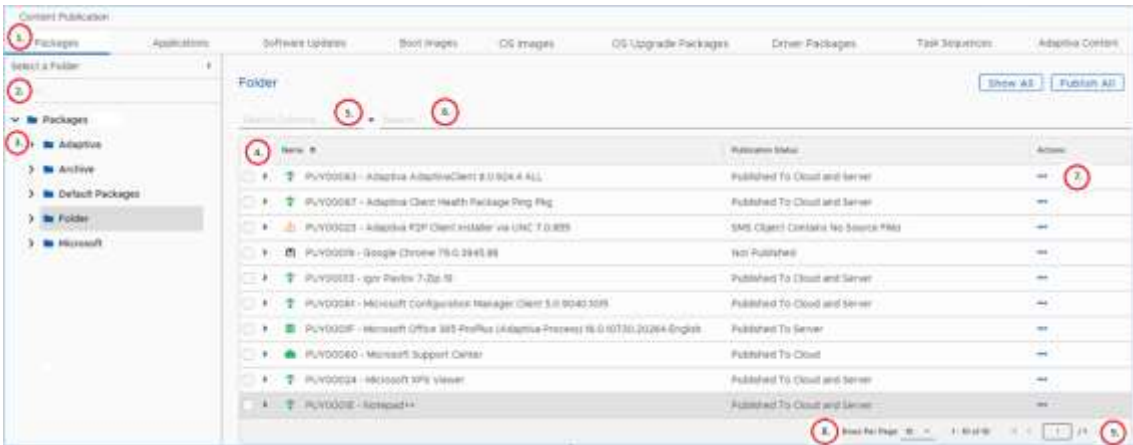
### Viewing ConfigMgr Content

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

- Click **Content Publication** and select the content type associated with the ConfigMgr content, Package, Application, etc.



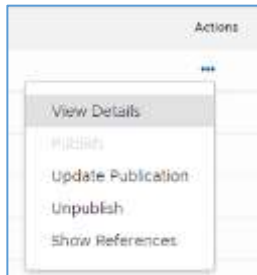
- There will be a list of content from Configuration Manager that is known to Adaptiva



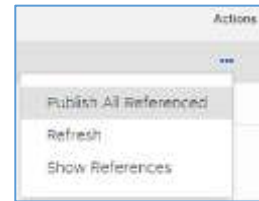
To navigate this page, reference the numbers in the picture above with the descriptions below

- This row allows you to select the different content types, including Adaptiva Content
- This Search box allows you to search for different folders. It is specific to the content type selected
- This is the list of folders for that content type. Select the folder to view the content in that folder.
  - Applications and Software Updates are different because they have sub-items. Applications will show the *Package ID – Application Name* in the folder hierarchy. Selecting the folder will allow it to be expanded or collapsed. Select the Application to see the Deployment Types with their Content ID and their Publication Status
  - Software Update Deployment Packages cannot have folders. Each *Package ID – Deployment Package Name* will show the individual updates. Each update may have one or more associated content items that has been published.
- The results are sortable by clicking on the column name in the column header
- Select a column to limit the Search to. If no column is selected, then the first column will be searched by default
- Use the Search box to filter the returned list of content items

- Click the ellipses, ..., under the **Actions** column to bring up a context menu



Because Task Sequences may contain multiple content types, the following context menu is available:



- Select the number of rows returned and displayed. This can be changed to 10, 25, 50 or 100
- Use the navigation buttons to move to the next/previous page or to the end/beginning of the list

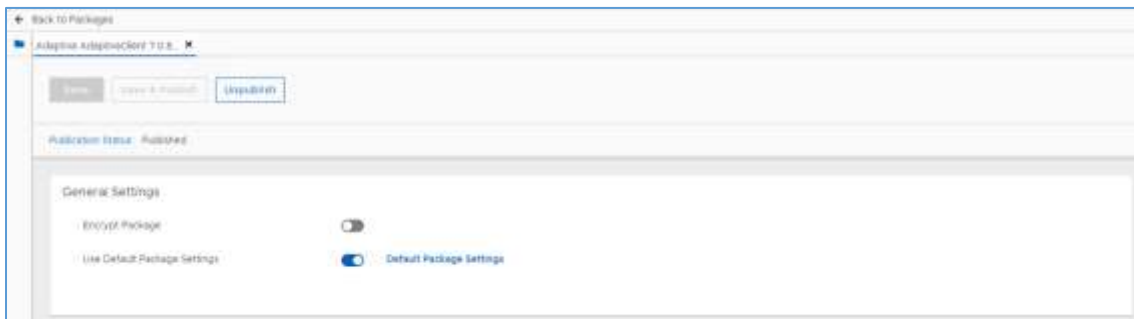
You will notice that the icon will change to several other icons as the content is being published. Depending on the size of the content this may take some time. Once the content is published the color of the flag icon will turn green or .

In the case of a publication error hover over the package and select the ellipses, ..., under the Actions column and select View Detail where additional error information will be displayed. By default, if there is an error publishing a package, the Adaptiva Server will await manual resolution/retry.

**NOTE:** In version 5.6 and later, there is now a server-side registry setting available to instruct the Adaptiva Server to retry publication periodically. To enable this setting, set the following registry value on the Adaptiva server [onesite.publication\_request\_retry\_processing\_delay]. Set this to a value in Milliseconds to automatically retry publication (e.g. 600000 for every 10mins)

### View Details

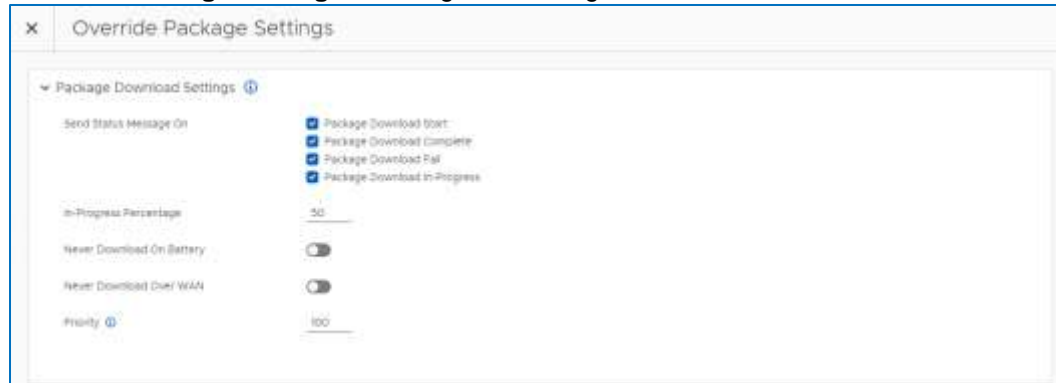
With this menu you can get more details about a content item, enable encryption, change the package settings and change the Content Publication settings



- Encrypt Package** – If the Encrypt Package setting is enabled (slid to the right), the content will be encrypted during publication.

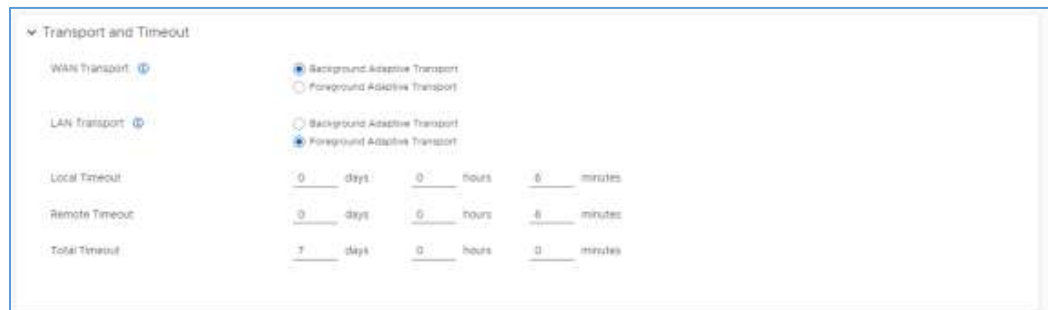
**NOTE:** Enabling this setting on an already published content item will force re-publication. Publishing encrypted content items will take longer than publishing a non-encrypted content item due to the resources needed to perform the encryption.

- **Use Default Package Settings** – When this setting is enabled (this is the default), the default package settings will be used. Click the button to toggle to the left and select **Override Package Settings** to change the settings.



Update these settings to override the default settings that control the download and reporting behavior of a content item.

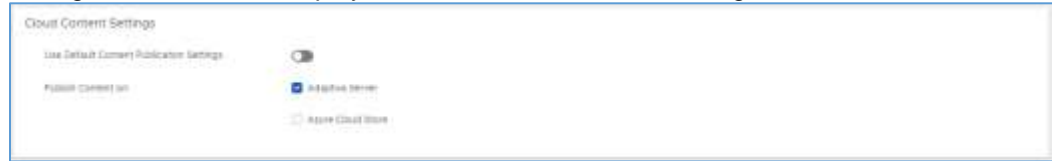
- **Send Status Message On** – The content can be configured to send ConfigMgr status messages when the download starts, when it finishes, if it fails and at any **In-Progress** completion percent interval. Content download status can be reviewed in ConfigMgr reports.
- **Never Download On Battery** – When enabled (slid to the right), laptops running on battery power will not attempt to download the content.
- **Never Download Over WAN** – When enabled (slid to the right), the content is set to never download over the WAN or between offices.
- **Priority** - ConfigMgr allows the user to specify Content Distribution Priorities for content relative to one another as High, Medium, or Low. OneSite takes this concept a step further and provides more flexibility by allowing an administrator to define 255 levels of priority (with 1 being lowest and 255 being highest priority). WAN downloads of lower priority content are automatically paused when a higher priority download starts. By specifying a priority for a content item, you are choosing which content downloads it can pre-empt, and which content can pre-empt it.



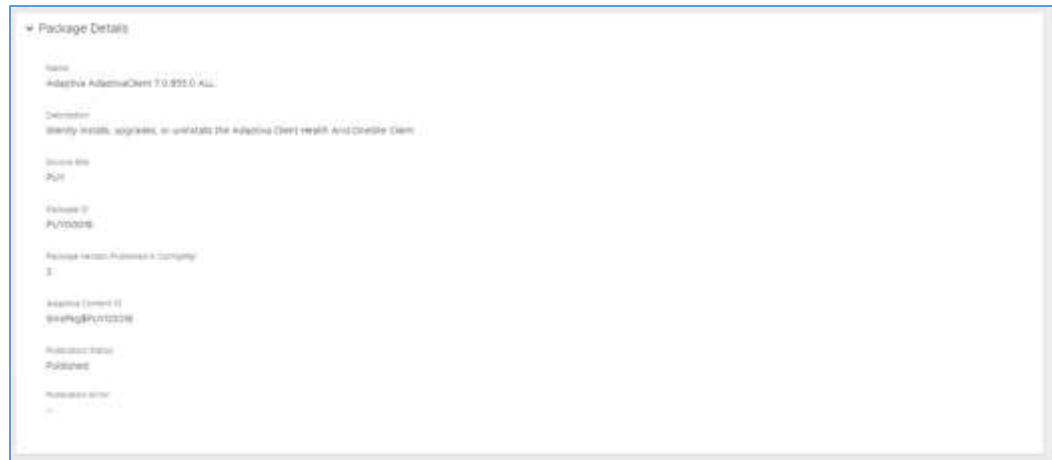
- **WAN Transport** – Select the default transport for downloads across the WAN
- **LAN Transport** – Select the default transport for downloads across the LAN
- **Timeout Settings** - Determines how long clients will wait for the package before abandoning the request

Click **OK** to save these overrides for this content item

- **Use Default Content Publication Settings** – Clicking on the button will toggle this setting to disabled and display the **Publish Content on** settings



Check the appropriate boxes to override where the content should be published



Package Details will display information about the package. If there was a publication error, information about the error will be listed.

If changes were made, the **Save** and **Save & Publish** buttons will be activated



Click on **Save** to save the changes to the Content Item

Click on **Save & Publish** to save the changes and publish the content

### **Publish or Publish Parent Content**

If the content is not published, this action can be used to publish the content. For Applications and Software Updates all content items will be published

### **Update Publication**

This action will update the content in the defined content locations. If the content is not published to the Cloud store and the Default settings for this content type have Cloud store checked, the content will be published in the Cloud store

### **Unpublish or Unpublish Parent Content**

If the content is published, this action can be used to unpublish the content. This will remove the content from the Content Library and the Cloud store

### **Show References**

This will show where the content item is referenced. Specifically, if it is part of a task sequence or Content Push, if not, it will just show the folder the content is in

## Refresh

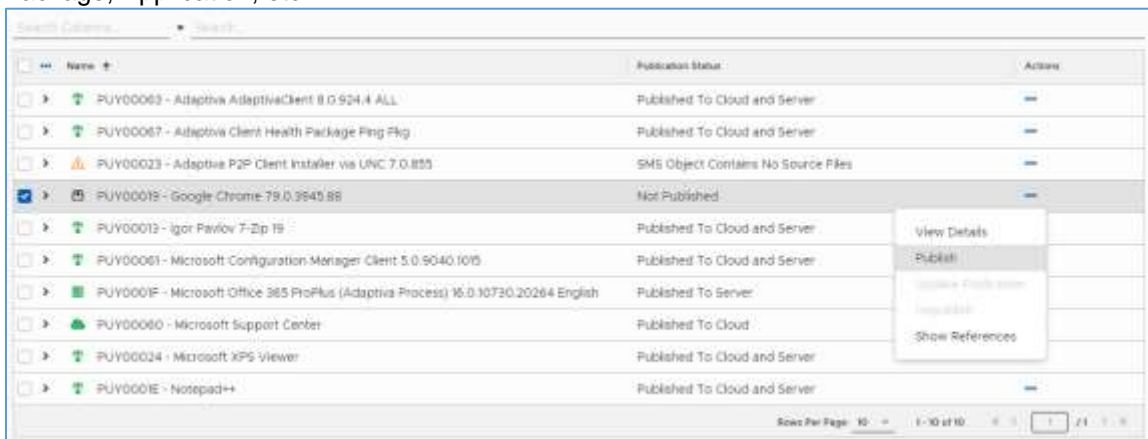
This will refresh the publication status of the select content item

## Publishing ConfigMgr Content

If Auto Publish Everything was not selected, then content will need to be manually published in order for Adaptiva to be able to download the content.

Follow the steps below to manually publish ConfigMgr content in OneSite.

1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – [http\[s\]://AdaptivaServerFQDN\[:port\]](http[s]://AdaptivaServerFQDN[:port])
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Go to OneSite ConfigMgr Edition** or click **OneSite Anywhere, OneSite ConfigMgr Edition**
4. Click **Content Publication** and select the content type associated with the ConfigMgr content, Package, Application, etc.



5. Use the search box to filter the list if necessary
6. Click on the ellipses, ..., under the **Actions** column and select **Publish**
7. You will notice that the icon will change to several other icons as the content is being published. Depending on the size of the content this may take some time. Once the content is published the color of the icon will turn green

**NOTE: In the case of a publication error, click the ellipses, ..., under Actions and select Edit to open the editor where additional error information will be displayed.**

8. Once the content is published, it is now available for Adaptiva clients to download and can be used in Content Push Policies

## Using the Adaptiva Workbench

Configuration Manager content should be automatically published based on the Content Publication Settings when that content is created in Configuration Manager. Create a package, application or other content type in the ConfigMgr console, then open **Adaptiva Workbench, OneSite, OneSite – Package Perspective** to view the content in the respective Explorer.

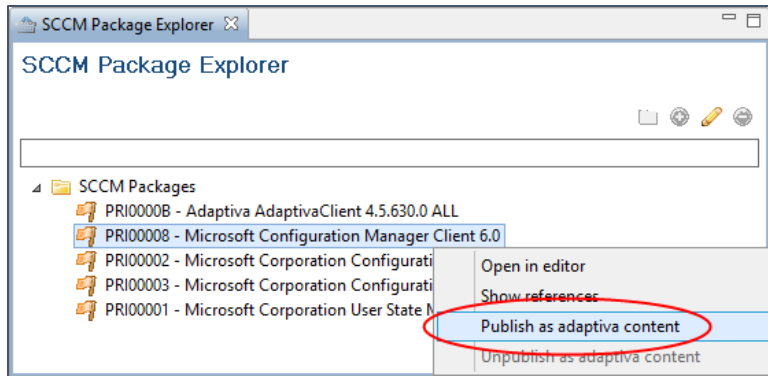
## Publishing ConfigMgr Content

If Auto Publish Everything was not selected, then content will need to be manually published in order for Adaptiva to be able to download the content.

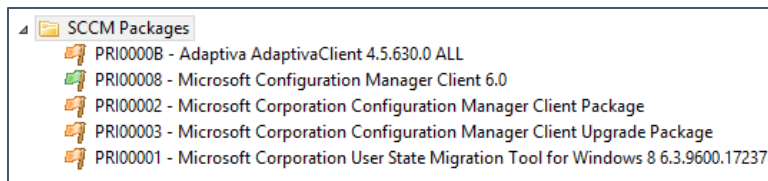
Follow the steps below to manually publish content in OneSite.

1. In the Adaptiva Workbench, in the **Home Perspective**, expand the **OneSite** folder and open the **OneSite – Package Perspective**.

- On the right side of the Workbench, in the **SCCM Package Explorer**, expand the **SCCM Packages** folder.
- Right-click the desired package, and in the context menu select **Publish as adaptiva content**.



- You will notice that the orange flag icon will change to several other icons as the content is being published. Depending on the size of the content this may take some time. Once the content is published the color of the flag icon will turn green.



In the case of a publication error which may be indicated by a red flag icon, double-click the package to open the **SCCM Package Settings Editor** where additional error information will be displayed. By default, if there is an error publishing a package, the Adaptiva Server will await manual resolution/retry.

**NOTE: In version 5.6 and later, there is now a server-side registry setting available to instruct the Adaptiva Server to retry publication periodically. To enable this setting, set the following registry value on the Adaptiva server [onesite.publication\_request\_retry\_processing\_delay]. Set this to a value in milliseconds to automatically retry publication (e.g. 600000 for every 10 minutes)**

- Once the content is published, advertise/deploy the package as you normally would via the ConfigMgr Console. Any targeted machines with the Adaptiva Client installed will receive the content from OneSite instead of the Data Transfer Service in ConfigMgr.

## Intune Content

### Using the Adaptiva Web Portal

The following applications types can be created as P2P Apps for peer to peer distribution.

- Any EXE installer
- Any MSI installer
- Any Script-based installer

Deploying an application using Intune with OneSite is a multi-step process all automated using the Adaptiva Web Portal.

- Create the Intune P2P App in Adaptiva
- Generate the OneSite win32 P2P application (Win32 .intunewin)
- Create the Windows app (Win32) in Intune

The last step is the only step that needs to be completed manually:

#### 4. Target end-users or devices

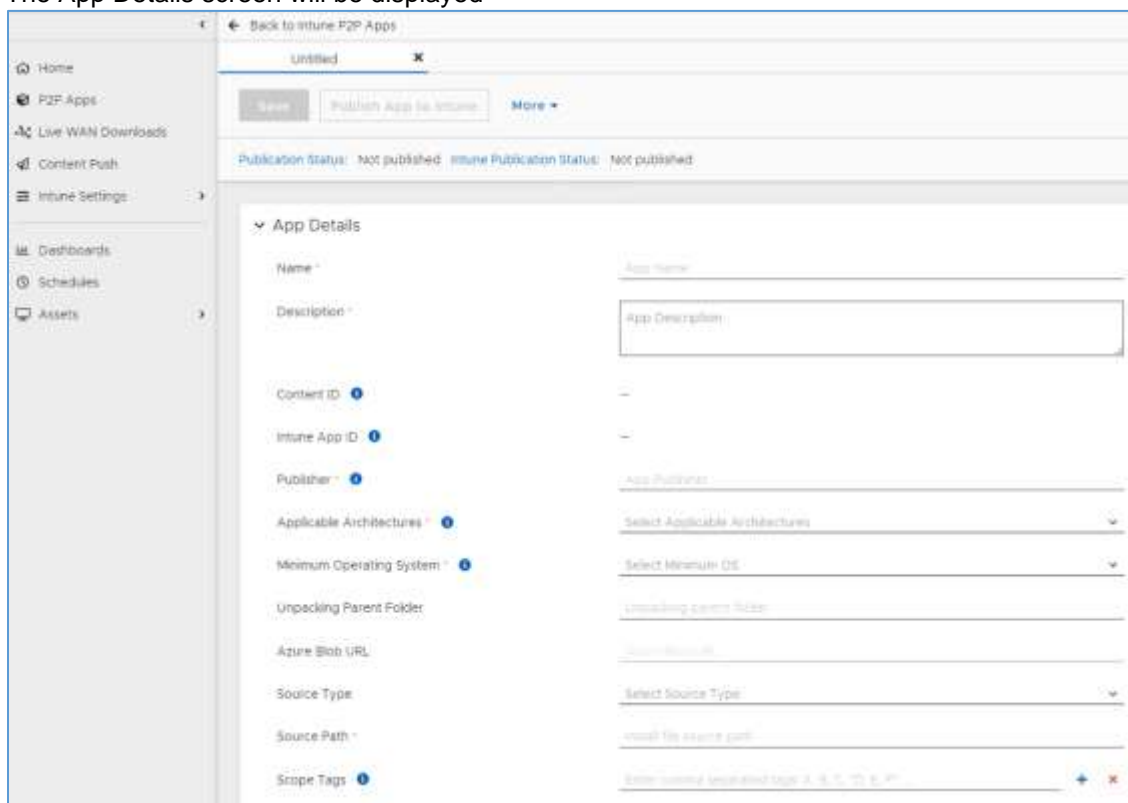
When content is created in Adaptiva for distribution using Intune, the source files are compressed, optionally encrypted, and stored on the Adaptiva server in the `<AdaptivaServerInstallPath>\data\ContentLibrary` folder. This is stored as a .content file. The .content file will also be uploaded to the Azure Storage container. If the storage location is only in Azure, then the .content file will be removed from the Adaptiva Server Content Library.

In addition, an .intunewin file is created that will provide an 80kb executable to download. The .intunewin file will be used as the app package file when creating the Windows app (Win32) in Intune. The .intunewin file is created by the Microsoft Win32 Content Prep Tool.

App Registration must be completed prior to creating and deploying content using Adaptiva OneSite for Intune. See the App Registration section in the Installation Prerequisites section of the Adaptiva Installation Guide.

### Creating New Intune P2P Content

1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Go to OneSite Intune Edition** or click **OneSite Anywhere, OneSite Intune Edition**
4. Select **Go to P2P Apps** or click on **P2P Apps** in the Activity workspace on the left
5. Click on **+ New** to create a new P2P App in Intune
6. The App Details screen will be displayed



Complete **App Details** screen with the following information:  
You must enter the items with the \*



**Name:** Enter the Application Name. This will be displayed to the end user if using the Company Portal

**Important:** The Name should NOT contain any special characters or spaces as this name is used to create an executable program

**Description:** Enter the Application description

**Publisher:** Enter the Publisher name

**Applicable Architectures:** Select the OS architecture required to install the application

**Minimum Operating System:** Select the minimum OS version required to install the application

**Source Type:** Select **Local Source Path** if the content source exists on the server or **Network Source Path** if the content requires a UNC. When using Network Source Path, **Network Access Account** can then also be used to define the domain, username and password to connect to the UNC path.

**Source Path:** Enter the path to the source files

**Scope Tags:** Enter the Scope Tags to link to this App. Scope Tags must already be defined in Intune (See Tenant administration, Roles, Scope (Tags)). Click the + to add the tag. Multiple tags can be added.

**Scope Tags may be automatically attached to the App if they are Assigned to Groups and one of the Deferred Accounts was selected for the Login Type**

The following fields are optional:

**Unpacking Parent Folder:** By default, the content will be unpacked in the AdaptivaCache folder. To unpack to a different location, enter that location here.

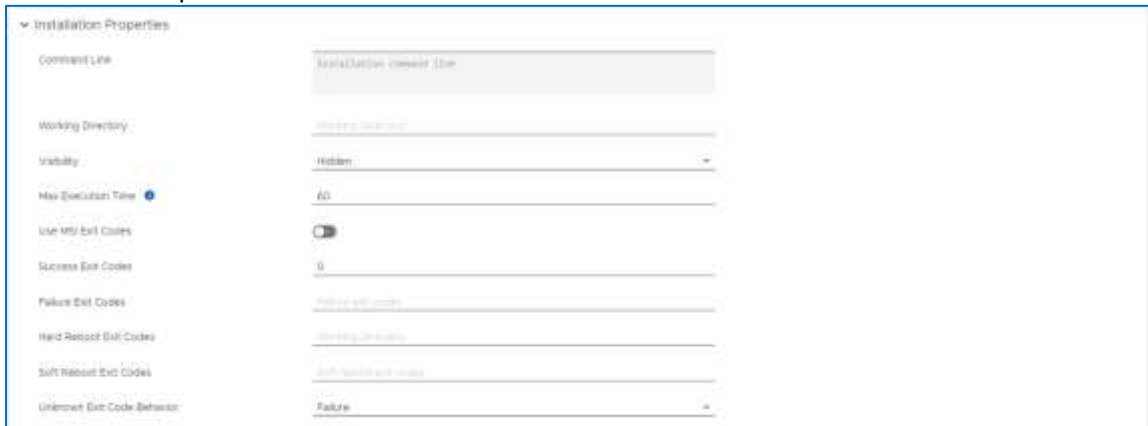
**Azure Blob URL:** Is not used

The following fields will be entered automatically:

**Content ID:** Unique ID assigned to the content in the Content Library

**Intune App ID:** Unique ID assigned to the application by Intune upon successful publication

## 7. Installation Properties



The screenshot shows the 'Installation Properties' section of an application configuration in Intune. It includes the following fields and controls:

- Command Line:** A text input field for the installation command line.
- Working Directory:** A text input field for the working directory path.
- Visibility:** A dropdown menu with options: Hidden (selected), Normal, Minimized, and Maximized.
- Max Execution Time:** A text input field with a blue information icon.
- Use MSI Exit Codes:** A toggle switch currently turned on.
- Success Exit Codes:** A text input field.
- Failure Exit Codes:** A text input field.
- Hard Reboot Exit Codes:** A text input field.
- Soft Reboot Exit Codes:** A text input field.
- Unknown Exit-Code Behavior:** A dropdown menu with the option 'Failure' selected.

Complete the following fields:

**Command Line:** Enter the installation command line

**Working Directory:** If a working directory is required, enter the working directory path

**Visibility:** Select from Hidden (Default), Normal, Minimized or Maximized

**Max Execution Time:** Enter the maximum time the installation should run. Default is 60 minutes.

**Use MSI Exit Codes:** If this is a Windows installer-based app, slide the toggle to the right, otherwise, enter the various exit codes in the remaining fields

**Success Exit Codes:** Default is 0. Enter the return code(s) in a comma separated list of a successful installation

**Failure Exit Codes:** Enter the return code(s) in a comma separated list if the installation failed

**Hard Reboot Exit Codes:** Enter the return code(s) in a comma separated list if the installation requires a hard restart

**Soft Reboot Exit Codes:** Enter the return code(s) in a comma separated list if a soft restart is required

**Unknown Exit Code Behavior:** If the exit code is not listed above, select from Failure, Success, Soft Reboot or Hard Reboot

## 8. Uninstallation Properties

Complete the following fields:

**Command Line:** Enter the uninstall command line

**Working Directory:** If a working directory is required, enter the working directory path

**Visibility:** Select from Hidden (Default), Normal, Minimized or Maximized

**Max Execution Time:** Enter the maximum time the uninstall should run. Default is 60 minutes.

**Use MSI Exit Codes:** If this is a Windows installer-based app, slide the toggle to the right, otherwise, enter the various exit codes in the remaining fields

**Success Exit Codes:** Default is 0. Enter the return code(s) in a comma separated list of a successful uninstall

**Failure Exit Codes:** Enter the return code(s) in a comma separated list if the uninstall failed

**Hard Reboot Exit Codes:** Enter the return code(s) in a comma separated list if the uninstall requires a hard restart

**Soft Reboot Exit Codes:** Enter the return code(s) in a comma separated list if a soft restart is required

**Unknown Exit Code Behavior:** If the exit code is not listed above, select from Failure, Success, Soft Reboot or Hard Reboot

## 9. Detection Rules

At least one Detection Rule must be entered

Click on **+ Add Detection Rule**

Select one **Rule type** and complete the form  
Rule type: File

× Detection Rule

Rule type \* ⓘ File ▾

Path \* ⓘ

File or Folder Name \* ⓘ

Detection Type \* ⓘ Select detection type ▾

Associated with a 32-bit app on 64-bit clients ⓘ

Rule type: Registry key

× Detection Rule

Rule type \* ⓘ Registry ▾

Key Path \* ⓘ

Value Name \* ⓘ

Detection method \* ⓘ Enter detection type ▾

Operator \* ⓘ Select operator ▾

Value \* ⓘ

Check as 32-bit ⓘ

Rule type: MSI

× Detection Rule

Rule type \* ⓘ MSI ▾

MSI product code \* ⓘ

MSI product version check ⓘ

Rule type: PowerShell

Click **OK**

10. Click **Save**. Notice Publish App to Intune is not available yet. Once the app information has been saved, **Publish App to Intune** will be available.

11. Click **Publish App to Intune**. This step will create the app in Intune and place the content file in the location specified in Intune Settings, Cloud Content.

12. If the Intune Configuration is using one of the Deferred Login Types and Authentication has not been completed the following Reauthentication request will be displayed

13. Click **Authenticate**

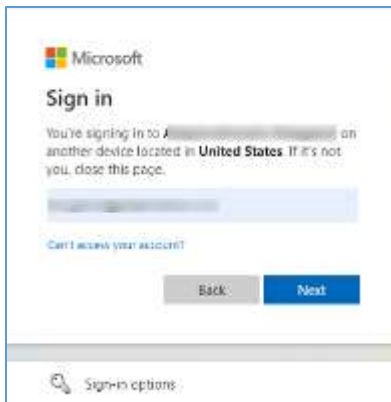


14. Copy the Device Code, then click **Authenticate**

**IMPORTANT.** The code will be requested on the next screen, be sure to copy it or write it down

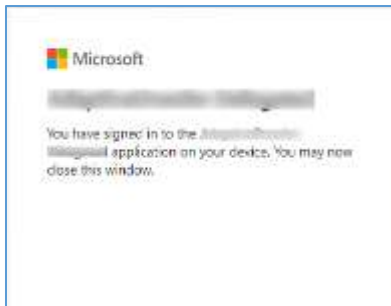
15. A login for Microsoft will be displayed, enter the code from the previous screen. Click **Next**

16. Confirm the Tenant and the username is correct. Click **Next**



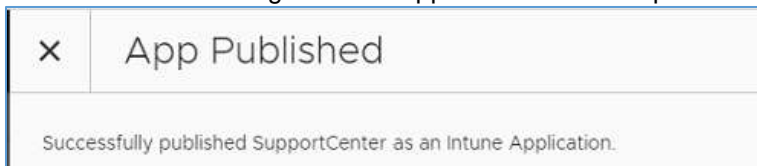
17. Enter the password for that account in that Tenant. Click **Sign in**  
Complete any authentication that is required.

18. Close the tab

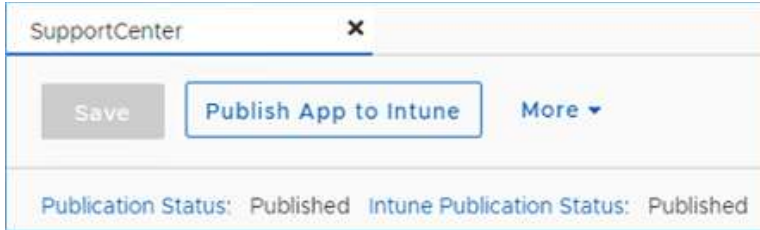


19. If you had to Authenticate, you will need to close the App Editor by clicking **← Back to Intune P2P Apps**, open the App again and click on **Publish to Intune**

20. Click **OK** to the message that the application has been published as an Intune Application.



21. After the content has been published to the Content Library, notice the Publication Status:



Publication Status will denote the status of the content in the Content Library  
 Intune Publication Status will denote the status of the Windows 32-bit app in Intune

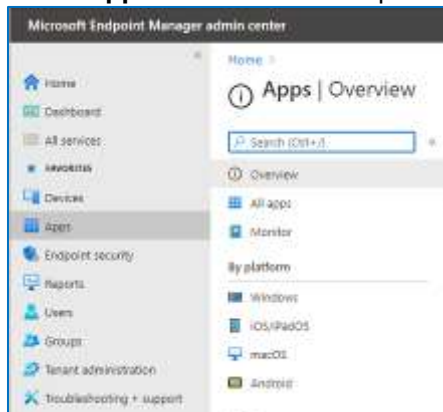
## Publishing or Updating Intune Content

Intune content will be published when the P2P App is created by clicking on Publish App to Intune. If that was not done, or if changes have been made to the app, do the following:

1. Select **P2P Apps** from the Activity pane on the left
2. Click the App or hover over the app and select the ellipses, ..., under **Actions** and select **Edit App**
3. Click on Save, then click on **Publish App to Intune**  
 Alternatively, hover over the app and select the ellipses, ..., under Actions and select **Update App in Intune**

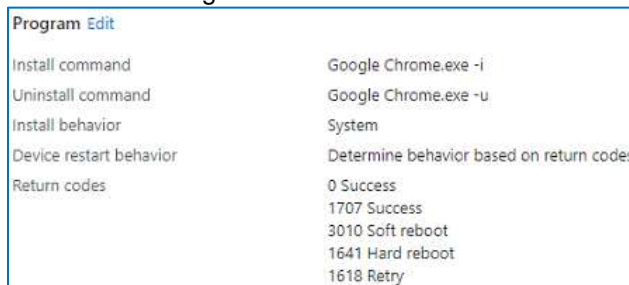
## Assign the App for Delivery

1. Connect to the Endpoint Management Admin Portal using your web browser (except Internet Explorer) – <https://endpoint.microsoft.com>
2. Enter the appropriate credentials
3. Select **Apps** from the left workspace pane



4. In the Apps blade, select **Windows** under **By platform**
5. Select the app to open it
6. Click **Properties**

Notice in the Program section the Install and Uninstall commands:

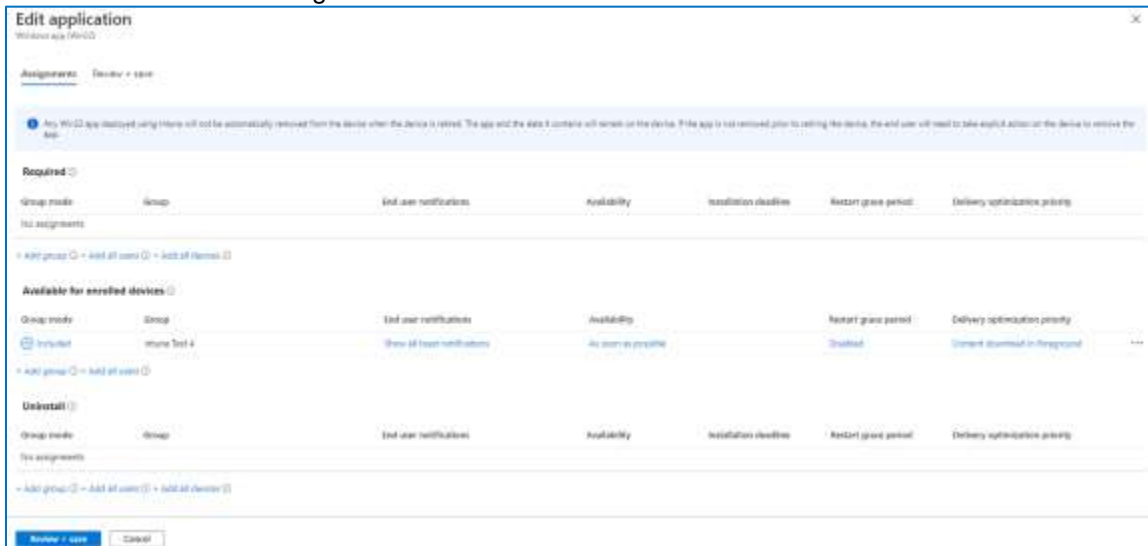


The Install and Uninstall commands have the application name.exe as the command line with -i for installation and -u for uninstall

These command lines will invoke Adaptiva to download the .content file using Adaptiva P2P technologies.

**Do not change the command lines**

7. Scroll down further to Assignments and click on **Edit**



Assignments do not need to be entered right now; they can be entered later.

Add a group to **Required** to force the installation

Add a group to **Available** for enrolled devices to make the installation optional via the Company Portal app. When adding a group to Available, the group must contain **Users**, not **Devices**.

Add a group to **Uninstall** for managed devices to have this app removed

**NOTE: If scope tags, supersedence (a new feature) or dependencies are to be used, those must be configured in the Endpoint Management Admin console.**

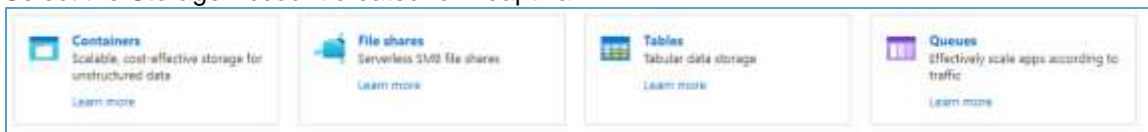
### (Deprecated) Viewing the Azure Storage-based Content Library

This feature is only available when Azure Storage Accounts are used. The recommended storage is the Adaptiva CDN and the content published there is not directly viewable as it is with Azure Storage.

1. Connect to the Azure Portal using your web browser (except Internet Explorer) – <https://portal.azure.com>
2. Enter the appropriate credentials



3. Select **Storage Accounts**. If it is not listed, enter Storage in the Search bar, then select it
4. Select the Storage Account created for Adaptiva



5. Select **Containers**
6. Select the Container created for Adaptiva
7. A folder will be created for each type of content: ConfigMgr, Adaptiva, Intune. Select the respective folder. Under the ConfigMgr folder will be a folder structure for each content type. E.g. packages, applications, etc.
8. There will be a folder named with the Content ID (Package ID) of the content. Select the folder
9. Finally, there will be a folder named with a GUID. Select the folder

10. The .content file will be listed

## Using the Adaptiva Workbench

All Intune content should be created using the Adaptiva Web Portal as this includes automation that will automatically create the Windows 32-bit app in Intune as well.

Intune content created in the Adaptiva Web Portal will not be visible in the Adaptiva Workbench and P2P apps (v1) created in the Workbench, will not be visible in the Adaptiva Web Portal.

## Workspace ONE Content

All Workspace ONE administrative activities are completed using the UEM Airwatch portal.

## Creating and Deploying Applications

The Workspace ONE UEM screens are updated regularly so screens may have changed.

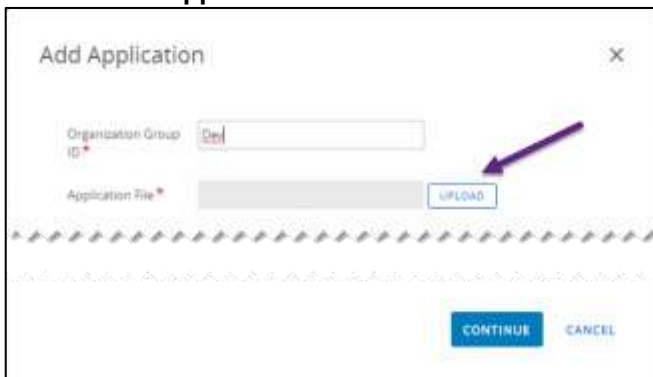
For more information on the options available see the VMWare documentation here:

<https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1811/VMware-Workspace-ONE-UEM-Mobile-Application-Management/GUID-AWT-CONFIG-INTERNAL-APPS-LOCAL.html>

1. Open a web browser and connect to <https://cn800.airwatchportals.com>
2. Log in with your UEM account
3. Select **Apps & Books, Applications, Native**



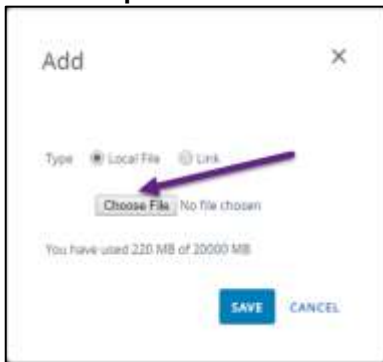
4. Click on **Add Application**



The Organization Group will already be entered



5. Click on **Upload**

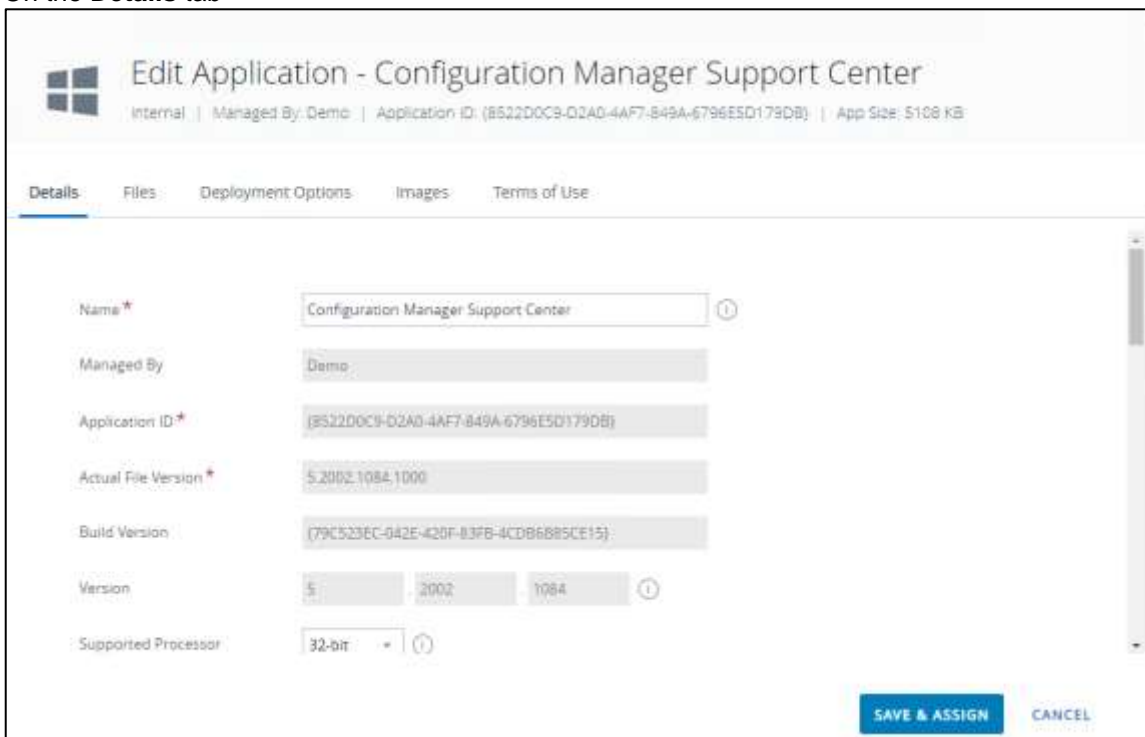


6. Click on **Choose File**  
Browse to the location of the installation .EXE, .MSI, or .ZIP with a script and select it  
Click **Open**, then click **Save**

**NOTE: File size MUST be under 20GB. The file uploaded must be the sole source of the installation. There cannot be a source folder with many files and subfolders, everything must be self-contained in the file selected.**

**Using a ZIP file is possible as long as there is a file with .EXE in the zipped contents. It does not need to be a real executable.**

7. The file will be uploaded, and you will be returned to the **Add Application** page.  
If this installer will be used as a dependency for another app, select Yes.  
Click on **Continue**
8. On the **Details** tab



Enter or Update the items below

**Name:** Update the App name as required

**Application ID:** For an MSI-based installation this will automatically be entered

**Actual File Version:** For an MSI-based installation this will automatically be entered

**Supported Processor:** If this installation requires a 64-bit OS architecture, change to **64-bit**, otherwise 32-bit apps will install on **both** 32-bit and 64-bit OSES.

**Minimum OS:** Select from the drop-down the minimum OS version capable of installing this app  
Update the rest of the entries as required

**Supported Models:** Select Desktop

The other fields are optional

Is Beta

Change Log

Categories

Description

Keywords

URL

Support Email

Support Phone

Internal ID

Copyright

Developer, Developer email, Developer Phone

Cost Center, Cost, Currency

9. (Optional) Select the **Files** tab

**NOTE: If a non-MSI installer is used, this is mandatory**

- If this installation requires another application to be installed first, select the application. That application must have been created and marked as a dependency first.
- If the installation is using an MSI script and there is an .MST available, expand the **App Transforms** section, click **+ ADD** and select the .MST file and click **Save**

- MSI installers also support Patching. If there are .MSP files to add, expand the **App Patches** section, click **+ ADD** and select the .MSP file and click **Save**

- There can also be custom uninstall processes.

**NOTE: This is mandatory when a non-MSI installer is used**

This could be another script, or a command line. If a custom uninstall process exists, expand **App Uninstall Process**, select **Yes**. Select the Script type of **Upload** or **Input**. If Input is selected, enter the command line. If Upload is selected, click on **Upload**, select the script file and click **Save** and enter the command line to execute the script

- (Optional) Select the **Deployment Options** tab

**NOTE: If a non-MSI installer is used, this is mandatory**

- If there are installation conditions, they can be entered here. Detection methods can use the following methods:

- App exists
- App does not exist
- File exists
- File does not exist
- Registry exists
- Registry does not exist

- If a detection method (Data Contingencies) is required, click on **+ ADD**
- Select the Criteria Type
  - **App exists or App does not exist**

Enter the **Application Identifier** – this is the Product code for an MSI-based product

Normally, a specific version is not required, but if one is, select **Equal to**, **Greater than**, or **Less than** and enter the **Version**  
Click **Add**

- **File exists or File does not exist**

Enter the path where the file should or should not be

If there is a specific file version that must be found, select **Equal to**, **Greater than**, or **Less than** and enter the **Version**

Enter the Modified On timestamp. If the file has a newer timestamp, it will be considered met.

Click **Add**

- **Registry exists or Registry does not exist**

Enter the registry path

If there is a specific value that must be confirmed, check the box **Configure Registry Values**

- Enter the Value name, Value Type
- If there is specific data, check the box **Configure Registry Data**

- Enter the Value Data

Click **Add**

- Enter the **Disk Space Required**
- If the computer requires a specific percentage of battery before installation can start, enter that number for **Device Power Required**
- Enter the **RAM Required**

Scroll down to the **How To Install** section

- **Install Context:** Choose if this app is installed for the Device or for the User
- **Install Command:** Enter the command line to perform the installation.

**NOTE: This is mandatory when a non-MSI installer is used**

- **Admin Privileges:** Select Yes or No if Admin privileges are required to perform the installation
- **Device Restart:** If the app install requires a restart, select the appropriate option
- **Retry Count, Retry Interval, Install Timeout:** Update the defaults if required
- **Installer Reboot Exit Code:** If applicable, enter the exit code that will tell the computer a restart is required. E.g. 3010
- **Installer Success Exit Code:** Enter the exit code the installer will return for a successful install

Scroll down to the **When To Call Install Complete** section

**NOTE: This is mandatory when a non-MSI installer is used**

- **Identify Application By:** Select the condition that tells Workspace ONE that app has installed and is complete.
  - **Defining Criteria:** Using the same rules as above for Data Contingencies, create Detection criteria to determine if the application successfully installed
  - **Using Custom Script:** If there is a script to be used, Upload the script, select the Script Type, Command to Run and Success Exit Code.

- (Optional) Select the **Images** tab



The picture uploaded will be shown to user in the app catalog.

- (Optional) Select the **Terms of Use** tab



If there is a specific Terms of Use that must be displayed before the installation select it from the drop down

If the required Terms of Use does not exist, click on **Manage Terms of Use** to Add the Terms of Use text.

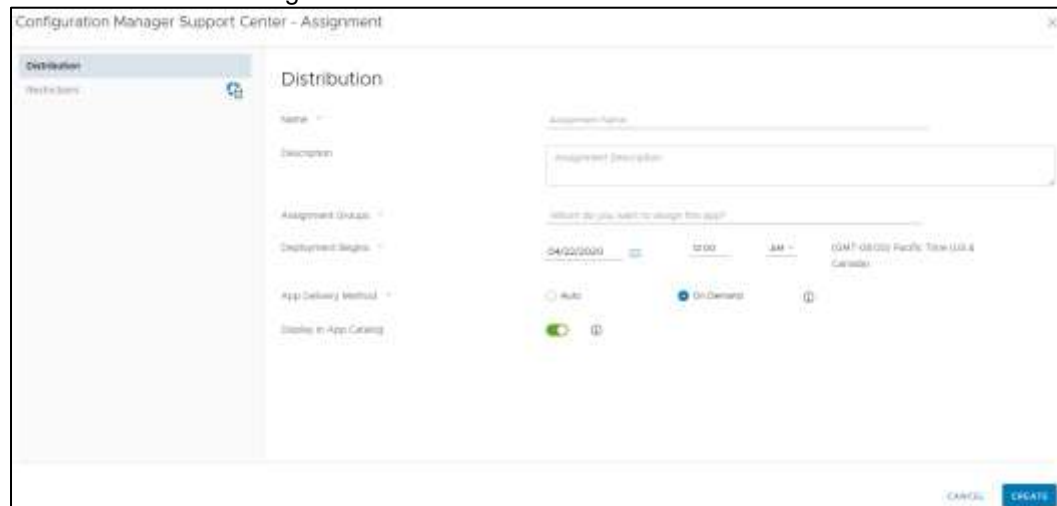
This will open a new tab. After the Terms of Use has been created, close the tab.

- Click on **Save & Assign**



- The Assignment page will be displayed. Assignment is not required at this time. Click Cancel to create the Assignment later, otherwise:

- On the **Distribution Page**



Complete the items on the form:  
**Name:** Enter the Assignment name

- Description:** Enter the description for this deployment
- Assignment Groups:** Enter the group name to receive this app. This must exist beforehand. Enter the first character of the group name and a list of Assignment groups beginning with that character will be displayed. Multiple Assignment groups can be entered To create an Assignment Group, see the section below
- Deployment Begins:** Enter the date and time when the installation is to start
- App Delivery Method:** Select **Auto** to force the installation at the entered Deployment Begins time. Select **On Demand** to allow the user to install from the **App Catalog** when they are ready
- Display in App Catalog:** Move the slider to the right to display in the App Catalog

15. Click on **Create**

CANCEL CREATE

- 16. Additional assignments can be added if required
- 17. Click **Save**
- 18. **Preview Assigned Devices** will list the targeted computers, click **Publish**

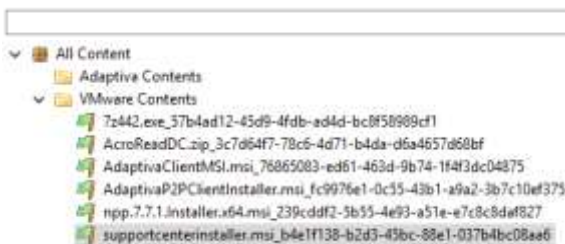
### Viewing the App in the Workbench

When the App is created in the Workspace ONE UEM console, Workspace ONE will contact the ACC which will contact the Adaptiva Server and create a content record which is then visible in the Adaptiva Workbench.

At this time, the Workspace ONE app metadata is only visible in the Adaptiva Workbench.

- 1. Open the Adaptiva Workbench
- 2. Log in with an appropriate account
- 3. From the Home perspective, expand **Content Management** and select **Content Distribution Perspective**
- 4. Under **All Content**, expand **VMware Contents**  
Notice the list of apps

Content Explorer



- 5. Select an app. The GUID after the installation executable is the AirWatch MDM application Identity ID
- 6. In the **Content Distribution Status Viewer**, notice the different Adaptiva Offices the content has been copied to. Select an office  
You will be able to see which computers have downloaded the content, computers with downloads in progress and computers with partial downloads

**NOTE:** There will be no downloads shown until computers assigned to install the app begin the download and report status

### Create Assignment Group

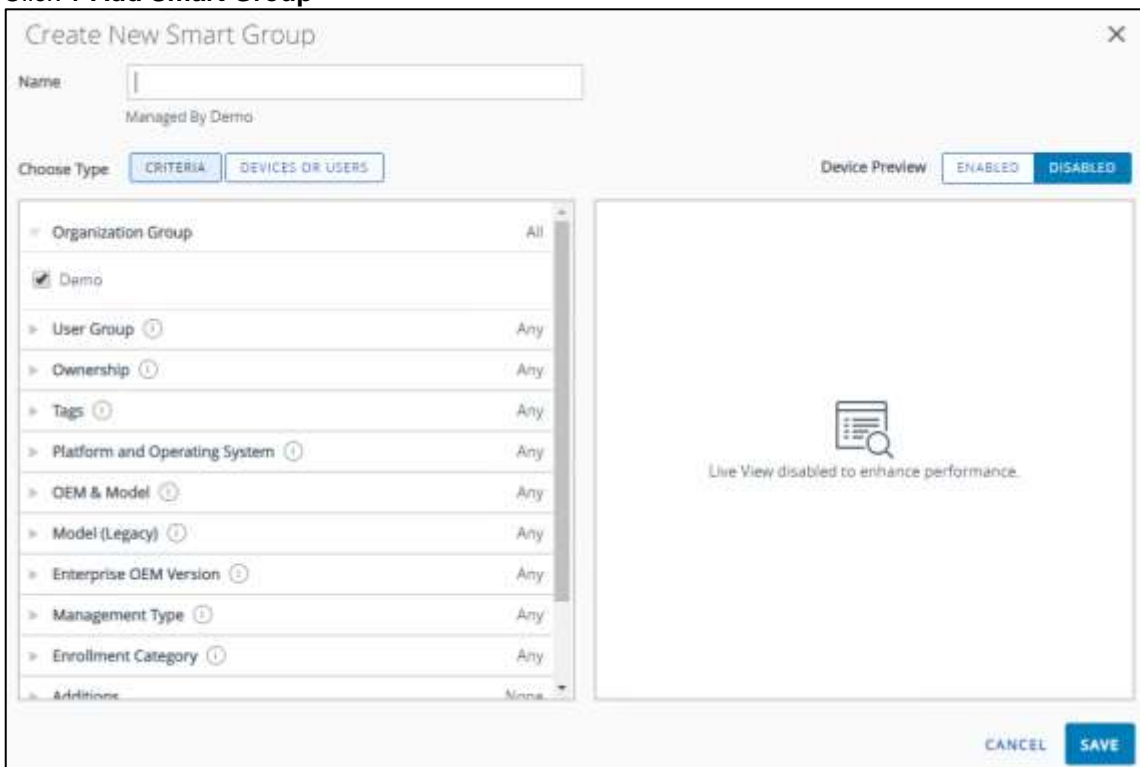
Use the steps below to create a new assignment group to use to target an app with.

- 1. Open a web browser and connect to <https://cn800.airwatchportals.com>
- 2. Log in with your UEM account

3. Select **Groups & Settings, Groups, Assignment Groups**



4. Click **+ Add Smart Group**



5. Select the criteria to be in this group and click **Save**

6. Refer to the section **Workspace ONE – Installing the App – What Does the User See** for more information on installation user experience and content download troubleshooting

## Adaptiva Content

### Using the Adaptiva Web Portal

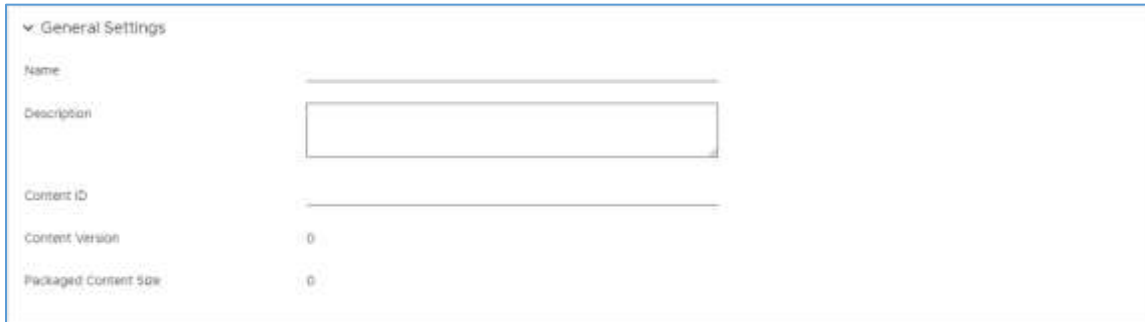
#### Creating Adaptiva Content

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



4. Click **Content Publication, Adaptiva Content**
5. This will open the Publication Status page for Adaptiva content
6. Click on **+ New** to create new Adaptiva content

### General Settings



▼ General Settings

Name

Description

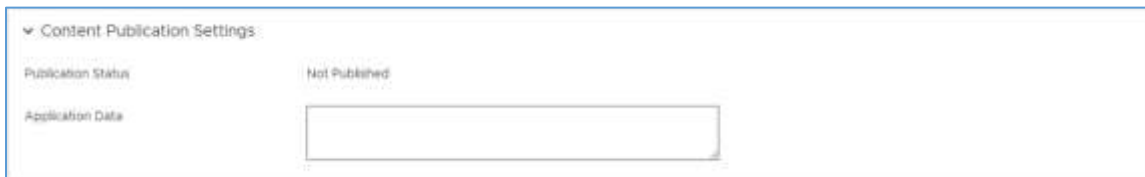
Content ID

Content Version 0

Packed Content Size 0

- **Name** – Enter a display name to identify the content item.
- **Description** – This text field allows you to add a description for the content item (optional). The description will display in a popup when you hover over the name.
- **Content ID** – Enter a unique ID for this content item. This ID must be unique to any other content items in the system, and allowed characters are \$, \_, -, 0-9, a-z, A-Z. The ID will be used to create the content file and in logs.
- **Content Version** – Shows the current version number of the content item. This is a read-only field and will be generated and updated automatically when the item is published.
- **Packed Content Size** – Shows the size of the packed content item in bytes. This is a read-only field and will be generated and updated automatically when the item is published.

### Content Publication Settings



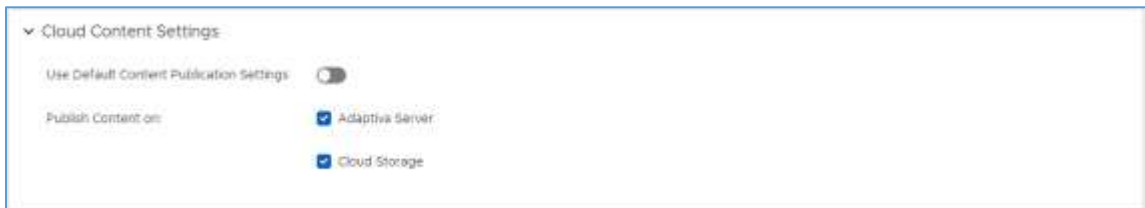
▼ Content Publication Settings

Publication Status Not Published

Application Data

- **Publication Status** – Shows the publication status of the content item. This is a read-only field and will be updated once the content item is created and updated.
- **Application Data** – Any string can be used as a description.

### Cloud Content Settings



▼ Cloud Content Settings

Use Default Content Publication Settings

Publish Content on:  Adaptive Server  Cloud Storage

- **Use Default Content Publication Settings** – Toggle this to the left to disable and use settings different than what is defined in Cloud Storage, Adaptiva Content Publication. The Default is on (slid to the right).
- **Publish Content on:** Check the appropriate box

## Content Details

▼ Content Details

Source Type:  Local Source Path  
 Network Source Path  
 CDN URLs

Source Path: \_\_\_\_\_

Actual File Name: \_\_\_\_\_

Publish Unchanged ⓘ

Compress Content ⓘ

Encrypt Content ⓘ

Flat File Publication ⓘ

- **Source Type** – There are 3 options to choose from where the source files are to be obtained:
  - **Local Source Path** – Choose this option to select source files from a local path on the Adaptiva server.
  - **Network Source Path** – Choose this option to select source files from a remote network source path.
  - **CDN URLs** – Choose this option to select source files from a cloud-hosted provider.
- **Source Path** – Type the full path, UNC, or URL to the source folder/files that you want to use for this package. These file(s) will be used to create the content file within the Adaptiva Content Library when the item is published.
- **Network Access Account** – If the source type is **Network Source Path**, this allows you to specify account credentials to establish the connection to the source UNC. Specify the **Domain**, **User Name** and **Password** in the associated fields (optional).
- **CDN URLs** – If the source type is **CDN URLs** - this points to one or more URLs to get content from the cloud-if your hosted it there. (i.e. AWS, Azure, Akamai)
  - **Actual File Name** – CDN URL Only feature, allows you to rename the file being downloaded from the CDN.
  - **Content Hash (SHA 256)** – CDN URL Only, allows you to specify the SHA256 hash of the file to be downloaded. OneSite will validate the downloaded file to ensure that it matches.

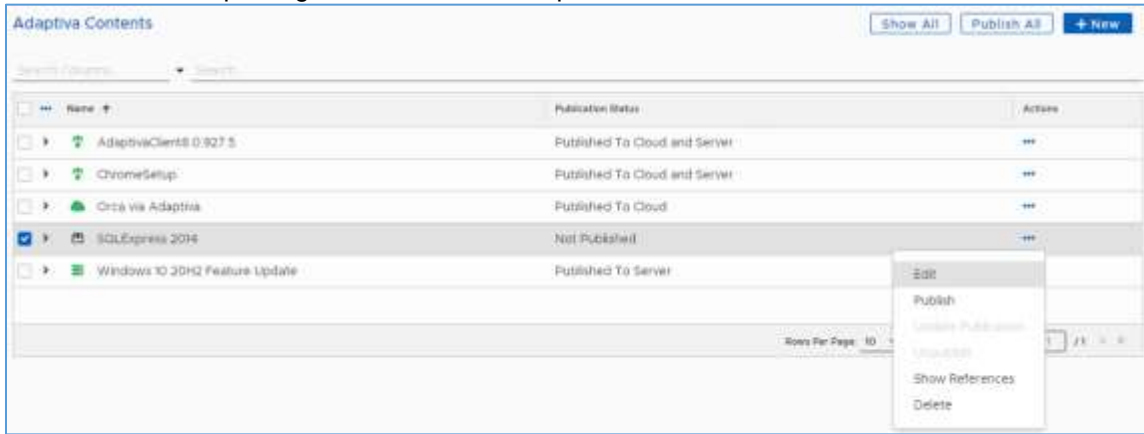
**NOTE: The hash value must be retrieved from the CDN provider. This differs with each provider so you will need to get instructions from your provider.**

- **Publish Unchanged** – Select this option only when publishing a single file that is already compressed (zip, wim, etc.)
  - **Compress Content** – Select this option to compress the content when the source files are added to the content file. This is enabled (slid to the right) by default.
  - **Encrypted Content** – Select this option if you want the content to be encrypted
  - **Flat File Publication** – If you specify a folder for the source path, all sub folder structure and contents will be maintained when added to the content file. Check this option if you would like all files to be in a flat folder structure when added to the content file (no subdirectories).
7. Once you have entered the required information, scroll up to the top and click on **Save** or **Save & Publish** to create the package.

## Publishing Adaptiva Content

Once you have created Adaptiva content items, you then need to publish them to make them available for download.

1. Select the desired package and click on the ellipses, ..., under **Action**, select **Publish**



2. You will notice that the icon will change to several other icons as the content is being published. Depending on the size of the content this may take some time. Once the content is published, the icon will change to , published to the server, , published to the CDN, or , published to both the server and the CDN

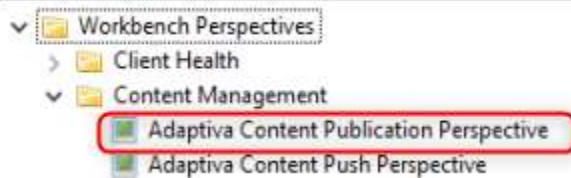
**NOTE:** In the case of a publication error, click the ellipses, ..., and select **Edit** to open the editor where additional error information will be displayed.

3. Once the content is published, it is now ready to use for content push

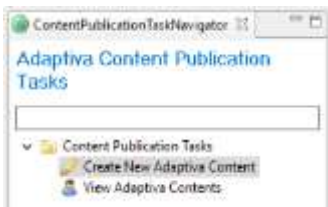
## Using the Adaptiva Workbench

### Creating Adaptiva Content

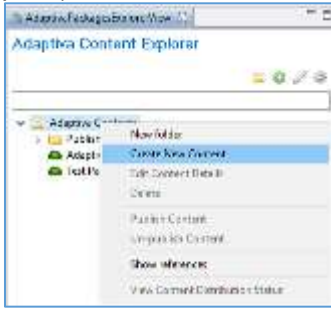
1. From the Home perspective, expand **Content Management** and select **Adaptiva Content Publication Perspective**



2. To create a new Adaptiva Content item, click on **Create New Adaptiva Content** in the **Adaptiva Content Publication Tasks** view.



You can also right-click on **Adaptiva Contents** in the **Adaptiva Content Explorer** (right-hand pane) and select **Create New Content**



3. Complete the form to create an Adaptiva Package item.

### Basic Content Details Settings:

The screenshot shows the 'Adaptiva Content' form. At the top right are 'Save' and 'Close' buttons. Below is a section titled 'Basic Content Details' with a dropdown arrow. It contains five input fields: 'Content Name' (empty), 'Content Description' (empty), 'Unique Content ID' (empty), 'Content Version' (value: 0), and 'Packed Content Size' (value: 0).

- **Content Name** – Enter a display name to identify the content item. This name will be shown when viewing the item within the **Content Explorer** in the workbench and in reporting.
- **Content Description** – This text field allows you to add a description for the content item (optional). The description will display in a popup when you hover over the name.
- **Unique Content ID** – Enter a unique ID for this content item. This ID must be unique to any other content items in the system, and allowed characters are \$, \_, -, 0-9, a-z, A-Z. The ID will be used to create the content file and in logs.
- **Content Version** – Shows the current version number of the content item. This is a read-only field and will be generated and updated automatically when the item is published.
- **Packed Content Size** – Shows the size of the packed content item in bytes. This is a read-only field and will be generated and updated automatically when the item is published.

### Content Publication Settings:

The screenshot shows the 'Content Publication Settings' form. It has a dropdown arrow at the top left. It contains two fields: 'Publication Status' (value: NOT PUBLISHED) and 'Application Data' (empty).

- **Publication Status** – Shows the publication status of the content item. This is a read-only field and will be updated once the content item is created and updated.
- **Application Data** – Any string can be used as a description.

## Content Source Details:

▼ Content Source Details

Source Type:  Local Source Path  Network Source Path  CDN Urls

Source Path:

Network Access Account: User Domain:  User Name:  Password:

CDN Urls (URLs are ; Separated):

Actual File Name:

Content Hash (SHA 256):

Publish Unchanged

Compress Content

Encrypted Content

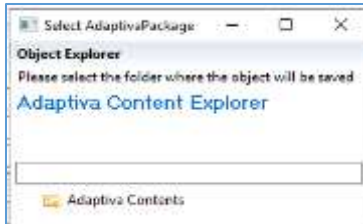
Flat File Publication

- **Source Type** – There are 3 options to choose from where the source files are to be obtained.
  - **Local Source Path** – Choose this option to select source files from a local path on the Adaptiva server.
  - **Network Source Path** – Choose this option to select source files from a remote network source path.
  - **CDN URLs** – Choose this option to select source files from a cloud-hosted provider.
- **Source Path** – Type the full path, UNC, or URL to the source folder/files that you want to use for this package. These file(s) will be used to create the content file within the Adaptiva Content Library when the item is published.
- **Network Access Account** – If the source type is **Network Source Path**, this allows you to specify account credentials to establish the connection to the source UNC. Specify the **Domain**, **User Name** and **Password** in the associated fields (optional).
- **CDN URLs** – If the source type is **CDN URLs** - this points to one or more URLs to get content from the cloud-if your hosted it there. (i.e. AWS, Azure, Akamai)
  - **Actual File Name** – CDN URLs Only feature, allows you to rename the file being downloaded from the CDN.
  - **Content Hash (SHA 256)** – CDN URLs Only, allows you to specify the SHA256 hash of the file to be downloaded. OneSite will validate the downloaded file to ensure that it is valid.

**NOTE:** *The hash value must be retrieved from the CDN provider. This differs with each provider so you will need to get instructions from your provider.*

- **Publish Unchanged** – Select this option only when publishing a single file that is already compressed (zip, wim, etc.)
- **Compress Content** – Select this option to compress the content when the source files are added to the content file. Checked by default.
- **Encrypted Content** – Select this option if you want the content to be encrypted
- **Flat File Publication** – If you specify a folder for the source path, all sub folder structure and contents will be maintained when added to the content file. Check this option if you would like all files to be in a flat folder structure when added to the content file (no subdirectories).

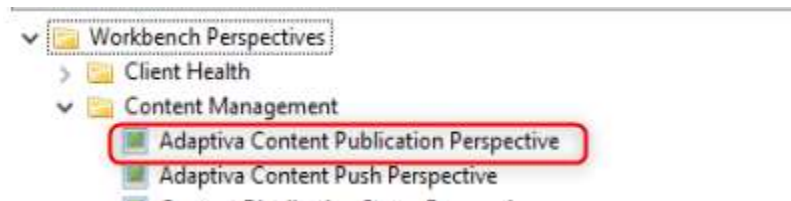
4. Once you have entered the required information, scroll up to the top and click on **Save** to create the package.
5. Select the folder where the object will be saved. The default first folder is **Adaptiva Contents**.



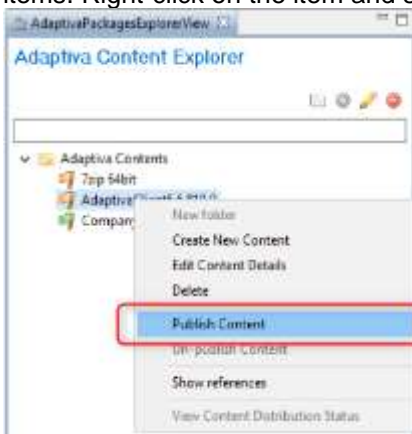
## Publishing Adaptiva Content

Once you have created Adaptiva content items, you then need to publish them to make them available for download.

1. Navigate to the **Adaptiva Content Publication Perspective** within the **Content Management** folder:



2. In the right-hand pane you will find the **Adaptiva Content Explorer**, this lists all Adaptiva content items. Right-click on the item and select **Publish Content**



You will notice that the orange flag icon will change to an hourglass as the content is being published. Depending on the size of the content this may take some time. Once the content is published, the color of the flag icon will turn green.

**NOTE:** *In the case of a publication error which may be indicated by a red flag icon, double-click the content to open the settings editor where additional error information will be displayed.*

3. Once the content is published, it is now ready to use in a content push policy

# Content Push

## Introduction

The Content Push feature is a powerful feature that allows any Adaptiva-published content (this excludes Workspace ONE apps) to be distributed to Adaptiva clients without using a deployment from ConfigMgr or Intune. The primary purpose of Content Push is pre-staging content to locations where it will be needed for future use. For example, ConfigMgr OSD content can be pre-staged at the location where machines will be imaged, so that it will be available for rapid copying from local Adaptiva peers when requested.

There are several ways to create a Content Push Policy. There are slight differences when using the Adaptiva Workbench, but each of the methods allow you to pre-stage content to the target devices.

Using the Adaptiva Web Portal

- OneSite Anywhere, OneSite ConfigMgr Edition or OneSite Intune Edition, Content Push

Using the Adaptiva Workbench

- Content Management > Adaptiva Content Push Perspective
- OneSite > OneSite – Content Push Perspective

***NOTE: VMWare Workspace ONE content is only published on their Content Delivery Network and will not be in the Adaptiva Content Library on the Adaptiva server or Cloud store. The Adaptiva Server will receive metadata information so clients can locate the content. Because there is only metadata, content push policies cannot include Workspace ONE content***

## Overview

Creation of a OneSite Content Push Policy is simple process. When a Content Push Policy is created, you specify a schedule on which the policy will be run, against a target collection or group, with a defined list of contents. The policy is sent to the target clients and on a set schedule the content is downloaded. As always with OneSite, the content will only cross a WAN link once for each office targeted, except VPN-configured offices, before being shared with OneSite peers at those locations.

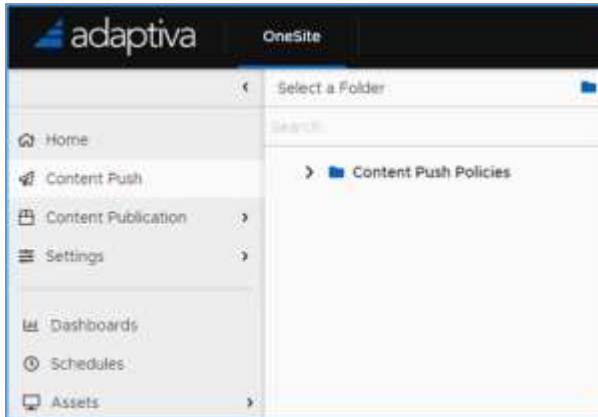
Advanced features of Content Push allow control over parameters that are used in the download; if and where the content is unpacked following the download; specification of workflows that can be triggered by various phases of the policy; and a post-download command to be executed following the download.

## Features

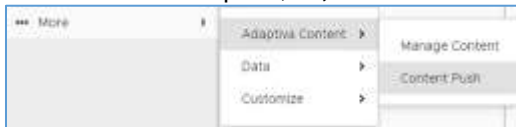
- Pre-stage content to Adaptiva clients, in any office(s), without involving ConfigMgr or Intune.
- Full control over policy start-time, expiration-time, and execution schedule.
- Automatically synchronize content changes. Applies to ConfigMgr Packages as well as Task Sequences and other content types, including Intune Apps.
- Full control over content download settings, such as Priority, Timeout, Do Not Download on Battery, Do Not Download Over WAN, and Transport Protocol(s) used.
- Unpack content to specified location and execute post-download command.
- Pre-Download, Download, Post-Download, and Content Push Server Workflows provide virtually limitless capability.
- IntelliStage grants administrators the ability to pre-determine a number of clients that are intelligently selected to cache content in each office.

## Using the Adaptiva Web Portal

1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Go to OneSite ConfigMgr Edition** or **Go to OneSite Intune Edition** or click **OneSite Anywhere, OneSite ConfigMgr Edition** or **OneSite Intune Edition**
4. Select **Content Push**



OR click on the ellipses, ..., **More** and select **Adaptiva Content > Content Push**



5. Click on **+ New** to create a new Content Push policy  
**General Settings**

The screenshot shows the 'General' settings section for a new Content Push policy. It contains two text input fields: 'Name' with a placeholder 'Policy name' and 'Description' with a placeholder 'Policy description'. Below the fields is a 'Show More' link.

- **Name** – (Required) Enter a display name to identify the Content Push Policy.
- **Description** – This text field allows you to add a description for the Content Push Policy (optional).

Click **Show More** to display the following:

The screenshot shows the expanded 'General Settings' form. It includes the following fields and controls:
 

- Start Time**: A date and time picker showing 8/6/2020, 2:54:25 PM.
- End Time**: A date and time picker showing 'Choose Date'.
- Use Server Time**: A toggle switch that is turned on.
- Encrypt Policy**: A toggle switch that is turned off.
- Policy Enabled**: A toggle switch that is turned on.
- Parent Folder**: A 'Select Folder' dropdown menu with a 'BROWSE' button next to it.

- **Start Time** – The time the policy will start on the target clients. By default, this is the current time.



- **End Time** – The time the policy will expire on the target clients, By default, this is empty so the policy will run forever.

Clicking on the calendar icon for the above two settings will display the following:



Use the v to select the month and the year or use the < > to cycle through the months.

Click the button to toggle the 24hr slider to the right to enable 24 hour time (military time)

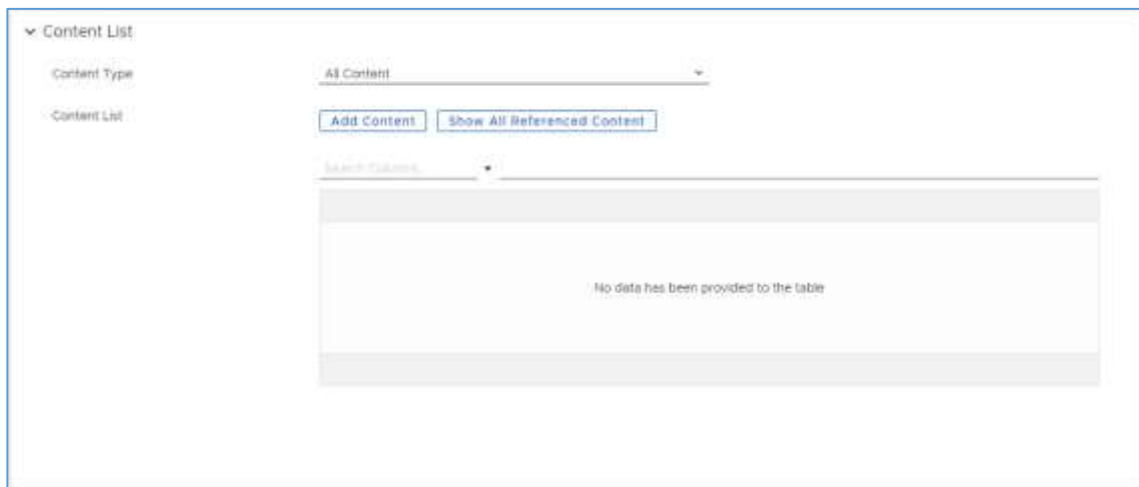
Enter the time the Content Push Policy is to start.

Click anywhere else to close the calendar window

- **Use Server Time** – Enabled (slid to the right) by default. All target clients will run the policy at the same time. When this is disabled, clients will run the policy based on their time.
- **Encrypt Policy** – Disabled (slid to the left) by default. Encrypts the policy settings.
- **Policy Enabled** – Enabled (slid to the right) by default. Enables the policy to start immediately upon saving.
- **Parent Folder** – Click browse to select a folder to organize the Content Push Policies

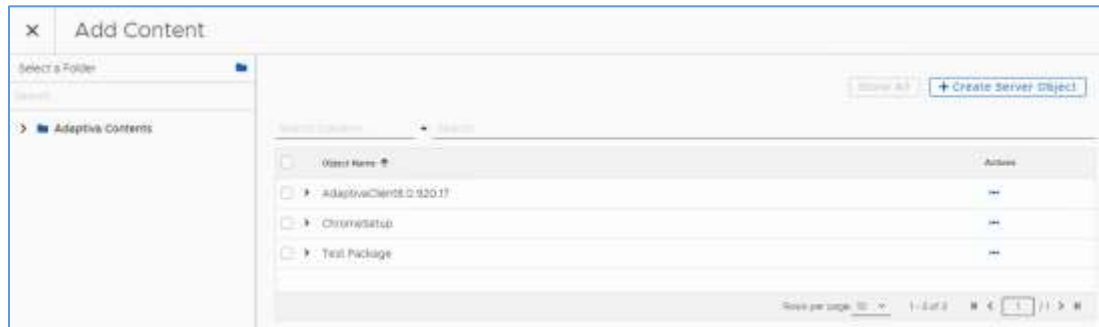
## Content List

The Content List is used to specify what content will be deployed by this Content Push Policy.



- **Content Type** – Filters the list of content added. Select All Content to show all content items included in this Content Push policy
- **Content List** – Displays the Content in the Content Push Policy

- **Add Content** - Click on **Add Content, <content type>** to display the list of respective content items.

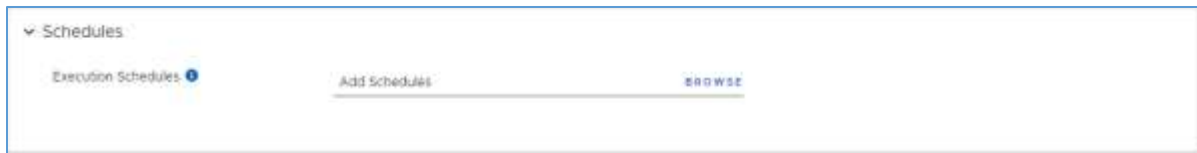


Check the box next to each content item to be added to the Content Push policy  
Click **Add to List** to return to the Content Push Policy

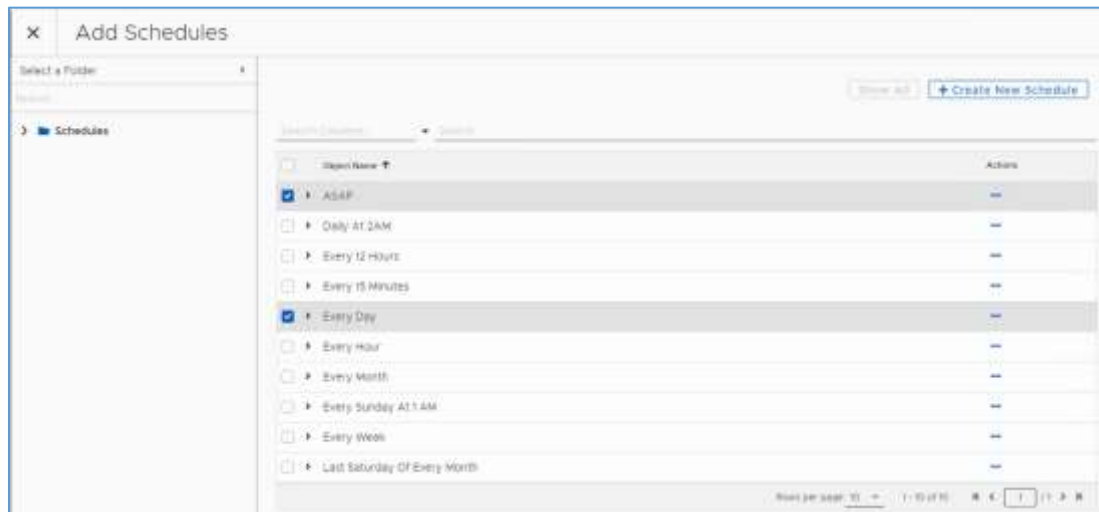
- **Show All Referenced Content** – When a Task Sequence has been added to the Content List, this will show all the referenced content in the task sequence along with any individually added items.

## Schedules

The Execution Schedule is a mandatory parameter.



1. Click **Browse** to select the schedule to add



**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.

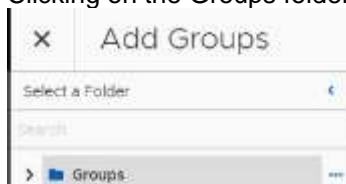
A recurring schedule will take effect after the configured start time. When a task is scheduled for a particular day, it will run at the time of day provided in the start time. For example, if a policy is scheduled to run on the last day of the month, starting on March 5th, at 5pm, it will fire on March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

2. Check one or more boxes next to the desired schedule(s) or click **+Create New Schedule** to create a new Schedule
3. Click **Add to List** to return to the Content Push Policy

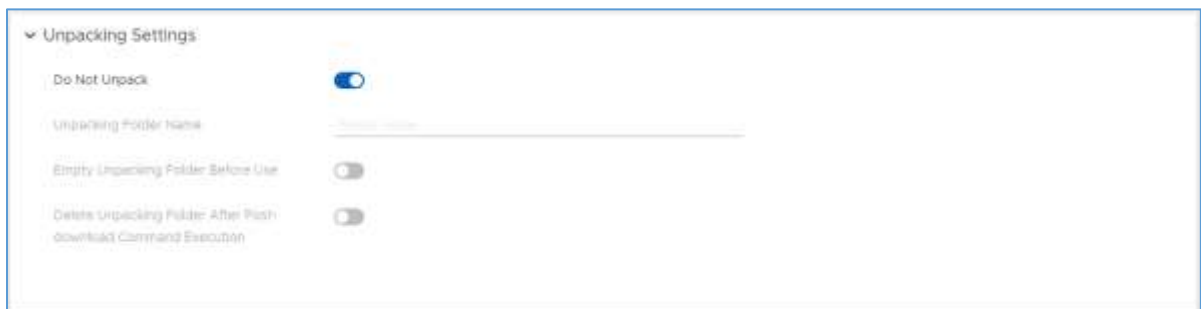
### Target Groups



- **Use All Adaptiva Clients** – Enable (slide to the right) to target All Adaptiva clients
- **Target Groups** – Or click on Browse to select a specific Adaptiva Group or ConfigMgr collection. Check the box by the group name(s) and click Add to List to return to the Content Push Policy. Clicking on the Groups folder will list only the Adaptiva Groups



### Unpacking Settings



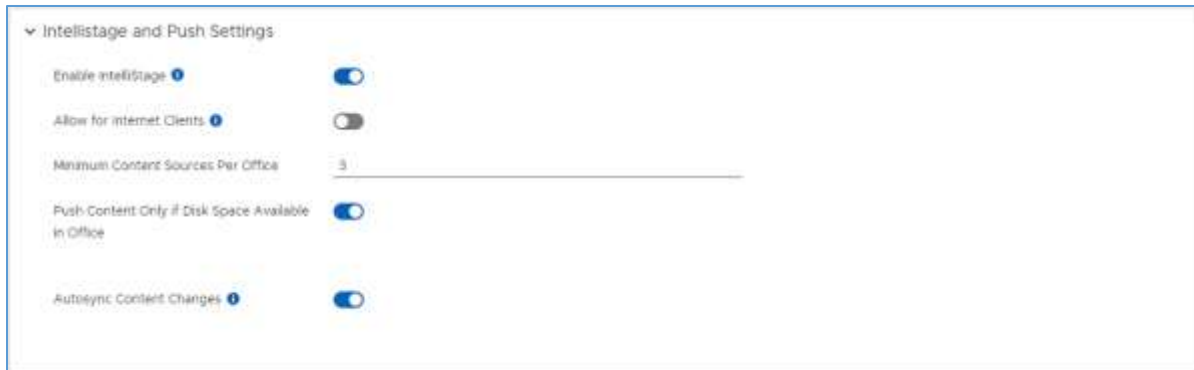
- **Do Not Unpack** – Enabled (slid to the right) by default. Disable to unpack the content and specify a folder destination
- **Unpacking Folder Name** – Enter the folder where the content should be unpacked
- **Empty Unpacking Folder Before Use** – Disabled (slid to the left) by default. Enable to delete the content of the Unpacking folder first
- **Delete Unpacking Folder After Post-download Command Execution** – Disabled (slid to the left) by default. Enable to delete the unpacking folder after running the command line.

### IntelliStage and Push Settings

IntelliStage Settings which are enabled by default, instructs the clients targeted by a Content Push Policy to create a minimum number of copies of the content to the best suited clients in each office.

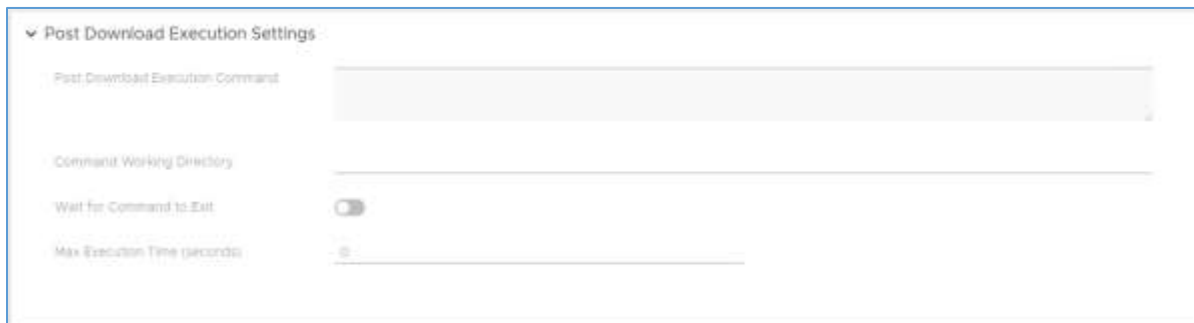
Operating System Deployment is one of many use cases for this feature. An administrator needing to ensure that OSD content will be present when machines are scheduled to be imaged could create a policy to push out the Task Sequence contents to *X* machines per office (*X* is the number of desired copies per office), and schedule the policy to run periodically. After pre-staging the content, if one of the sources leaves the network, when the policy runs it will cause another source to be created. The newly elected source will copy the content from a peer, thereby maintaining the desired number of sources per office.

If IntelliStage is not used, the Content Push policy will pre-stage the content on all machines in the targeted Adaptiva Group. This may be desirable for software that will go to many machines or to just a few.



- **Enable IntelliStage** – Enabled (slid to the right) by default.
- **Allow for Internet Clients** – Disabled (slid to the left) by default. When enabled, internet-based clients will execute Intellistage policies
- **Minimum Content Sources Per Office** – Enter the minimum number of clients that will receive the content
- **Push Content Only if Disk Space Available in Office** – Enabled (slid to the right) by default. When enabled the policy will evaluate if there is enough actual free disk space in the virtual SAN in the targeted Office(s) before initiating content download. (Standard determination is based on potential free space which could cause excessive file deletion to make room for the new content.)
- **Autosync Content Changes** – Enabled (slid to the right) by default. If enabled, when the Adaptiva Server detects changes to the source content, it will automatically push those changes out to the group(s) and/or collection(s) targeted by the policy. If the content list in the policy is a Task Sequence, any changes to content referenced by the Task Sequence will result in the changes being automatically pushed to the target collections.

### Post Download Execution Settings

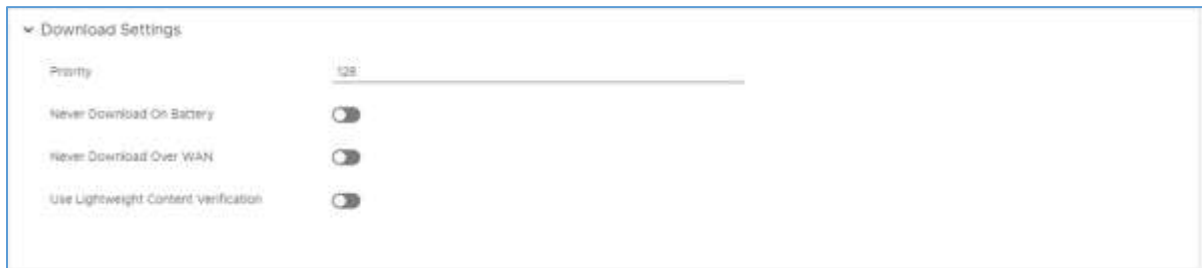


- **Post Download Execution Settings** – IntelliStage must be disabled first. Enter the command line to be executed after the content is downloaded and unpacked
- **Command Working Directory** – Enter the working directory, if required
- **Wait for Command to Exit** – Disabled (slid to the left) by default. Enable to have Adaptiva wait until the executed command completes.
- **Max Execute Time (seconds)** – Enter the number of seconds to wait for the executed command to complete. 3600 seconds is the default.

## Advanced Settings

These settings override the default download settings, or the download settings set on the content item.

### Download Settings

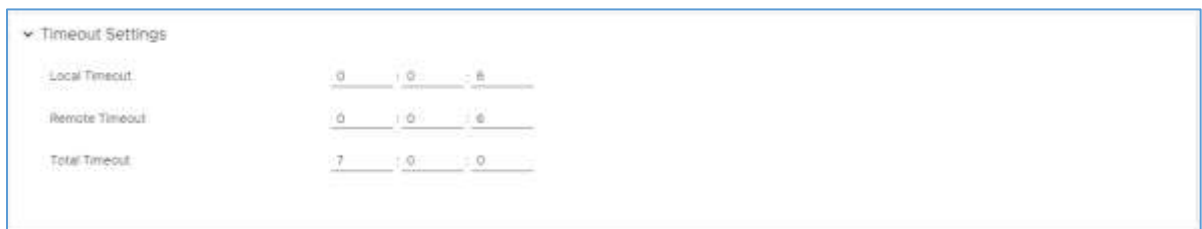


The screenshot shows the 'Download Settings' panel with the following configurations:

Setting	Value
Priority	128
Never Download On Battery	<input type="checkbox"/>
Never Download Over WAN	<input type="checkbox"/>
Use Lightweight Content Verification	<input type="checkbox"/>

- **Priority** – Enter a priority from 1 to 255. The highest priority will be downloaded first.
- **Never Download On Battery** – Disabled (slid to the left) by default. When selected, laptops running on battery power will not attempt to download the content.
- **Never Download Over WAN** – Disabled (slid to the left) by default. When selected, the content is set to never download over the WAN or between offices.
- **Use Lightweight Content Verification** – Disabled (slid to the left) by default. When enabled only the file size is checked, not the file hash.

### Timeout Settings

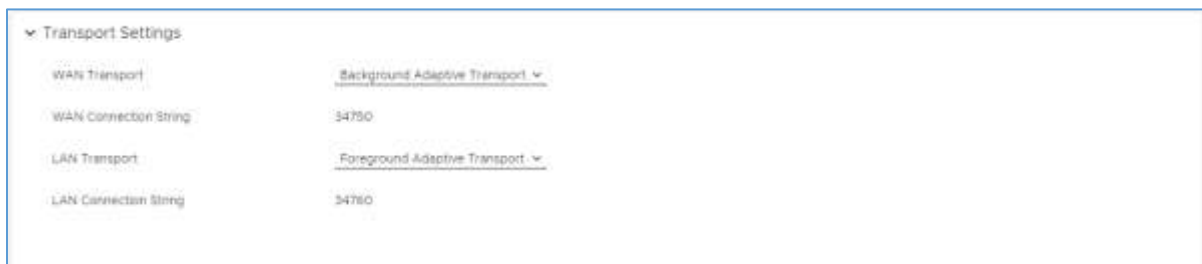


The screenshot shows the 'Timeout Settings' panel with the following configurations:

Setting	Value
Local Timeout	0 : 0 : 0
Remote Timeout	0 : 0 : 0
Total Timeout	7 : 0 : 0

- **Timeout Settings** – Determines how long clients will wait for the package before abandoning the request.

### Transport Settings



The screenshot shows the 'Transport Settings' panel with the following configurations:

Setting	Value
WAN Transport	Background Adaptive Transport
WAN Connection String	34750
LAN Transport	Foreground Adaptive Transport
LAN Connection String	34760

These settings control the transport protocol which will be used while downloading content across the WAN and over the LAN. By default, WAN downloads are configured to use Background Adaptive Transport and will prevent interference with other traffic. The speed of the download will automatically adapt to the amount of actual unused bandwidth on that network. The Foreground Adaptive

Transport, which is used on LAN connections by default, will still use our UDP based protocol, with checkpoint restart capability but will not perform Predictive Bandwidth Harvesting.

### Content Download Receipts Settings

▼ Content Download Receipts Settings

LAN Download Receipts

- Send Download Started Receipt
- Send Download Progress Receipt
- Send Download Stopped Receipt

WAN Download Receipts

- Send Download Started Receipt
- Send Download Progress Receipt
- Send Download Stopped Receipt

**NOTE:** *It is not recommended to change these settings*

### Content Download Status Settings

▼ Content Download Status Settings

Send ConfigMgr Status Messages

- Content Download Starts On Client
- Package Content Completes Successfully
- Content Download Failed On Client
- Content Download In Progress:

### Content Push Workflows

Content Push is a workflow-based feature. The workflows that are executed by a Content Push Policy can be selected in the **Content Push Workflows** section. Individual workflows can be edited via the Workflow Designer Perspective in the Workbench. The following sequence of events takes place when a Content Push Policy schedule fires. Events 2-4 take place asynchronously at the client:

1. Content Push Server Workflow is executed at the server.
2. Pre-Download Workflow
3. Either the Download Workflow or the Office Content Push Download Workflow
4. Post-Download Workflow

▼ Content Push Workflows

Pre-Download Workflow	<u>Pre-Download Workflow</u>	<a href="#">BROWSE</a> <a href="#">X</a>
Download Workflow	<u>Content Download Workflow</u>	<a href="#">BROWSE</a> <a href="#">X</a>
Post-Download Workflow	<u>Post-Download Workflow</u>	<a href="#">BROWSE</a> <a href="#">X</a>
Content Push Server Workflow	<u>Content Push Server Workflow</u>	<a href="#">BROWSE</a> <a href="#">X</a>
Office Content Push Download Workflow	<u>Add Workflows</u>	<a href="#">BROWSE</a>

- **Pre-Download Workflow** - The Pre-Download Workflow is executed before content download begins. By default, this workflow does nothing.
- **Download Workflow** - The Download Workflow does the work of downloading the content and reporting status.
- **Post-Download Workflow** - The Post-Download Workflow is executed after all content referenced by the policy has been downloaded.

- **Content Push Server Workflow** - This workflow executes whenever the Content Push policy schedule fires. By default, this workflow does nothing.
- **Office Content Push Download Workflow** - If the IntelliStage setting is enabled in the policy, then this workflow replaces the Content Download Workflow in the policy execution.

### Server Workflows

▼ Server Workflows		
Server Policy Created Workflow	Policy Created Workflow	<a href="#">BROWSE</a> <a href="#">X</a>
Server Policy Updated	Policy Updated Workflow	<a href="#">BROWSE</a> <a href="#">X</a>
Server Policy Enabled	Policy Enabled Workflow	<a href="#">BROWSE</a> <a href="#">X</a>
Server Policy Disabled	Policy Disabled Workflow	<a href="#">BROWSE</a> <a href="#">X</a>
Server Policy Deleted	Policy Deleted Workflow	<a href="#">BROWSE</a> <a href="#">X</a>
Server Policy Status	Add Workflows	<a href="#">BROWSE</a> <a href="#">X</a>

### Client Workflows

▼ Client Workflows		
Client Policy Assigned Workflow	Default Policy Assignment Client Workflow	<a href="#">BROWSE</a> <a href="#">X</a>
Client Policy Enabled Workflow	Default Policy Enable Client Workflow	<a href="#">BROWSE</a> <a href="#">X</a>
Client Policy Disabled Workflow	Default Policy Disable Client Workflow	<a href="#">BROWSE</a> <a href="#">X</a>
Client Policy Deleted Workflow	Default Policy Delete Client Workflow	<a href="#">BROWSE</a> <a href="#">X</a>
Client Policy Execution Workflow	Content Push Policy Execution Workflow	<a href="#">BROWSE</a> <a href="#">X</a>

When using Intellistage, change the Client Policy Execution Workflow to use the **Content Push Policy Execution Workflow - SuperRVP Only**. This assumes the target group includes all computers in one or more offices.

**Close** the Advanced Settings page to return to the Content Push Policy

Click **Save**

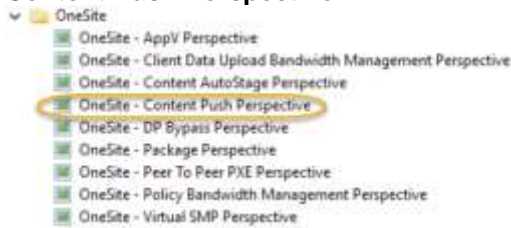
### Executing the Policy

After the Content Policy has been created, the policy can be run

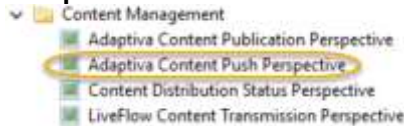
Under **Actions**, click the ellipses, ..., and select **Run Policy** to execute the policy on all target clients

## Using the Adaptiva Workbench

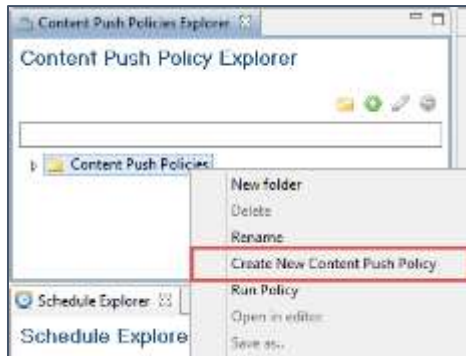
- ❑ In version 5.6 or later, to push content, expand the **OneSite** folder and open the **OneSite – Content Push Perspective**



OR Expand the **Content Management** folder and open the **Adaptiva Content Push Perspective**.



- ❑ In the **Content Push Policy Explorer** pane, right-click the **Content Push Policies** folder and in the context menu, select **Create New Content Push Policy**.



- ❑ The **Content Push Policy Settings** editor should appear in the center of the Workbench with four tabs: General, Content List, Advanced Content Push Settings, and Policy Workflows. Below the editor in the default perspective arrangement is the Generic Errors view. This shows the mandatory parameters that must be defined in order to run the policy.

Component	Setting type	Description	
NameText	General	Please specify the content server polic...	Resolve
ScheduleObjectList	General	No Schedule is defined for this Policy	Resolve
ObjectList1	Content List	Please specify atleast one content to b...	Resolve
GroupObjectList	General	No Target collection is defined for this...	Resolve

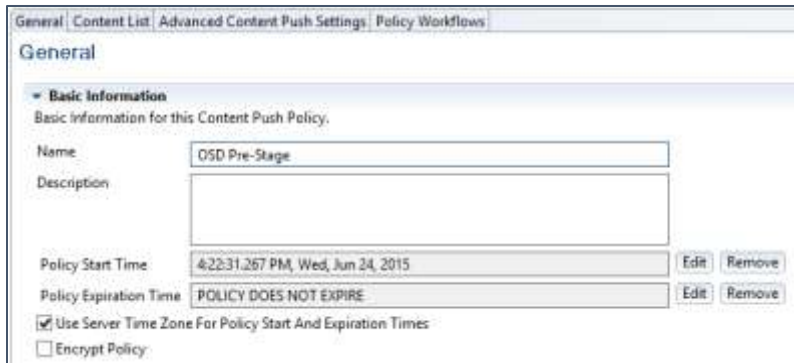
## General Settings Tab

### Basic Information

In the **Basic Information** section of the editor, enter a **Name** (required), and a **Description** (optional). Notice that after the Name was entered, the NameText warning disappears from the Generic Errors view.



To set a **Policy Start Time** or **Policy Expiration Time** (both optional), click on the **Edit** button next to each option. There are also options to **Use Server Time Zone for Policy Start and Expiration** and **Encrypt Policy**.



## IntelliStage Settings

IntelliStage Settings which are enabled by default, instructs the clients targeted by a Content Push Policy to create a minimum number of copies of the content to the best suited clients in each office.

Operating System Deployment is one of many use cases for this feature. An administrator needing to ensure that OSD content will be present when machines are scheduled to be imaged could create a policy to push out the Task Sequence contents to *X* machines per office (*X* is the number of desired copies per office), and schedule the policy to run periodically. After pre-staging the content, if one of the sources leaves the network, when the policy runs it will cause another source to be created. The newly elected source will copy the content from a peer, thereby maintaining the desired number of sources per office.

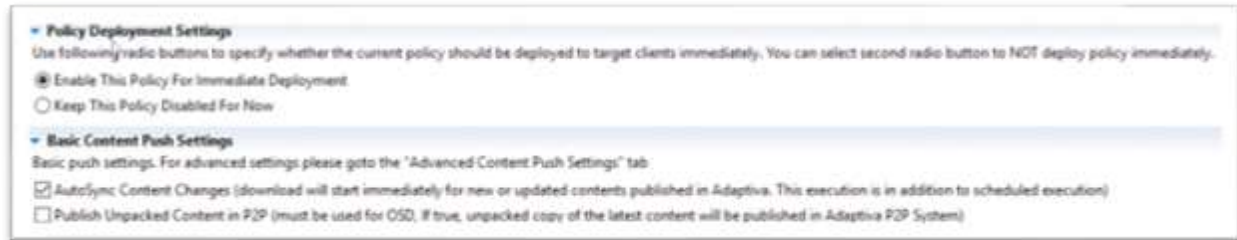
If IntelliStage is not used, the Content Push policy will pre-stage the content on all machines in the targeted Adaptiva Group. This may be desirable for software that will go to many machines or to just a few.

To enable IntelliStage, simply check the box **Enable IntelliStage For Content Push** and specify the minimum number of content sources per office.



By enabling the **Push content only if disk space is available in the office** option, the policy will evaluate if there is enough actual free disk space in the virtual SAN in the targeted Office(s) before initiating content download. (Standard determination is based on potential free space which could cause excessive file deletion to make room for the new content.)

## Policy Deployment Settings



The screenshot shows a configuration window with two sections. The first section, 'Policy Deployment Settings', contains a heading and a paragraph: 'Use following radio buttons to specify whether the current policy should be deployed to target clients immediately. You can select second radio button to NOT deploy policy immediately.' Below this are two radio buttons: 'Enable This Policy For Immediate Deployment' (which is selected) and 'Keep This Policy Disabled For Now'. The second section, 'Basic Content Push Settings', contains a heading and a paragraph: 'Basic push settings. For advanced settings please goto the "Advanced Content Push Settings" tab'. Below this are two checkboxes: 'AutoSync Content Changes (download will start immediately for new or updated contents published in Adaptiva. This execution is in addition to scheduled execution)' (which is checked) and 'Publish Unpacked Content in P2P (must be used for OSD, if true, unpacked copy of the latest content will be published in Adaptiva P2P System)' (which is unchecked).

The Policy Deployment Settings allow the policy to be enabled for immediate deployment or disabled for later use.

### Basic Content Push Settings

**AutoSync Content Changes** - If this option is checked, when the Adaptiva Server detects changes to the source content, it will automatically push those changes out to the group(s) and/or collection(s) targeted by the policy. If the content list in the policy is a Task Sequence, any changes to content referenced by the Task Sequence will result in the changes being automatically pushed to the target collections.

**Publish Unpacked Content in P2P (must be used for OSD)** - With this option checked, as soon as the content reaches the Adaptiva Cache on the target clients it will be unpacked into a subfolder under the AdaptivaCache folder, and a share will be created. OSD clients will always request unpacked content and will be pointed to these shares.

**NOTE:** *If you are using version 5.6 or later, and you prefer not to use file shares and the local account created by the client installation, please see the OneSiteDownloader and OSD Content Push Shares in the OSD User Guide.*

### Execution Schedules and Service Window Profiles

The Execution Schedule is a mandatory parameter. The schedule may be dragged from the **Schedule Explorer** or added by clicking the **Add Schedule** button. Additional schedules may be created using the Schedule Editor.

**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.

By default, the box is checked to use the Service Window if one exists in the selected schedule.

**Execution Schedules And Service Window Profiles**

Specify Schedule(s) for when this Policy should be run. The policy will execute on the client with changes" settings is selected above

ASAP

Daily At 2AM

Use the Service Window in the Schedule(s) if it exists.

Override Schedule(s) Service Window using the following Profile

## Target Collections

Drag one or more collections from either the **SCCM Collections Explorer** or **Adaptiva Groups Explorer** into the **Target Collections** field, or click the **Add Collections** button to choose a ConfigMgr collection (Adaptiva Groups must be dragged from the **Adaptiva Groups Explorer** or alternatively, right-click in the Target Collection box and select Add object. Select the group and click OK.). All machines in the specified group(s)/collection(s) will be targeted to receive the content. The exception to this rule is if IntelliStage is being used, in which case, only the specified number of machines per office will receive the content.

Alternatively, check the box to **Use All Adaptiva Clients** if the policy should run on all clients.

**NOTE: If IntelliStage is not used, and only 1 or 2 machines are targeted in an office, OneSite will still solicit volunteers to get 3 copies of the content in that office to ensure high availability.**

**If IntelliStage is selected, along with Use All Adaptiva Clients, every office will receive the specified number of copies of the content.**

## Content List Tab

The Content List tab is used to specify what content will be deployed by this Content Push Policy.

### SCCM Objects

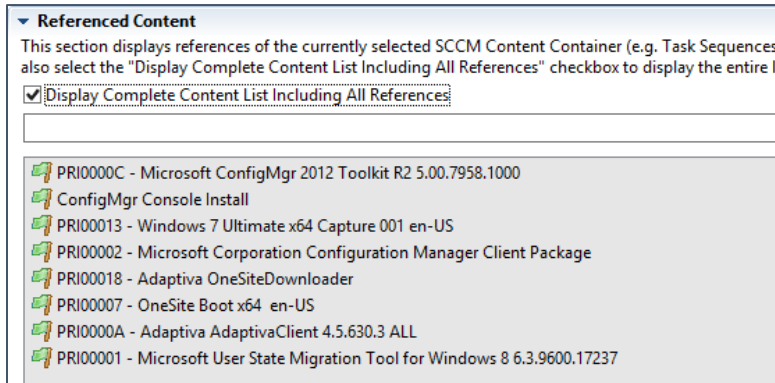
The SCCM Objects field is a required field and is where you will assign the list of contents that you wish to be pre-staged.

In the **OneSite - Content Push Perspective**, there are Explorers for each content type (SCCM Packages, Software Deployment Packages, SCCM Task Sequences, etc.), in the **Adaptiva Content Push Perspective**, there will be a single Explorer showing all content types. From one of these Explorers, drag one or more content objects to the Content List field.



## Referenced Content

If a container object is included in the SCCM Objects field, such as a Task Sequence or Intune P2P application, when that object is highlighted, the **Referenced Content** field will list the objects that are referenced by the container object. If a different container object is highlighted, a different list will appear in the **Referenced Content** field. To display all objects referenced by the policy, check the box labeled **Display Complete Content List Including All References**.

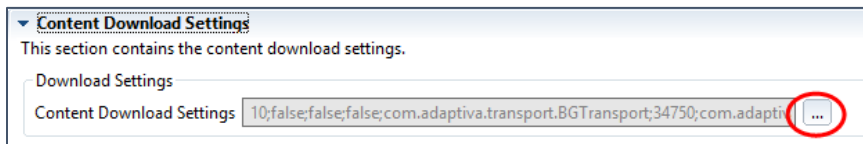


## Advanced Content Push Settings Tab

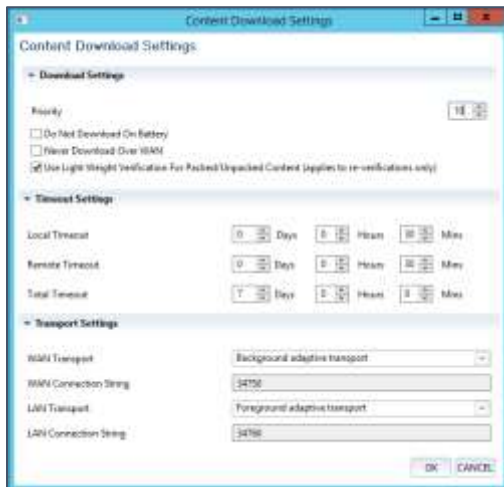
The Advanced Content Push Settings tab contains optional settings that can be used to further customize the Content Push Policy.

### Content Download Settings

The Content Download Settings field is a single read-only field showing download parameters that will be sent to clients targeted by the policy. Click the ellipsis button, ..., next to the field to bring up the **Content Download Settings** window.



In the Content Download Settings window, specific download settings can be configured such as content location timeout, download priority, and what transport setting should be used.



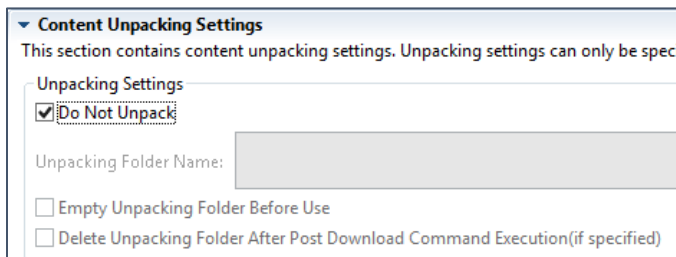
**NOTE: Administrators should use caution when modifying the WAN Transport Setting. Changing this setting can cause a significant, undesired impact to Wide Area Network bandwidth usage.**

## Content Unpacking Settings

By default, all content deployed using Adaptiva is compressed. The **Content Unpacking Settings** are used to specify if the content should be unpacked, where it should be unpacked, and if the unpacked content should be deleted following execution of the Post-Download Command.

These options are all unavailable if IntelliStage has been enabled, or if multiple objects have been added to the SCCM Objects content list. If an unpack content request is made for content in an office where only compressed content is available, then the Adaptiva Client will unpack it on demand.

To enable this setting, uncheck the **Do Not Unpack** checkbox and enter a path on the local system where the content should be placed.



The screenshot shows the 'Content Unpacking Settings' configuration window. It includes a title bar, a description, and several checkboxes. The 'Do Not Unpack' checkbox is checked. There is a text input field for 'Unpacking Folder Name' which is currently empty. Below it are two more unchecked checkboxes: 'Empty Unpacking Folder Before Use' and 'Delete Unpacking Folder After Post Download Command Execution(if specified)'.

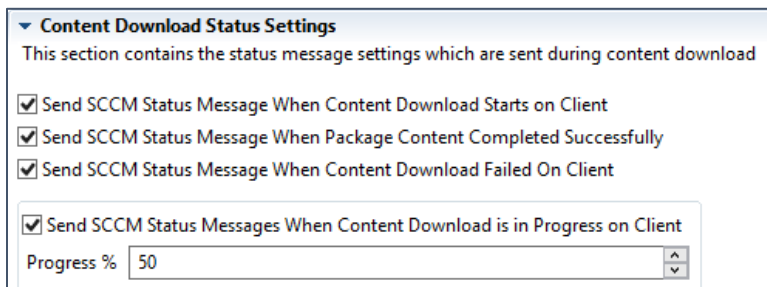
**Empty Unpacking Folder Before Use** – This setting will delete all items in the folder, specified in the **Unpacking Folder Name** setting above, before downloading the new content.

**Delete Unpacking Folder After Post Download Command Execution(if specified)** – This setting controls whether the specified folder should be deleted once the Post Download Command has been executed (or would have been executed, if added).

## Content Download Status Settings

These can be ignored when not downloading ConfigMgr content.

Content Download Status Settings are used to control when, and at what milestones, status messages are sent to ConfigMgr, if used, during a Content Push download. In cases where large amounts of clients are targeted by the policy, it might be useful to limit status messages to reduce the number of messages being sent by clients.

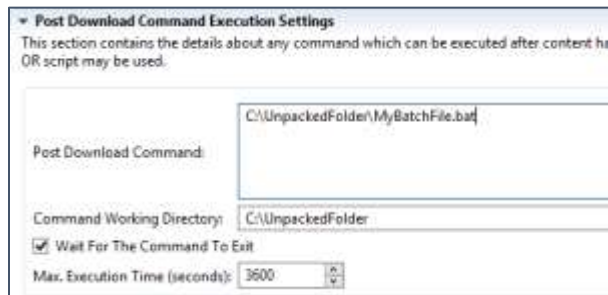


The screenshot shows the 'Content Download Status Settings' configuration window. It includes a title bar, a description, and four checkboxes, all of which are checked. Below the checkboxes is a 'Progress %' field with a value of 50 and a small up/down arrow control.

## Post Download Command Execution Settings

A Post Download Command can be specified in this section. The **Post Download Command** field must contain the full path to the file (executable or batch file) to be executed. The **Command Working Directory** field is used to specify the folder from which the command will be made.

Check the **Wait for Command Exit** box to indicate that the policy should wait for a success or failure to be returned from the Post Download Command program before continuing on with next steps. To force the process to time out after a certain number of seconds, set the value for **Max. Execution Time (seconds)**.



## Content Push Workflows

Content Push is a workflow-based feature. The workflows that are executed by a Content Push Policy can be selected in the **Content Push Workflows** section. Individual workflows can be edited via the Workflow Designer Perspective in the Workbench. The following sequence of events takes place when a Content Push Policy schedule fires. Events 2-4 take place asynchronously at the client:

- Content Push Server Workflow is executed at the server.
- Pre-Download Workflow
- Either the Download Workflow or the Office Content Push Download Workflow
- Post-Download Workflow

**Content Push Server Workflow** - This workflow executes whenever the Content Push policy schedule fires. By default, this workflow does nothing.

**Pre-Download Workflow** - The Pre-Download Workflow is executed before content download begins. By default, this workflow does nothing.

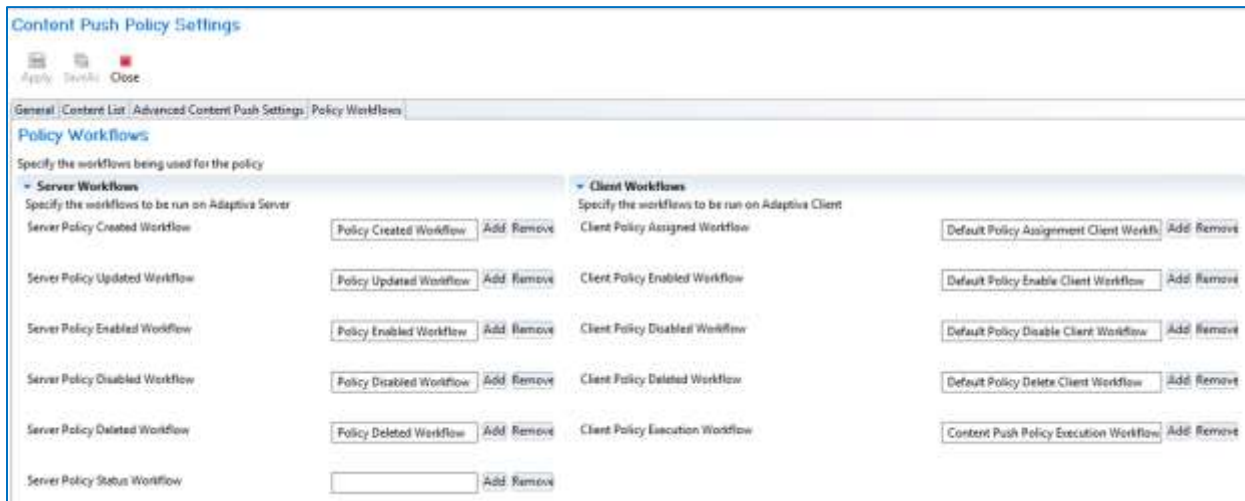
**Content Download Workflow** - The Download Workflow does the work of downloading the content and reporting status.

**Office Content Push Download Workflow** - If the IntelliStage setting is enabled in the policy, then this workflow replaces the Content Download Workflow in the policy execution.

**Post Download Workflow** - The Post-Download Workflow is executed after all content referenced by the policy has been downloaded.

## Policy Workflows Tab

The Policy Workflows tab is where Workflows can be configured to run at many different stages in the life of a Content Push Policy.



**Content Push Policy Settings**

Apply | Save | Close

General | Content List | Advanced Content Push Settings | Policy Workflows

**Policy Workflows**

Specify the workflows being used for the policy

Server Workflows	Client Workflows
Server Policy Created Workflow: Policy Created Workflow [Add] [Remove]	Client Policy Assigned Workflow: Default Policy Assignment Client Workfl [Add] [Remove]
Server Policy Updated Workflow: Policy Updated Workflow [Add] [Remove]	Client Policy Enabled Workflow: Default Policy Enable Client Workflow [Add] [Remove]
Server Policy Enabled Workflow: Policy Enabled Workflow [Add] [Remove]	Client Policy Disabled Workflow: Default Policy Disable Client Workflow [Add] [Remove]
Server Policy Disabled Workflow: Policy Disabled Workflow [Add] [Remove]	Client Policy Deleted Workflow: Default Policy Delete Client Workflow [Add] [Remove]
Server Policy Deleted Workflow: Policy Deleted Workflow [Add] [Remove]	Client Policy Execution Workflow: Content Push Policy Execution Workflow [Add] [Remove]
Server Policy Status Workflow: [ ] [Add] [Remove]	

When using Intellistage, change the Client Policy Execution Workflow to use the **Content Push Policy Execution Workflow – SuperRVP Only**. This assumes the target group includes all computers in one or more offices.

## Executing the Policy

After the required steps have been completed the policy can be run. The **Apply** button at the top of the Content Push Policy Settings editor will cause the policy object to be distributed to the target collection(s), and when the Run Policy schedule fires, the policy will be executed.

# Distribution Status

## LiveFlow Content Transmission

LiveFlow gives an administrator the ability to view and control the transmission of content that is traversing the WAN.

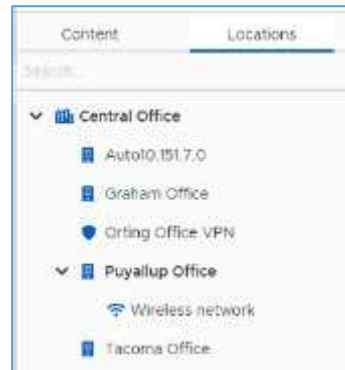
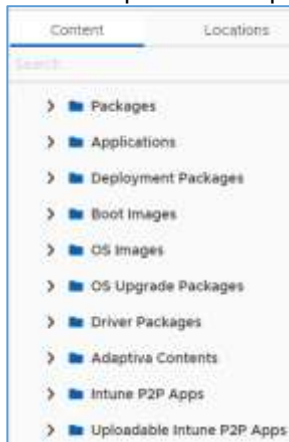
### Using the Adaptiva Web Portal

LiveFlow (Live WAN Downloads) is available in build 8.0.928.0 and later.

1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Go to OneSite ConfigMgr Edition** or **Go to One Intune Edition** or click **OneSite Anywhere, OneSite ConfigMgr Edition** or **OneSite Intune Edition**
4. Select **Live WAN Downloads**

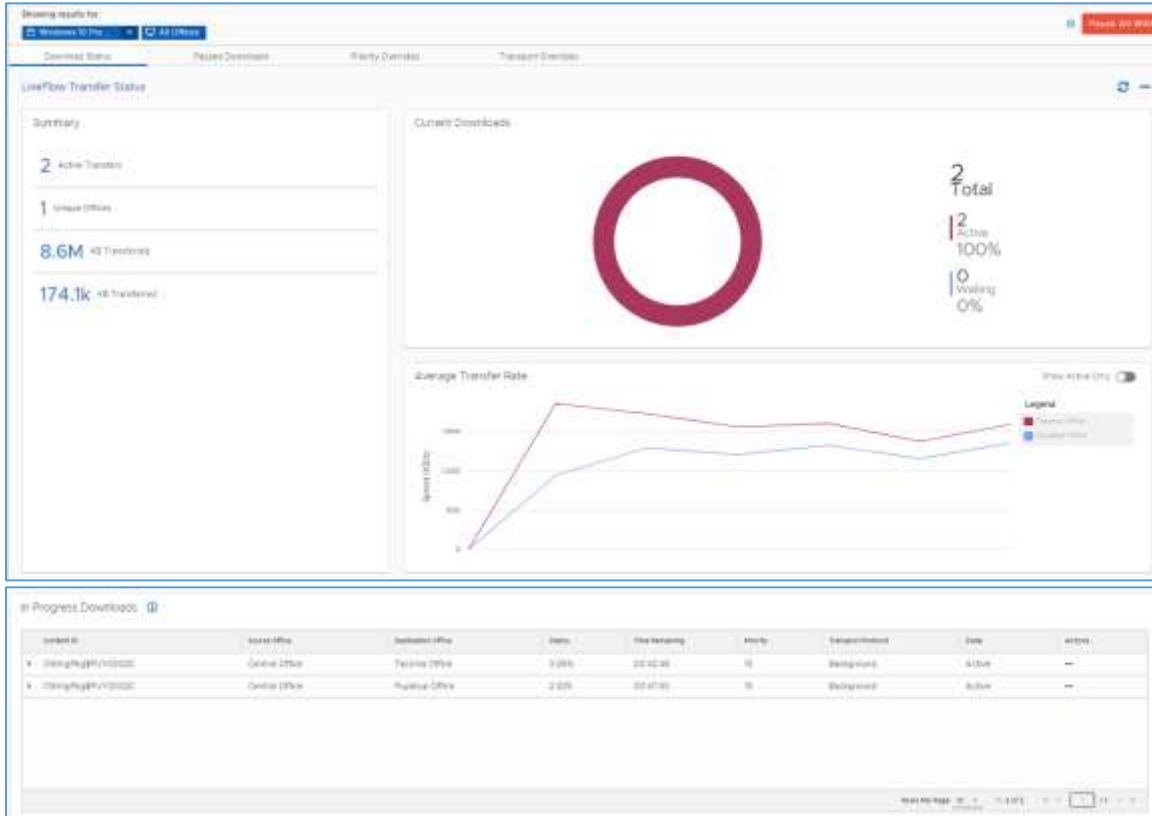


5. The center pane will display Content or Locations. This is the Content/Location pane.





- After selecting a specific piece of content or a specific location, the right-most pane will display the current transfer status



After selecting **Live WAN Downloads**, the default page in the right pane will be Download Status. There are other pages that can be used to manage the content transfers.

### View and Manage All Live WAN Transfers

- In the Content/Location pane determine if you want to view by Content or by Location or both by selecting the appropriate items. Selecting an item from the list of Content will update the **Showing results for:** in the right-pane, by default it will show the content going to All Offices



- Selecting Locations, expanding the list of Locations and selecting a specific location will then update the **Showing result for:** in the right-pane



- If content is currently being transferred, the **LiveFlow Transfer Status** will show the progress of the transfer and the content item will be displayed in the **In Progress Downloads** section at the bottom.

The LiveFlow Transfer Status has three sections:

<b>Summary</b>	This shows the number of active transfers, number of unique offices and the amount transferred to each destination
<b>Current Downloads</b>	This is a donut chart showing the amount of content Active versus Waiting
<b>Average Transfer Rate</b>	This is a line graph showing the speed at which the content is being transferred to each destination

The **In Progress Downloads** will include information about the devices downloading the content – **source** and **destination**, **percent complete**, **bytes sent**, and **transfer rates**.

- To manage the content transfer between locations, select the ellipses (...) under **Actions** while hovering over a line item.



**Pause** - Selecting this option will pause the content transfer to its target.



Click **OK** to pause the transfer to that location

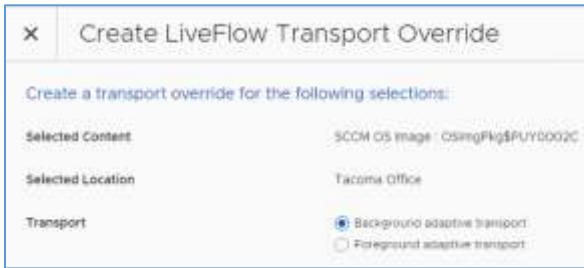
**Override Priority** - Selecting this option will display the current priority of the content item, which can be changed to raise or lower the priority.



Enter the new priority and click **OK**

**Transport override** - Offers the option to change the transport for a content item on the fly with the option of using **Background adaptive transport**, the default, or **Foreground adaptive**

**transport.** It is not recommended to switch to Foreground transport as it will function like a SMB file copy, which may impact bandwidth availability over the WAN.



Select the desired transport and click **OK**

**Cancel Transfer** - Cancels the selected WAN Transfer.



Click **OK** to Cancel the transfer

### Big Red Button – Global WAN Pause/Resume

This allows you to immediately pause or resume ALL WAN transfers taking place between Adaptiva clients across ALL Adaptiva locations.

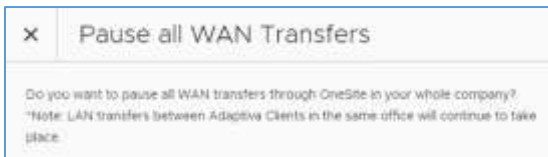
1. At the top, right of the pane, click **Pause All WAN**.



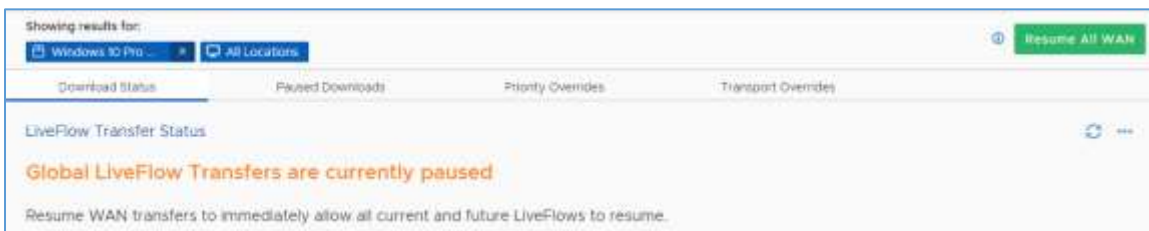
Notice the information bubble to its left



2. The following will be displayed:



Click **OK** to Pause all transfers. It will take a few seconds. When it is complete, the right pane will show:



**NOTE: LAN transfers between Adaptiva clients located in the same office will continue.**

- To resume WAN transfers, click the green **Resume ALL WAN** button.



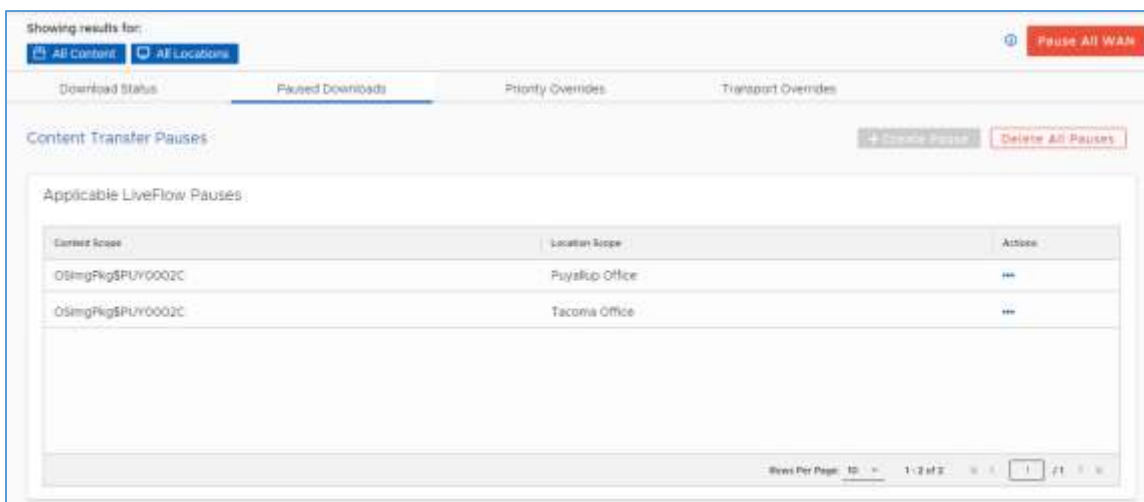
Click **OK** to Resume all transfers. It will take a minute or so to re-display the graph showing the content transfer statistics and information.

## Manage LiveFlow Pauses

This task allows you to view, create and resume any paused WAN transfers

### Showing Paused Downloads

- Select **Live WAN Downloads**
- In the right pane, select **Paused Downloads**



By default, All Content at All Locations is shown. If there are applicable LiveFlow Pauses they will be shown.

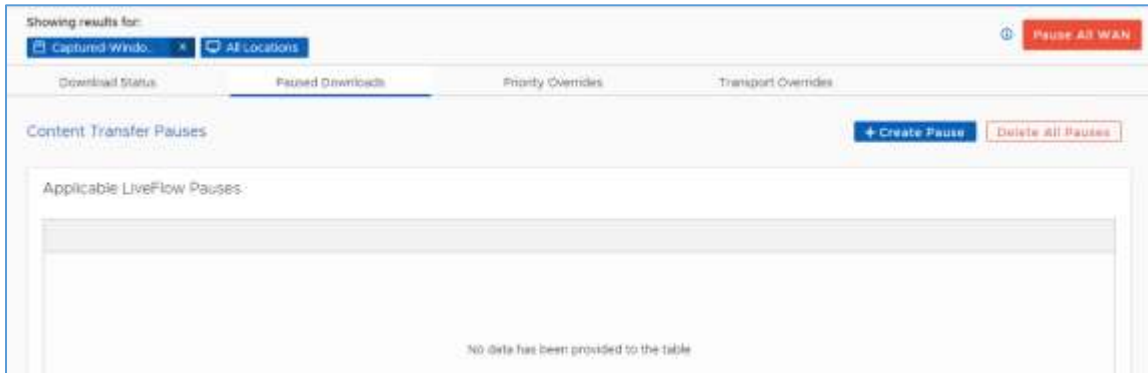
- In the **Content/Location** pane, select either specific content or a specific location to filter the pauses to those items. After selecting a Content item or specific Location, click the **x** under **Showing results for:** to remove that selection and go back to All



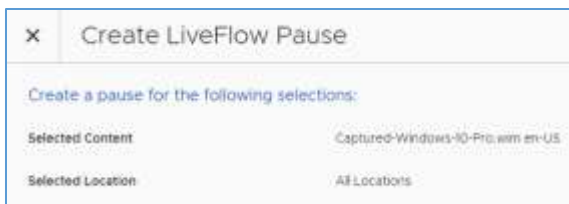
### Creating Paused Downloads

When either a specific content item or a specific location is selected, a Pause can be created for that content item to any location, or for all content to the specific location

1. In the **Content/Location** pane, select either specific content or a specific location to filter the pauses to those items.



2. Click on **+ Create Pause**



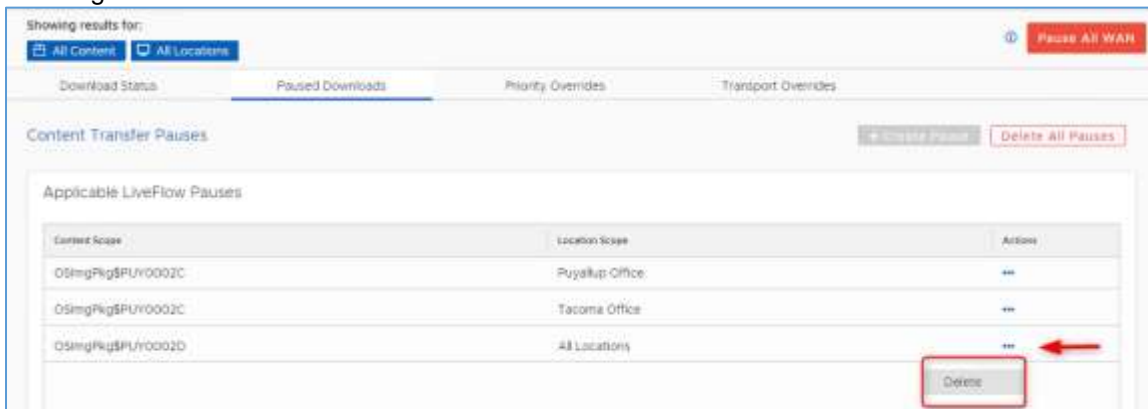
Click **OK**

If a content item was selected, then distribution of that content to all locations will be paused

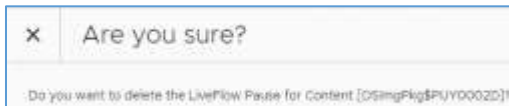
If a location was selected, then distribution of all content to that location will be paused.

### Deleting a Paused Download

1. To remove a specific LiveFlow Pause, click on the ellipses (...) under the **Actions** column while hovering over the line item.



Select **Delete**



Click **OK**

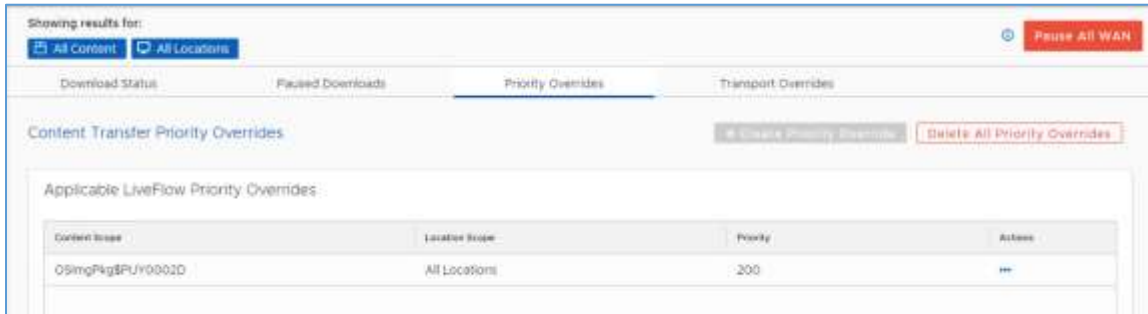
2. To resume all transfers, click the **Delete ALL Pauses** button and click OK

## Manage LiveFlow Priority Overrides

This task allows you to view, create or remove any priority overrides set against any LiveFlow content transfers.

### Showing Priority Overrides

4. Select **Live WAN Downloads**
5. In the right pane, select **Priority Overrides**



By default, All Content at All Locations is shown. If there are applicable LiveFlow Priority Overrides they will be shown.

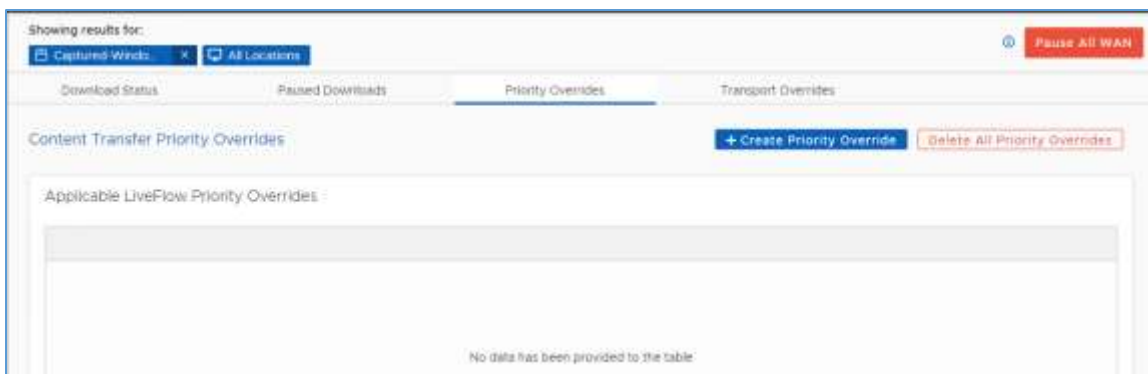
6. In the **Content/Location** pane, select either specific content or a specific location to filter the overrides to those items. After selecting a Content item or specific Location, click the **x** under **Showing results for:** to remove that selection and go back to All



### Creating Priority Overrides

When either a specific content item or a specific location is selected, a Priority Override can be created for that content item to any location, or for all content to the specific location

3. In the **Content/Location** pane, select either specific content or a specific location to filter the overrides to those items.



4. Click on **+ Create Priority Override**

Enter a new priority

Click **OK**

If a content item was selected, then distribution of that content to all locations will have its priority changed

If a location was selected, then distribution of all content to that location will have its priority changed

### Deleting a Priority Override

3. To remove a specific Priority Override, click on the ellipses (...) under the **Actions** column while hovering over the line item.

Select **Delete**

Click **OK**

4. To delete all Priority Overrides, click the **Delete ALL Priority Overrides** button and click **OK**

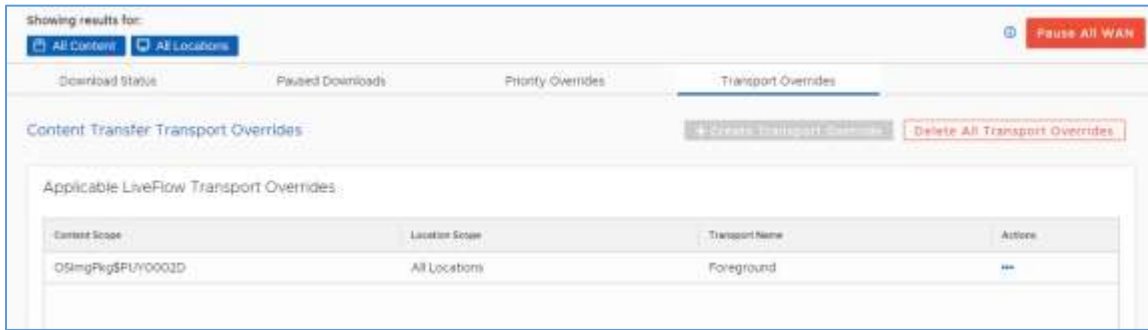
### Manage LiveFlow Transport Overrides

This task allows you to view, create or remove any transport overrides set against any LiveFlow content transfers.

#### Showing Transport Overrides

1. Select **Live WAN Downloads**

- In the right pane, select **Transport Overrides**



By default, All Content at All Locations is shown. If there are applicable LiveFlow Priority Overrides they will be shown.

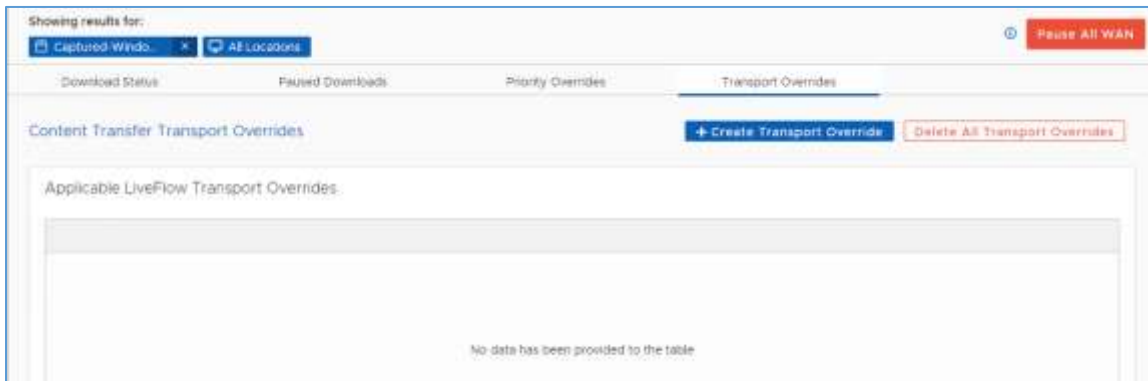
- In the **Content/Location** pane, select either specific content or a specific location to filter the overrides to those items. After selecting a Content item or specific Location, click the **x** under **Showing results for:** to remove that selection and go back to All



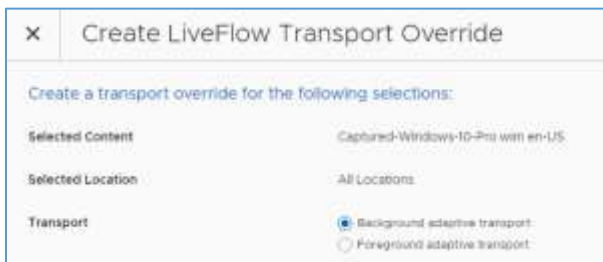
### Creating Transport Overrides

When either a specific content item or a specific location is selected, a Transport Override can be created for that content item to any location, or for all content to the specific location

- In the **Content/Location** pane, select either specific content or a specific location to filter the overrides to those items.



- Click on **+ Create Transport Override**



Select the desired Transport

Click **OK**

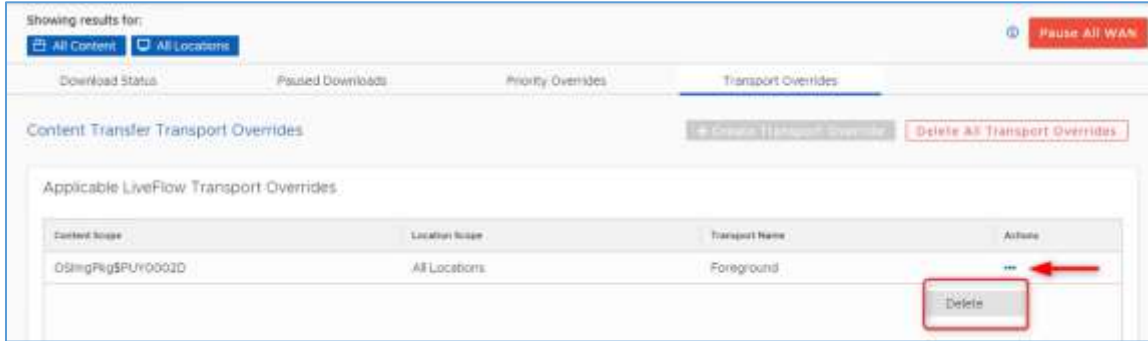


If a content item was selected, then distribution of that content to all locations will have its transport protocol changed

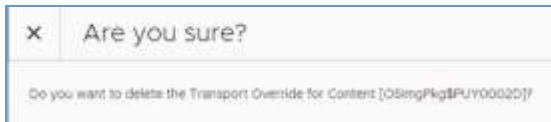
If a location was selected, then distribution of all content to that location will have its transport protocol changed

### Deleting a Transport Override

- To remove a specific Transport Override, click on the ellipses (...) under the **Actions** column while hovering over the line item.



Select **Delete**



Click **OK**

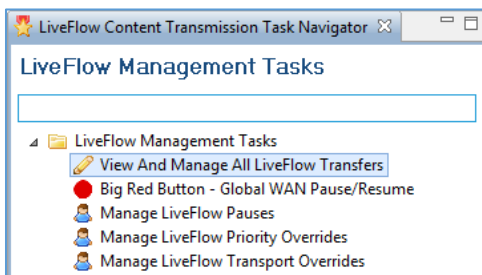
- To delete all Transport Overrides, click the **Delete ALL Transport Overrides** button and click **OK**

### Using the Adaptiva Workbench

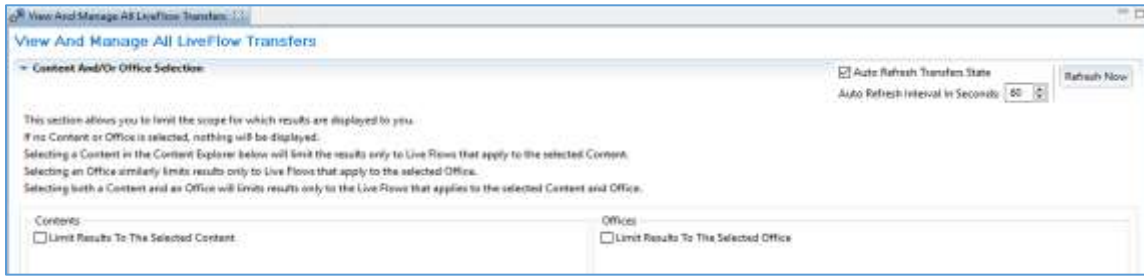
Open the Adaptiva Workbench and in **Workbench Perspectives** expand the **Content Management** folder and launch the **LiveFlow Content Transmission Perspective**. There are several Live Flow Management Tasks available.

#### View and Manage All LiveFlow Transfers

- In the **Live Flow Management Tasks** pane, select **View and Manage All LiveFlow Transfers**.



- In the **Content And/or Office Selection** section, first determine if you want to view by Content or by Office or both and check the associated box



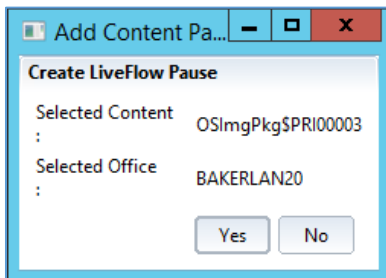
- Next, either select a content item from the left to see the status of a specific content item or select an Office from the right to see content transfers to the office itself.
- If content is currently being transferred, the content item will be displayed in the **Current Live WAN Transfers for Selected Content And/or Office** section at the bottom.
- The list of live transfers will include information about the clients downloading the content, percent complete, bytes sent, and transfer rates.



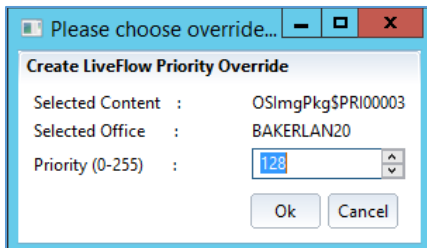
- To manage the content transfer between offices, select the line item and use one of the below options. You can also select an office and apply the below settings.

**Show Details** - Displays additional information about the transfer such as Content and version information and download status.

**Pause Transfer** - Selecting this option will immediately pause the content transfer to its target.

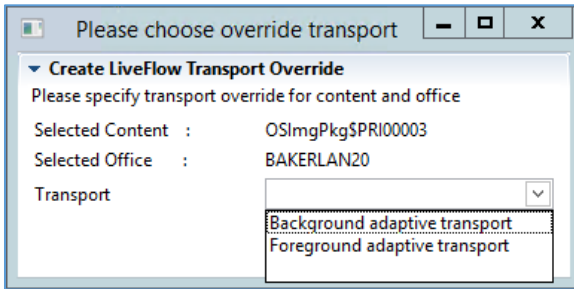


**Change Priority** - Selecting this option will display the current priority of the content item, which can be changed to raise or lower the priority.

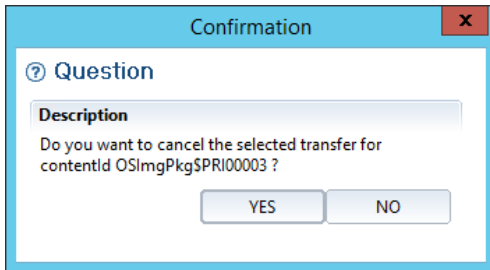


**Change Transport** - Offers the option to change the transport for a content item on the fly with the option of using the default, **Background adaptive transport** or **Foreground adaptive**

**transport.** It is not recommended to switch to Foreground transport as it will function like a SMB file copy, which may impact bandwidth availability over the WAN.



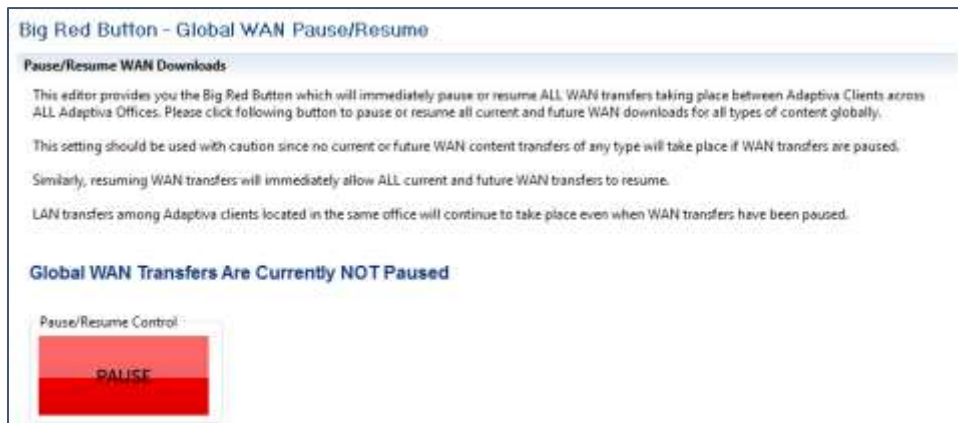
**Cancel Transfer** - Cancels the selected WAN Transfer.



### Big Red Button – Global WAN Pause/Resume

This task allows you to immediately pause or resume all WAN transfers taking place between Adaptiva clients across all Adaptiva offices.

4. In the **Live Flow Management Tasks** pane, select **Big Red Button – Global WAN Pause/Resume**.
5. To pause all transfers, click the red **PAUSE** button.



**NOTE:** LAN transfers between Adaptiva clients located in the same office will continue.

- To resume WAN transfers, click the green **RESUME** button.



## Manage LiveFlow Pauses

This task allows you to view, create and resume any paused WAN transfers.

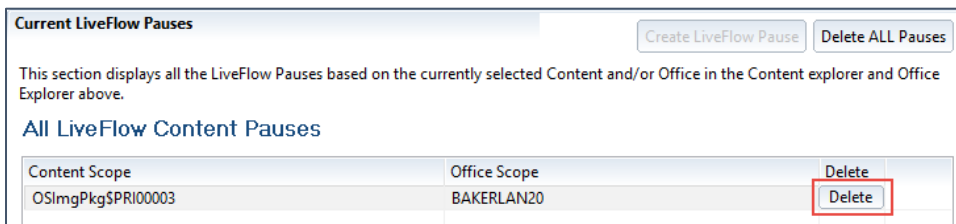
- In the **Live Flow Management Tasks** pane, select **Manage LiveFlow Pauses**.
- In the **Content and/or Office Selection** section, check the box **Limit Results to the Selected Content** and/or **Limit Results to the Selected Offices** checkbox(es) to view pause states for a content item and/or office. If both boxes are unchecked, all pauses will be displayed.

To Pause all content transfers for a particular content item, select the content item and click the **Create LiveFlow Pause** button.

To Pause all content transfers to a particular office, select the office and click the **Create LiveFlow Pause** button.

To resume all LiveFlow transfers, click the **Delete ALL Pauses** button.

To resume the transfer of a specific content item, click the **Delete** button next to the item.

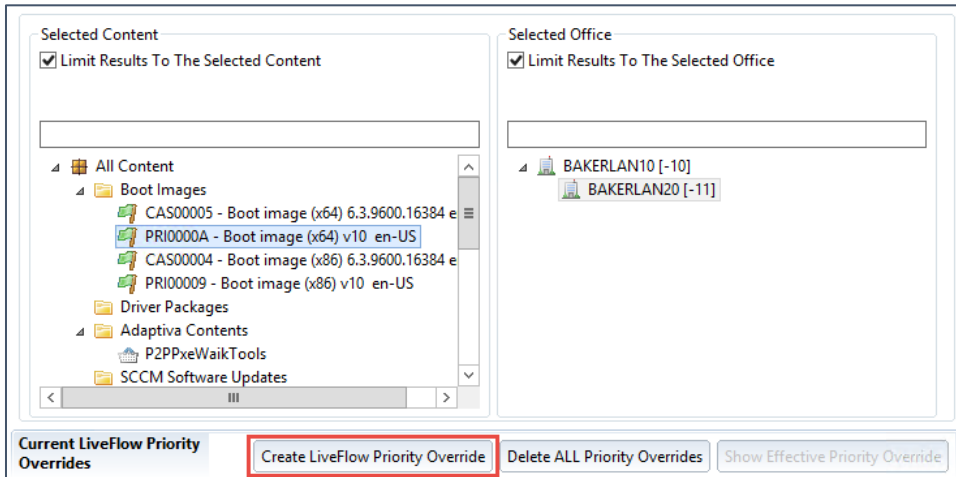


## Manage LiveFlow Priority Overrides

This task allows you to view, create or remove any priority overrides set against any LiveFlow content transfers.

- In the **Live Flow Management Tasks** pane, select **Manage LiveFlow Priority Overrides**.
- In the **Content and/or Office Selection** section, check the box **Limit Results to the Selected Content** and/or **Limit Results to the Selected Offices** to view priority overrides set against a LiveFlow content transfer. If both boxes are unchecked, all overrides will be displayed.

- To change the LiveFlow Priority Override, select the specific content item, content item and office, or simply all content for an office, then press the **Create LiveFlow Priority Override** button.



- In the **LiveFlow Priority Override** dialog, edit the priority and click **OK**.



To remove all priority overrides, click the **Delete All Priority Overrides** button. The priorities of each content item will be reverted to their original value.

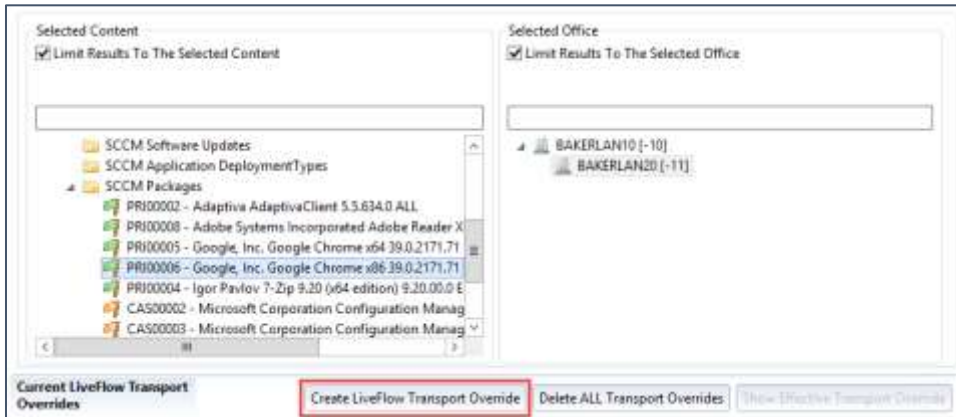
To remove a specific priority override, click the **Delete** button next to the item.

## Manage LiveFlow Transport Overrides

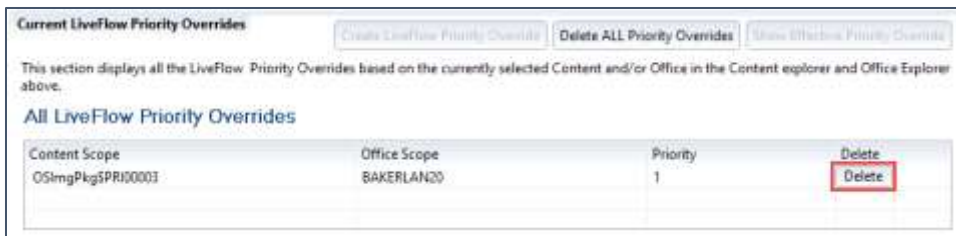
This task allows you to view, create or remove any transport overrides set against any LiveFlow content transfers.

- In the **Live Flow Management Tasks** pane, select **Manage LiveFlow Transport Overrides**.
- In the **Content and/or Office Selection** section, check the box **Limit Results to the Selected Content** and/or **Limit Results to the Selected Offices** to view transport overrides set against a LiveFlow content transfer. If both boxes are unchecked, all transport overrides will be displayed.
- To create a new LiveFlow Transport Override, select the specific content item, content item and office, or simply all content for an office, then press the **Create LiveFlow Transport Override**

button. Alternatively, click the **Delete All Transport Overrides** button to delete overrides for the content and/or office selected.



- To see all LiveFlow Transport Overrides, uncheck both **Limit Results to the Selected Content** and **Limit Results to the Selected Office**, and in the **Current LiveFlow Priority Overrides** section, a list will appear of all overrides as well as their priority. To remove the override, click the **Delete** button next to the item.



## Content Distribution Status

### Using the Adaptiva Web Portal

This is currently only available in the Adaptiva Workbench.

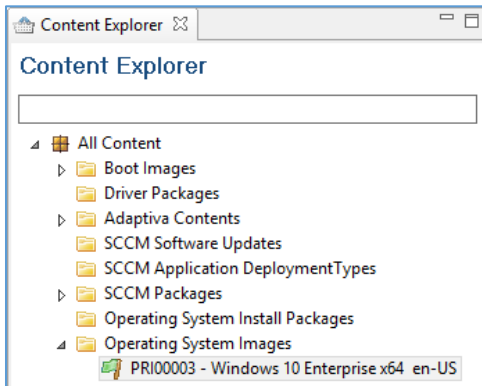
### Using the Adaptiva Workbench

The Content Distribution Status perspective lists the various content types and content items with their current distribution status. An administrator can select a content item such as an ConfigMgr package, Adaptiva package or Intune P2P package, and quickly determine the following:

- Which offices the content has started, or completed downloading to
- Specific clients which have the content
- Specific clients currently downloading the content
- Specific clients who partially downloaded the content

- Open the Adaptiva Workbench and in **Workbench Perspectives** expand the **Content System** folder and launch the **Content Distribution Status Perspective**.

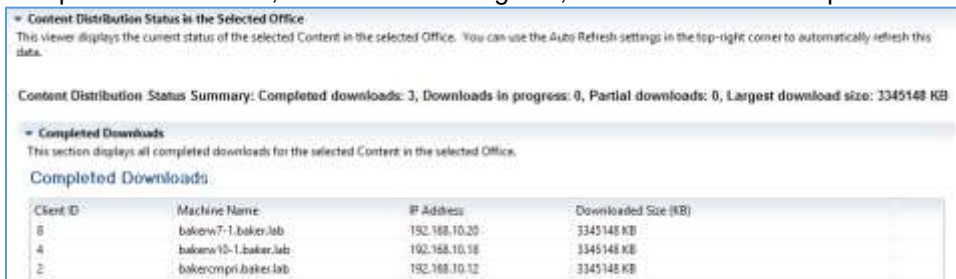
- In the **Content Explorer** pane, navigate to and select a content item that you want to view distribution status.



- In the **Content Distribution Status Viewer** pane, in the **Content Distribution Status Viewer** section, you will see a list of offices where the content is available. To view the status, select one of the offices.



In the **Content Distribution Status in the Selected Office** section, you can view a list of Completed Downloads, Downloads in Progress, or Partial Downloads per machine.



Each list displays information about the clients as well as the amount of content which has been downloaded.

# Additional Settings for ConfigMgr Environments

## Linked Servers and Object Export

This is currently only available in the Adaptiva Workbench.

### Overview

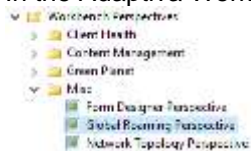
Linking Adaptiva servers allows for two different functions. First is to enable Global Roaming of clients to download content from a local source, and second is to allow objects (i.e. policies, workflows, etc.) created on one Adaptiva server to be exported directly to another Adaptiva server.

Global Roaming of content allows for Adaptiva clients assigned to one Adaptiva server, to travel to a location where all the clients are assigned to another Adaptiva server. With this set, content discovery and sharing are enabled between the clients assigned to two different Adaptiva servers.

**IMPORTANT: For Global Roaming and sharing of content to work, all the Adaptiva servers must be in the same time zone.**

### Linking Adaptiva Servers

1. In the Adaptiva Workbench, navigate to **Misc\Global Roaming Perspective**



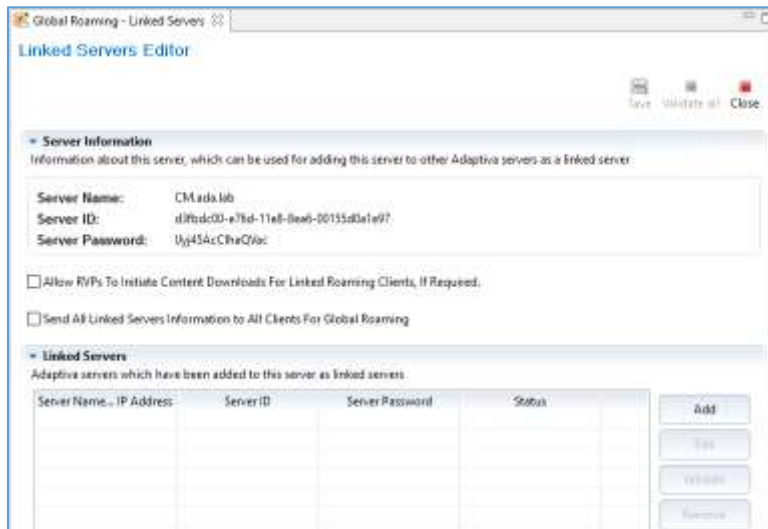
2. Select **Manage Linked Servers** from the task navigator to bring up the **Linked Servers Editor**.



Here you will note the given **Server Name**, **Server ID**, and **Server password**, you will use this information on the other server to add the link. To link servers, select the **Add** button, and enter the information found here on the other Adaptiva server. Also notice the button to **Validate** (or the



button above to **Validate All**), this will ensure the data entered is correct and that communications can be established. Once complete, select the **Save** button.



The settings above suffice to allow for exporting of policies and other objects between Adaptiva servers.

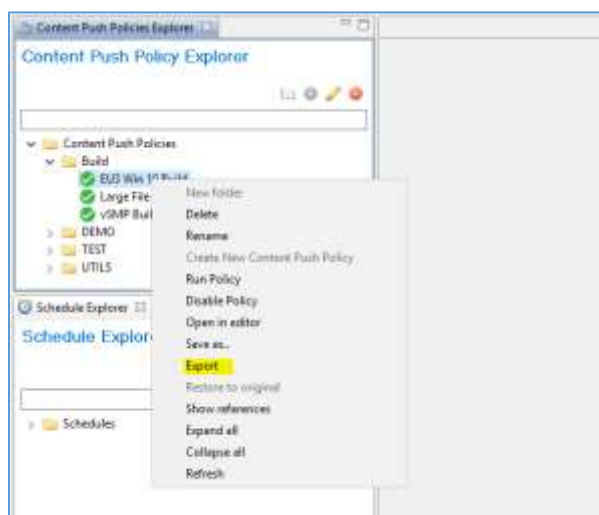
For Global Roaming of content, note there are the two configurable options:

1. **Allow RVPs To Initiate Content Downloads For Linked Roaming Clients, If Required** – this should not be selected, as this is for a future product enhancement.
2. **Send All Linked Servers Information to All Clients For Global Roaming** - To allow content sharing between clients assigned to different servers. This is required for Global Roaming.

## Exporting Objects to Linked Adaptiva Servers

Starting with version 5.6 of OneSite, support has been added to export many item types, such as policies (content push, system configuration, health check), schedules and workflows, directly from the workbench of one Adaptiva server to other Adaptiva servers.

To export any object to 1 or more linked server(s), from the perspective in the workbench that contains the object, simply right-click the object, and select **Export**. In this example, we will use a Content Push policy.



This will bring up the export settings page. At the top of the form you can optionally enter the **Exporting Organization** and/or add a **Description**.

Next, you can select to **Automatically import objects into the specified** folder, this will allow you to specify the folder on the target server where the object should be saved. If you leave this option unselected, the object will be saved into the root on the new server.

To export to another Adaptiva server it is required to select the toggle to **Allow Export To Linked Servers**, and select via the Export toggles, the server(s) target to replicate.

In the **Import Preferences** you can optionally select to use existing objects or overwrite existing objects.

Once ready, at the top of the form, select the **Export To Linked Servers** button to complete the replication.

The screenshot shows the 'Object Export Editor' window. At the top right, there are buttons for 'Export To Linked Servers', 'Export To File', and 'Cancel'. The main area is divided into several sections:

- Object Export Settings:** Includes text boxes for 'Exporting Organization' and 'Description'.
- Import Folder Settings:** A checkbox for 'Automatically import objects into the specified folder' is checked. Below it is a 'Folder Name' field containing 'Build'.
- Object Export Tree:** A tree view showing a hierarchy of objects. The root is 'Objects', which contains 'ContentPushServerPolicy - EU3 Win 10 Build'. Under this, there are several workflow objects: 'Workflow - Default Policy Assignment Client Workflow', 'Workflow - Pre Download Workflow', 'Workflow - Policy Created Workflow', and 'Workflow - Policy Download Workflow'.
- Export To Linked Servers Settings:** A checkbox for 'Allow Export To Linked Servers' is checked. Below it are three dropdown menus for 'Import Preferences': 'Resolution for Top Level Object' (set to 'OVERWRITE EXISTING OBJECT'), 'Resolution for Built-in Referenced Objects' (set to 'USE EXISTING OBJECT'), and 'Resolution for Non Built-in Referenced Objects' (set to 'OVERWRITE EXISTING OBJECT').
- Table:** A table with columns: 'Export', 'Server Name Or IP Address', 'Server ID', 'VerificationStatus', 'ExportStatus', and 'Details'. Two rows are visible, both with 'Not Started' in the 'ExportStatus' column.
 

Export	Server Name Or IP Address	Server ID	VerificationStatus	ExportStatus	Details
<input checked="" type="checkbox"/>	EURLABSCCM01.EUR.LAB	2d6d3ffe-1f05-11e5-9ce8-00155d956e07	Valid	Not Started	Details
<input checked="" type="checkbox"/>	EURLABSCCM04.EUR.LAB	ec01245c-b5f6-11e8-be55-00155d956e33	Valid	Not Started	Details
- Export Status:** A message at the bottom states: 'Objects are ready for export. Please click on the Export button to export the objects. You may also add some more objects for export.'

In the ExportStatus column, the status will automatically update to *In Progress*, and finally *Success* when finished.

Export	Server Name Or IP Address	Server ID	VerificationStatus	ExportStatus	Details
<input checked="" type="checkbox"/>	EURLABSCCM01.EUR.LAB	2d6d3ffe-1f05-11e5-9ce8-00155d956e07	Valid	Success	Details
<input checked="" type="checkbox"/>	EURLABSCCM04.EUR.LAB	ec01245c-b5f6-11e8-be55-00155d956e33	Valid	Success	Details

Nothing need be done on the server(s) doing the import, as the object will be automatically created there and ready for use.

**NOTE: The export import process is a one-time operation. If changes are made on the exporting server, these will not be replicated to the destination server(s). To replicate changes, another export to the servers would be required.**

## Microsoft App-V Perspective

### Overview

ConfigMgr 2012 SP1 introduced powerful App-V streaming capabilities. These capabilities allow large enterprises to provision a vast number of virtualized applications to their entire estate, with actual deployments taking place on demand only in those areas where each application is actually in use.

Adaptiva OneSite version 3.0 and above provides advanced, native App-V streaming capabilities, which seamlessly integrate with the native App-V streaming capabilities in ConfigMgr.

OneSite eliminates the need to maintain a ConfigMgr Distribution Point infrastructure or an App-V Streaming Server infrastructure. Instead, OneSite provides an elegant and self-maintaining Peer to Peer infrastructure based on the Adaptiva OneSite Caching File System and Virtual SAN technologies.

This section provides guidance for deploying the App-V Streaming capabilities of Adaptiva OneSite.

As you will see below, little, if any, configuration is required in order to enable App-V Streaming in OneSite.

### Prerequisites

The following software should have been correctly deployed and configured.

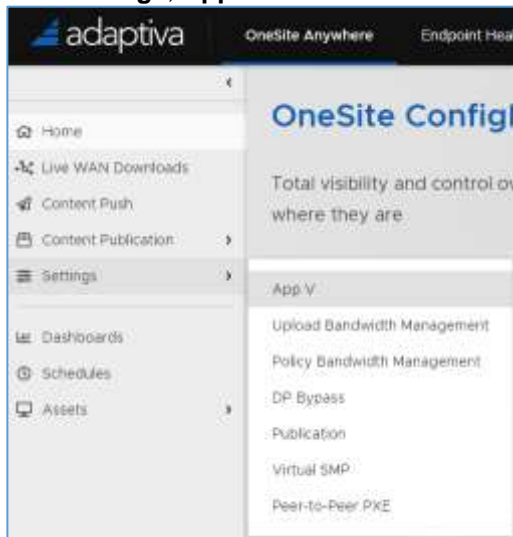
- ConfigMgr 2012 SP1 or later
- App-V Client Version 5 or later
- Adaptiva OneSite

### Enabling App-V Streaming in OneSite

#### Using the Adaptiva Web Portal

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

- Click **Settings, App V**



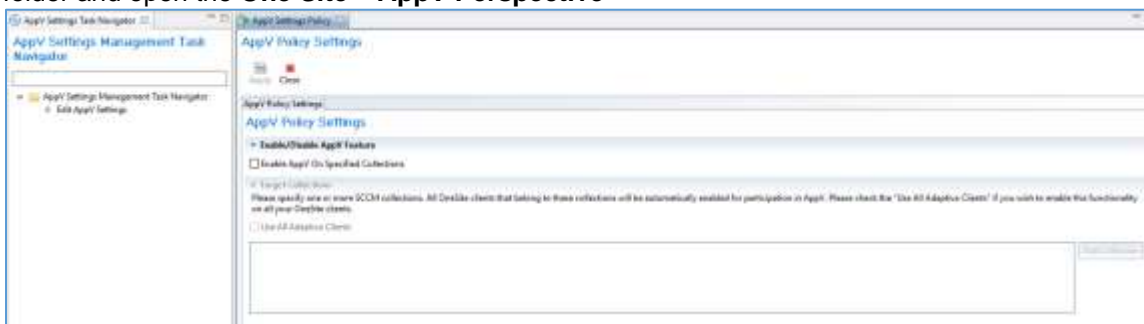
- To **Enable AppV** support, click the button to toggle to the right



- Either click the button to toggle the Use All Devices button to the right to enable App-V on all Adaptiva clients  
OR click on Browse and select and Adaptiva Group or ConfigMgr Collection to target this setting to. Click on **Add To List**
- Click on **Save**

## Using the Adaptiva Workbench

- Open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **One Site** folder and open the **One Site – AppV Perspective**



- To enable App-V support, check the box **Enable AppV On Specified Collections**
- In the **Target Collections** section, check the box to **Use All Adaptiva Clients** or specify a collection or group

## Enabling App-V Streaming on the ConfigMgr Distribution Point

ConfigMgr Distribution Points are already pre-configured with the necessary protocol support for App-V Streaming. Please ensure that at least one Distribution Point which contains the desired App-V Application and Deployment Type content is accessible to all ConfigMgr client machines.

Adaptiva OneSite App-V streaming will never actually make use of any Distribution Point for content, but ConfigMgr itself requires the content to be available on at least one Distribution Point.

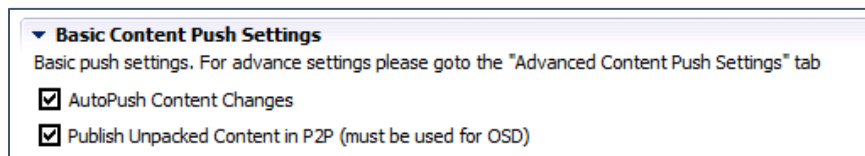
## Enabling App-V Streaming on Deployment Types

In ConfigMgr, to enable App-V Streaming on App-V Deployment Types, please select the **Stream content from distribution point** Deployment option in the **Content** tab of the **Application Virtualization 5 Properties** dialog box, as shown below.



## Pre-staging App-V Packages for Faster Streaming

Please consider using the Adaptiva Content Push features in OneSite for pre-staging App-V packages to remote locations. For additional speed, remember to check the **Publish Unpacked Content in P2P** checkbox.



1. If unpacked content has been pre-staged to a location, it will be discovered and used automatically, and App-V streaming will commence immediately.
2. If only packed content has been pre-staged to a location, it will be discovered and automatically unpacked and published on demand. App-V Streaming will commence as soon as the content has been unpacked. Once the unpacked content has been published, it will be automatically discovered in future deployments, and subsequently, App-V Streaming will commence immediately at that location.
3. If the content has not been pre-staged to a location, it will automatically be downloaded across the WAN on demand, using the Adaptive Protocol technology, cached, and unpacked, before App-V Streaming commences. Once the unpacked content has been published, it will be automatically discovered in future, and subsequently, App-V streaming will commence immediately at that location.

## Client Data Upload Bandwidth Management

Most ConfigMgr administrators are dependent on the results of ConfigMgr client inventory cycles such as hardware and software inventory for accurate reporting, as well as to define collection membership. The

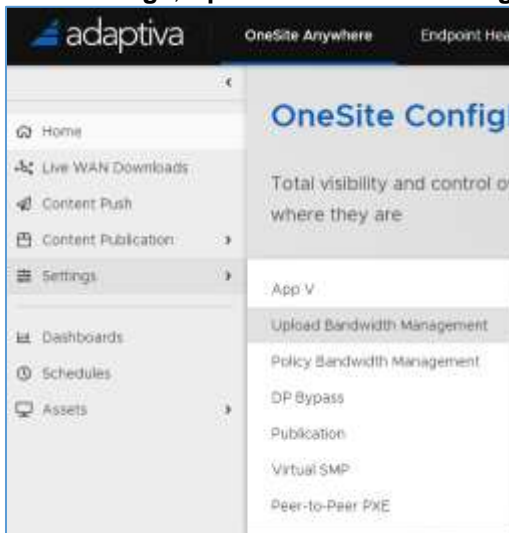
inventory cycles are typically a scheduled operation or set to an interval where each client randomly runs inventory and uploads the results to their assigned Management Points. In the case where inventory is set to run on a specified schedule, clients will upload inventory data to their MP at the same time, thus possibly causing network disruption.

With OneSite, administrators can enable **Client Data Upload Bandwidth Management** for each major inventory action including file collection and status messages. This feature gives administrators the ability to define how many clients can concurrently upload inventory data to the MP at a given time and it is configurable per each inventory action. By default, this is an Adaptiva site-wide setting, but there is also an option to override the default setting for specific clients based on collection and/or Adaptiva group membership. If an administrator knows that clients at a given location have a much faster connection to their MP, the number of concurrent uploads can be increased accordingly.

## Enabling Client Data Upload Bandwidth Management

### Using the Adaptiva Web Portal

1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – [http\[s\]://AdaptivaServerFQDN\[:port\]](http[s]://AdaptivaServerFQDN[:port])
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Go to OneSite ConfigMgr Edition** or click **OneSite Anywhere, OneSite ConfigMgr Edition**
4. Click **Settings, Upload Bandwidth Management**



5. In the **Default Settings** section, **Enable Upload Bandwidth Management** by toggling the slider to the right.



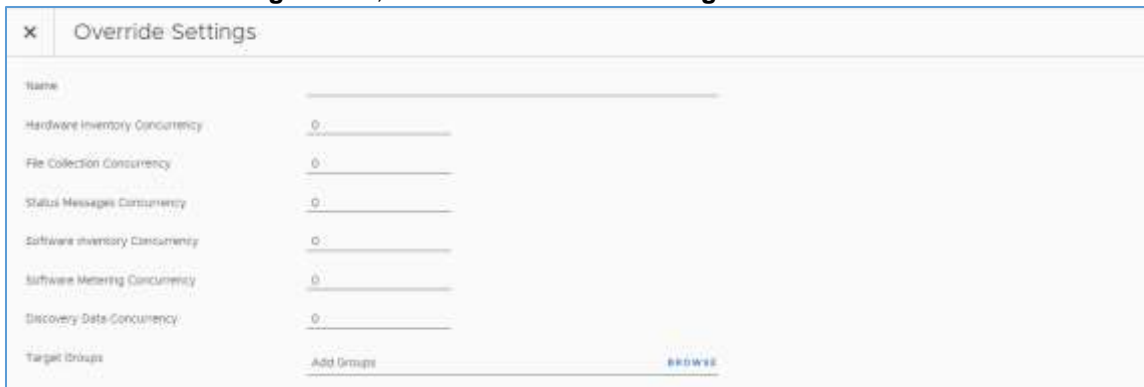
- By default, all of the values are set to 0 which means there is no limit on the number of concurrent machines that can perform the specific activity. To change that enter a number for each activity. For example,



▼ Default Settings ⓘ

Enable Upload Bandwidth Management	<input checked="" type="checkbox"/>
Hardware Inventory Concurrency	10
File Collection Concurrency	5
Status Messages Concurrency	20
Software Inventory Concurrency	10
Software Metering Concurrency	5
Discovery Data Concurrency	1

- In the case where different settings should apply to a different group of clients, create a collection or Adaptiva Group for the clients which should receive the policy override.
- In the **Override Setting** section, click **Add Override Setting** to create a new override.



✕ Override Settings

Name	
Hardware Inventory Concurrency	0
File Collection Concurrency	0
Status Messages Concurrency	0
Software Inventory Concurrency	0
Software Metering Concurrency	0
Discovery Data Concurrency	0
Target Groups	Add Groups <span style="float: right;">BROWSE</span>

- Enter the **Name** of the policy override. Modify the settings for the actions available. Click the **Browse** to choose the collection/group to target for the override. Click **OK** to apply the changes.
- Click **Save**



## Using the Adaptiva Workbench

- Open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **One Site** folder and open the **One Site – Client Data Upload Bandwidth Management Perspective**.



- In the **Client Data Upload Bandwidth Management Settings** editor, in the **Enable client data upload bandwidth management** section, check the box next to **Enable client data upload bandwidth management**.

Client Data Upload Bandwidth Management Settings



Save
Close

**▼ Enable client data upload bandwidth management**

Check the box below to enable bandwidth management for all data uploaded by SCCM clients, including Hardware inventory, Software inventory, File collection, Software metering, Status messages, and Data discovery records.

**Enable client data upload bandwidth management**

- By default, the number of machines which can upload inventory at a given time is set to 0 which means infinite. Modify the value for each inventory action specifying how many clients can upload inventory at the same time.

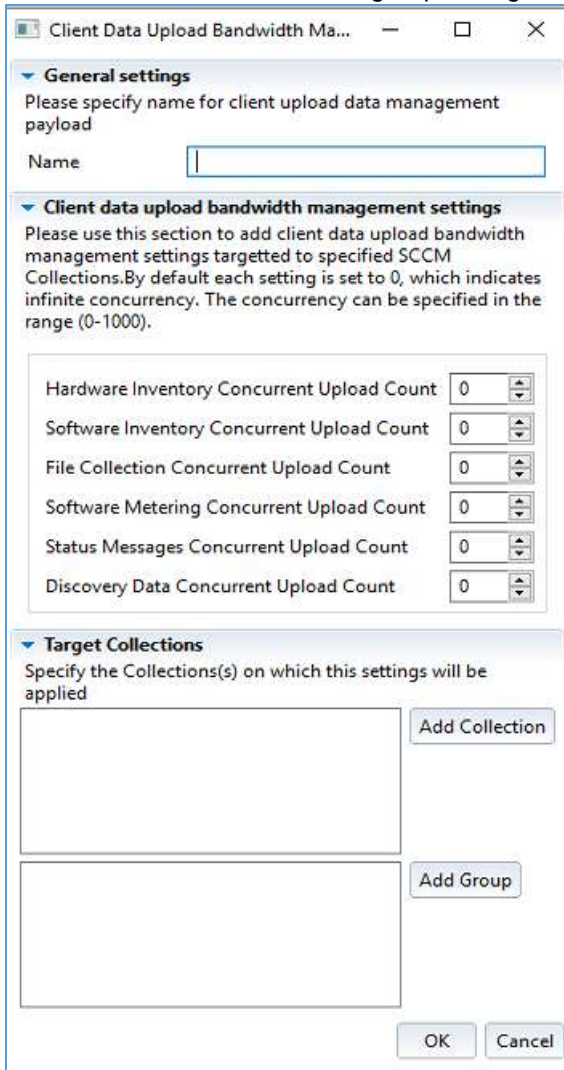
If you enable client data upload bandwidth management, you must specify the default settings that will apply to all clients. You may then override these default settings using the "Setting Overrides" section below. By default each setting is set to 0, which indicates infinite concurrency. The concurrency can be specified in the range (0-1000).

Hardware Inventory Concurrent Upload Count	10	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/> <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/>	Software Inventory Concurrent Upload Count	10	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/> <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/>
File Collection Concurrent Upload Count	5	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/> <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/>	Software Metering Concurrent Upload Count	5	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/> <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/>
Status Messages Concurrent Upload Count	20	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/> <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/>	Discovery Data Concurrent Upload Count	5	<input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/> <input style="width: 15px; height: 15px; border: 1px solid #ccc;" type="text"/>

- In the case where different settings should apply to a different group of clients, create a collection for the clients which should receive the policy override.
- In the **Setting Overrides** section, click the **Add** button to create a new override.



- In the dialog that appears, under the **General Settings** section, enter the **Name** of the policy override. Modify the settings for the actions available. Click the **Add Collection** or **Add Group** button to choose the collection/group to target for the override. Click **OK** to apply the changes.



- The setting override should appear in the list. If multiple overrides exist, the settings higher in the list have the most priority.
- Click **Save** at the top of the editor to apply the changes.

## Content AutoStage

### Overview

This is currently only available in the Adaptiva Workbench.

Content AutoStage provides the ability to automatically add content to an existing Content Push policy by using the content item priority in ConfigMgr.

Prior to creating a new AutoStage policy, a Content Push policy must be available.

### Creating a New AutoStage Policy

- Open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **One Site** folder and open the **One Site – Content AutoStage Perspective**.

2. Right-click on **Content-AutoStage Policies** and click **Create New Content AutoStage Policy**. In the center pane you will see the **Content AutoStage Policy Editor**
3. In the **Basic Information** section, enter a **Name** and **Description** (optional) for the policy.
4. In the **Content Push Policy** section, use the **Add** button to open the **Content Push Policy Explorer** dialog and select a content push policy. Alternatively, drag a Content Push Policy from the **Content Push Policy Explorer** in the right-hand pane into the **Content Push Policy** box.
5. In the various content type sections (Packages, Boot Images, etc.), select the priority which you want to automatically be added to the content push policy.



6. When complete, click **Save** to apply the policy. Any content type with the priority you specified will automatically be added to the policy.

**NOTE:** All content types in ConfigMgr, by default, are set to priority level Medium. Be aware of this prior to assigning Medium content types to an AutoStage policy.

## DP Bypass and DP Fallback

### Overview

The DP Bypass and DP Fallback features allows a OneSite administrator to control which systems, and in which scenarios, a client communicates with a ConfigMgr Distribution Point.

**DP Bypass** - prevents ConfigMgr clients from using ConfigMgr Distribution Points regardless of whether Adaptiva OneSite is installed on the client. This setting is useful in the case where the Adaptiva Client isn't installed, the service is disabled, or the ConfigMgr client is failing to invoke the Alternate Content Provider and an administrator wants to prevent clients from downloading content over the WAN.

**DP Fallback** – controls the behavior of the Adaptiva Client in various scenarios for when it should fallback to a ConfigMgr Distribution Point or fail a content download. The Adaptiva Client must be installed for these settings to be enforced.

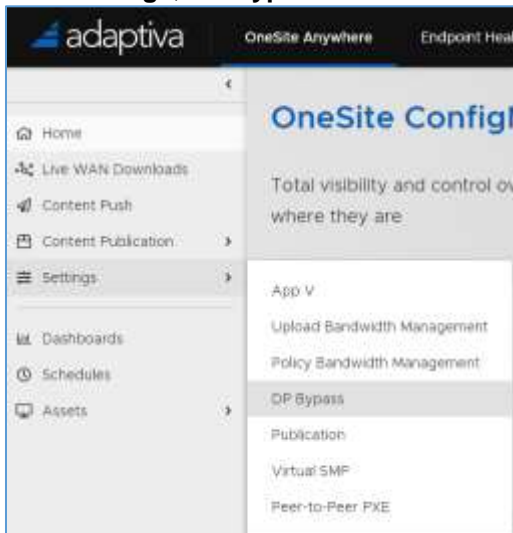
### DP Bypass Settings

- Prior to enabling DP Bypass, the Adaptiva Client must be installed on all the Management Points for the ConfigMgr site.
- Once the Adaptiva Client is installed on the Management Points, they should be added to a ConfigMgr collection to be used for targeting this policy.

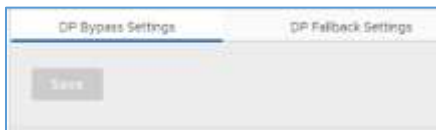
**NOTE:** To add the Management Point servers to a collection requires the servers to be discovered. The ConfigMgr client does not have to be installed.

### Using the Adaptiva Web Portal

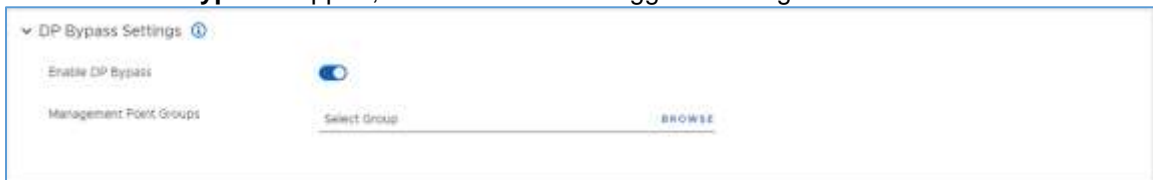
1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Go to OneSite ConfigMgr Edition** or click **OneSite Anywhere, OneSite ConfigMgr Edition**
4. Click **Settings, DP Bypass**



5. Notice at the top of the page DP Bypass Settings and DP Fallback Settings. DP Bypass Settings should be selected.



6. To **Enable DP Bypass** support, Click the button to toggle to the right

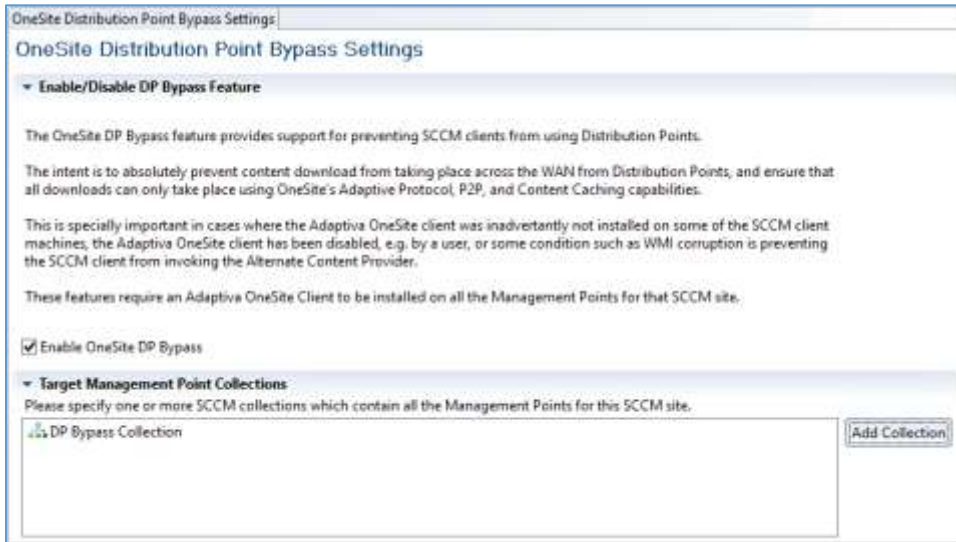


7. In the **Management Points Groups**, click the **Browse** and select the collection/group which contains your Management Points and then click on **Add to List**
8. Click on **Save**

### Using the Adaptiva Workbench

1. Open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **One Site** folder and open the **One Site – DP Bypass Perspective**.
2. In the **DP Bypass Settings Management Task Navigator** select **Edit DP Bypass Settings**.
3. To enable DP Bypass, check the box: **Enable OneSite DP Bypass**.

- In the **Target Management Points Collections** section, click the **Add Collection** button and select the collection which contains your Management Points.

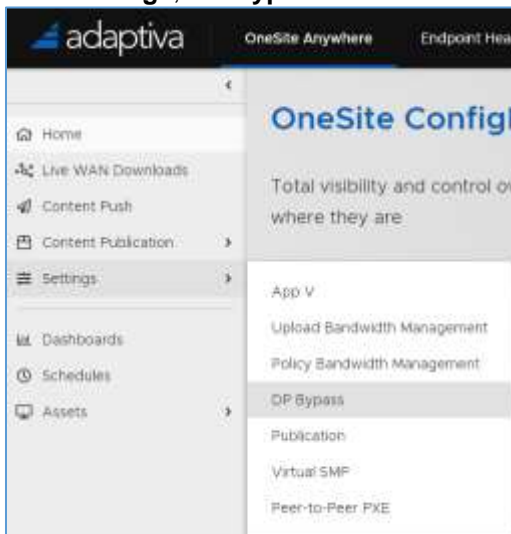


- Once complete, click the **Apply** button.

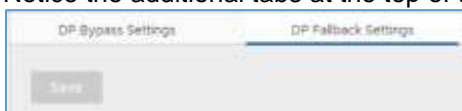
## DP Fallback Settings

### Using the Adaptiva Web Portal

- Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
- Enter the appropriate credentials or click on **Login with Active Directory**
- Click on **Go to OneSite ConfigMgr Edition** or click **OneSite Anywhere, OneSite ConfigMgr Edition**
- Click **Settings, DP Bypass**



- Notice the additional tabs at the top of the page **DP Bypass Settings** and **DP Fallback Settings**.



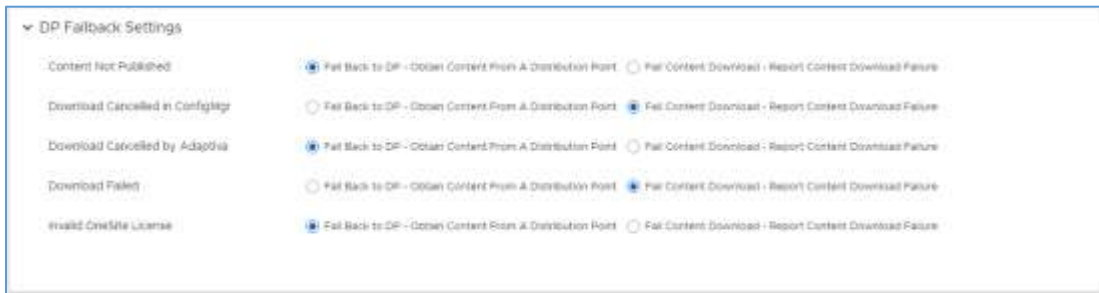
In the DP Bypass Settings tab



- **Enable DP Bypass** – Enable DP Bypass to ensure only Adaptiva is responsible for content downloads. The Adaptiva client must be installed on all ConfigMgr clients.
- **Management Point Groups** – Click on Browse and select a collection that contains the server(s) hosting the ConfigMgr Management Point role. It is recommended to include ALL Management Point servers. The ConfigMgr client and Adaptiva client do not have to be installed on the Management Point or Distribution Point Server.

**NOTE: If a content-enabled Cloud Management Gateway (CMG)/Cloud Distribution Point or Internet Based Client Management (IBCM)-enabled Distribution Point is configured, do not enable DP Bypass**

In the DP Fallback Setting tab:



Select the radio button

- **Fall Back To DP** – Obtain Content From A Distribution Point
- **Fail Content Download** – Report Content Download Failure

for the following scenarios:

- **Content Not Published** – Default: Fall Back To Distribution Point
- **Download Cancelled in ConfigMgr** – Default: Fail Content Download
- **Download Cancelled By Adaptiva** – Default: Fail Content Download
- **Download Failed** – Default: Fail Content Download
- **Invalid OneSite License** – Default: Fall Back to Distribution Point

6. Click **Save**

## Using the Adaptiva Workbench

1. Open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **One Site** folder and open the **One Site – DP Bypass Perspective**.

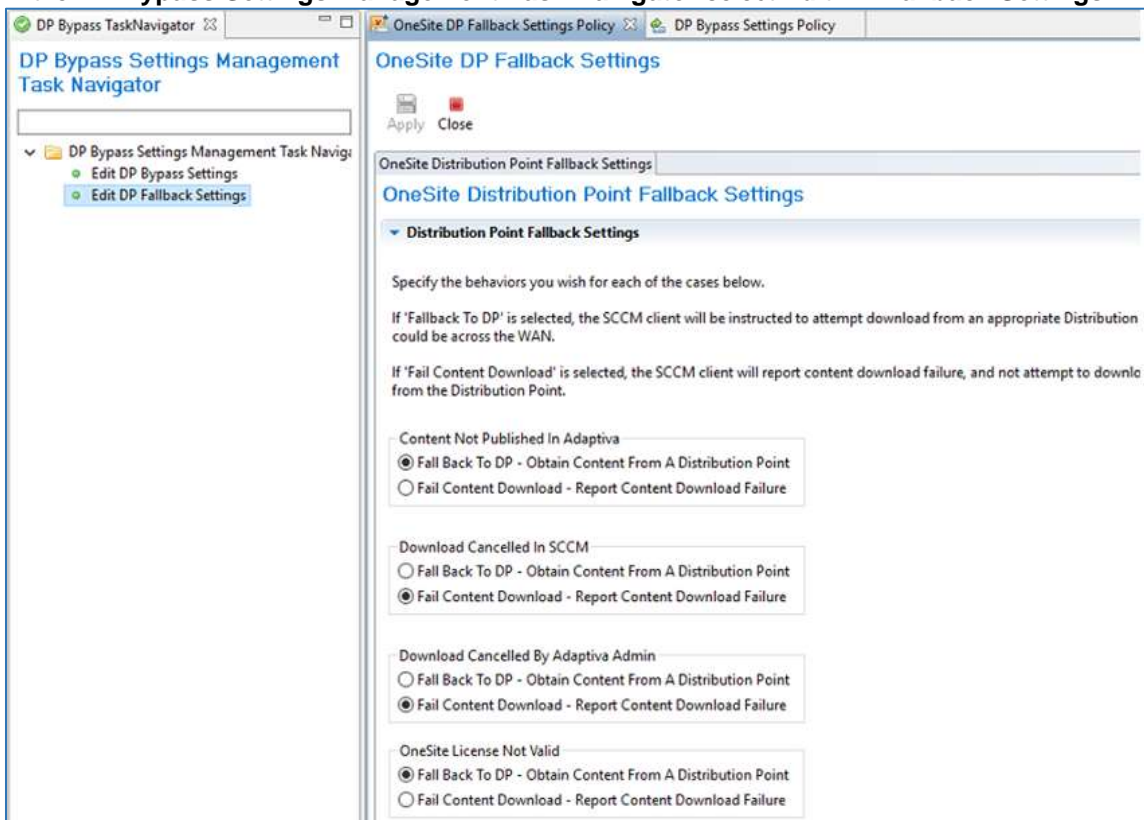
- In the **DP Bypass Settings Management Task Navigator** select **Edit DP Bypass Settings**.



- **Enable OneSite DP Bypass** – Enable DP Bypass to ensure only Adaptiva is responsible for content downloads. The Adaptiva client must be installed on all ConfigMgr clients.
- **Target Management Point Collections** – Click on Browse and select a collection that contains the server(s) hosting the ConfigMgr Management Point role. It is recommended to include ALL Management Point servers. The ConfigMgr client and Adaptiva client do not have to be installed on the Management Point or Distribution Point Server.

**NOTE: If a content-enabled Cloud Management Gateway (CMG)/Cloud Distribution Point or Internet Based Client Management (IBCM)-enabled Distribution Point is configured, do not enable DP Bypass**

- In the **DP Bypass Settings Management Task Navigator** select **Edit DP Fallback Settings**



- Use the radio buttons to instruct Adaptiva do either of the following:
  - **Fall Back To DP** – Obtain Content From A Distribution Point
  - **Fail Content Download** – Report Content Download Failure

for the following scenarios:

- **Content Not Published in Adaptiva** – Default: Fall Back To DP
  - **Download Cancelled in SCCM** – Default: Fail Content Download
  - **Download Cancelled By Adaptiva Admin** – Default: Fail Content Download
  - **Download Failed** – Default: Fail Content Download
  - **OneSite License Not Valid** – Default: Fall Back to DP
5. To save any changes made, click **Apply**.

## Peer-to-Peer PXE

### Overview

PXE (pronounced as pixie) is a set of protocols designed to boot computers using a network card, without requiring any pre-existing operating system. It was introduced by Intel in 1999 and builds upon widely used protocols such as IP, UDP, DHCP, and TFTP.

In fact, PXE does not use its own protocol, but rather is an extension of DHCP. It adds headers to the DHCP broadcast packages to declare its request for a PXE response. Originally, it was intended to have a PXE responder on the same subnet as the PXE client to respond to the broadcast messages.

Microsoft ConfigMgr provides support for PXE protocol to enable bare metal image deployment scenarios. This would normally require the installation of a “PXE Service Point” site system role on a server (SCCM 2007) or a PXE enabled Distribution Point (SCCM 2012/Current Branch), along with prerequisites such as Windows Deployment Services (WDS), and the associated changes to network infrastructure. Most environments utilize IP Helpers on their network equipment to forward DHCP broadcasts to the DHCP server. Likewise, one of the following is required to forward the PXE broadcast traffic across network segments:

- IP helper on network routers and level 3 switches to forward packets to PXE.
- Option configuration on DHCP server to point clients to a specific PXE responder.

These requirements for deploying servers, WDS, and network infrastructure changes present serious challenges in large, distributed networks, where bare metal provisioning capabilities need to be provided to hundreds or thousands of far flung locations.

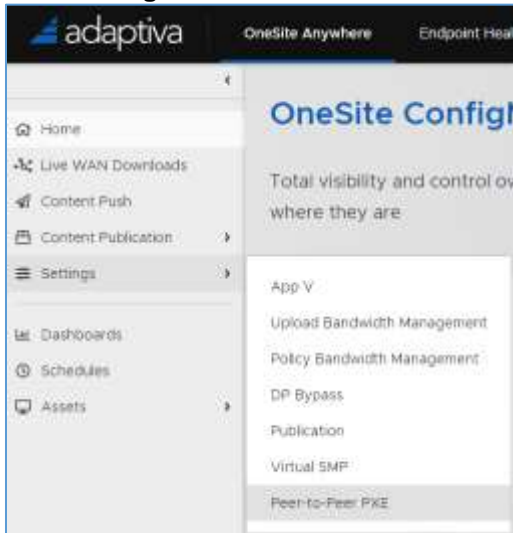
More information is available in the Adaptiva OneSite OSD User Guide

### Enabling Peer-to-Peer PXE

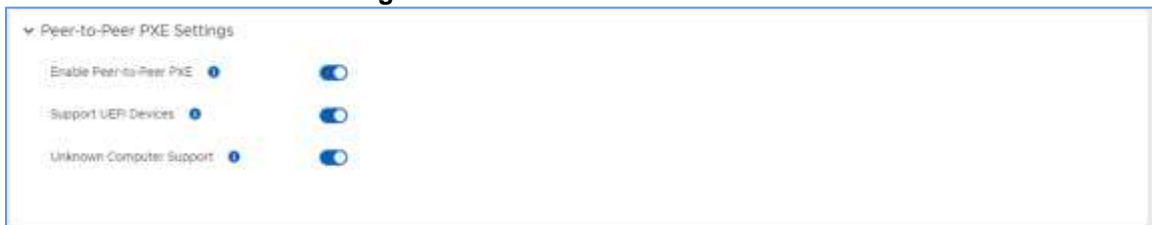
#### Using the Adaptiva Web Portal

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

- Click **Settings, Peer-to-Peer PXE**



- Notice at the top of the page Peer-to-Peer PXE Settings and Unknown Devices. **Peer-to-Peer PXE Settings** should be selected.
- In the **Peer-to-Peer PXE Settings** section



**Enable Peer-to-Peer PXE** – click on the button to toggle to the right to enable the setting  
**Support UEFI Devices** – click on the button to toggle to the right to enable the setting  
**Unknown Computer Support** – click on the button to toggle to the right to enable the setting

- In the **Target Groups** section, either click the button to toggle to the right to Use All Devices or click on Browse and check the box next to the collection / group of computers that will have PXE enabled. Click **Add to List** when complete.



- In the **WAIK/ADK Toolkit Settings** section



**PXE Toolkit** uses specific Microsoft utilities for PXE boot which would normally be present on a ConfigMgr server. If the Adaptiva Server is installed on a server other than the ConfigMgr server, you can use a UNC path to reference the installation location on that server.



- For Vista/Windows 7: Windows Automated Installation Kit (**WAIK**)
- For Windows 8.0: Assessment and Deployment Toolkit (**ADK**)
- From Windows 8.1 and Windows 10: Windows PE Add-on for ADK (**ADK 8.1 and Higher**)

**WAIK/ADK location** – Enter the path to the toolkit installation folder  
 e.g.: C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit

**BCDEdit.exe location** – Enter the path to the where the BCDEdit.exe utility is located.

**IMPORTANT:** If the ADK 8.1 and higher option is selected, the bcdedit.exe utility from ADK 8.0 must be specified. It can be downloaded and extracted from the following link:

<http://adaptiva.cloud/builds/private/bcdedit.zip>

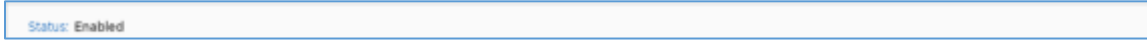
**Use Adaptiva Server Local System Account** – If the path specified is on a remote server and the Adaptiva server's computer account does not have access to the location, toggle the button to the left and enter the credentials to be used.

The remaining settings should be considered optional to enable P2P PXE

- In the **Mac Exclusion** section, add any client MAC addresses you would like to not PXE boot to a PXE enabled client.

- In the **Task Sequence Variables** section, add any task sequence variables and values that OneSiteDownloader may read

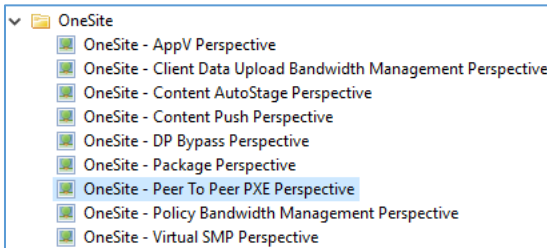
- **Task Sequence Variable Workflow** – specify a custom workflow that will execute on the PXE device to set Task Sequence variables
  - **PXE Approval Workflow** – specify an approval workflow to approve PXE requests. This can also be used to bypass F12 on required deployments
9. At the top of the page, click Save. The Status section will indicate any failures



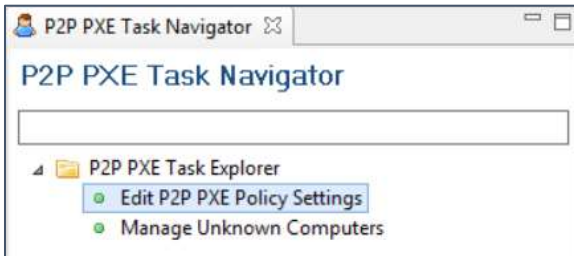
## Using the Adaptiva Workbench

To enable Peer-to-Peer PXE, you must first open the “Peer to Peer PXE Perspective”, which contains UI for enabling and using P2P PXE.

1. Open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **One Site** folder and open the **OneSite – Peer To Peer PXE Perspective**



2. In the **P2P PXE Task Navigator** pane on the left, there are two entries. To enable or disable Peer-to-Peer PXE select the **Edit P2P PXE Policy Settings** item



P2P PXE uses specific Microsoft utilities for PXE boot which would normally be present on a ConfigMgr server. If the Adaptiva Server is installed on a server other than the ConfigMgr server, you can use a UNC path to reference the installation location on that server.

- For Vista/Windows 7: Windows Automated Installation Kit (WAIK)
- For Windows 8.0: Assessment and Deployment Toolkit (ADK)
- From Windows 8.1 and Windows 10: Windows PE Add-on for ADK (ADK 8.1 and Higher)

1. In the **P2P PXE Settings** editor, check the box to **Enable P2P PXE**

- In the **WAIK/ADK toolkit settings** section, specify the following:

**WAIK/ADK toolkit settings**

Microsoft's WAIK/ADK toolkits provide essential tools for PXE booting. Please install the WAIK/ADK toolkit and specify the location below. The location may be on the Adaptiva server, or elsewhere, in which case a UNC path and logon credentials must be provided. A small set of tools from the WAIK/ADK toolkit will be automatically dispatched to computers where P2P PXE has been enabled. Changing the location specified below will trigger the republication and redispach of these tools to these PXE-enabled machines.

Default Locations:  
 C:\Program Files\Windows AIK  
 C:\Program Files (x86)\Windows Kits\8.1\Assessment and Deployment Kit

Select PXE Toolkit  
 WAIK  ADK 8.0  ADK 8.1 and Higher

WAIK/ADK location:

BCDEdit.exe location:

Notes:  
 1) If the PXE target collection contains 32-bit machines, the 32-bit version of the BCDEdit.exe should be selected  
 2) If the PXE target collection contains devices running Windows 7 or earlier, the maximum version of the BCDEdit should be 1607/v10.1.16299

**Select PXE Toolkit** - Select the appropriate toolkit that is installed – this should be **ADK 8.1 or Higher** if using any release of ConfigMgr CurrentBranch.

**WAIK/ADK location** – Enter the path to the toolkit installation folder  
 e.g.: C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit

**ADK 8.0 BCDEdit.exe location** – Enter the path to the where the BCDEdit.exe utility is located.

**IMPORTANT:** If the ADK 8.1 and higher option is selected, the bcdedit.exe utility from ADK 8.0 must be specified. It can be downloaded and extracted from the following link:

<http://adaptiva.cloud/builds/private/bcdedit.zip>

- If the path specified is on a remote server and the Adaptiva server's computer account doesn't have access to the location, uncheck the box: **Use Adaptiva server's local system account for accessing WAIK/ADK tools** and enter the credentials to be used.

Use Adaptiva server's local system account for accessing WAIK/ADK tools

Domain name:

User name:

Password:

- In the **PXE Support for UEFI Devices** section, check the box **Enable Support for PXE Booting UEFI Devices** to support PXE booting UEFI devices

**PXE Support For UEFI Devices**

If you plan to use UEFI devices in your environment, please enable UEFI support by checking the box below.

Enable Support For PXE Booting UEFI Devices

- In the **Enable/Disable unknown computer support** section, check the box **Enable Unknown Computer Support** to enable unknown computer support.

**Enable/Disable unknown computer support**

Please specify whether you wish to enable support for PXE booting of unknown computers using Peer-to-Peer PXE.

Enable Unknown Computer Support

**NOTE:** For OneSite to work with Unknown Computers, it must be enabled within the selected boot images in ConfigMgr.

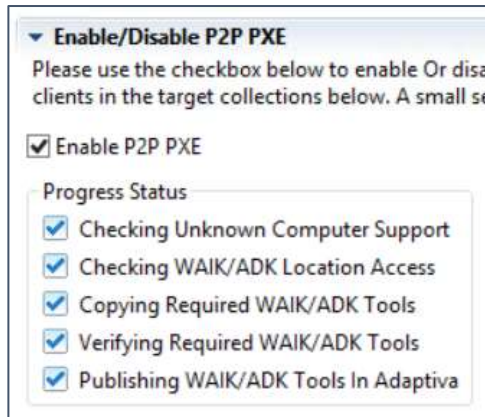
- In the **Target Collection** section, drag and drop one or more SCCM collections into the **Target Collection** field, or alternatively, check the box **Use All Adaptiva Clients**. All the computers that are part of these collections will automatically receive a small package of WAIK/ADK tools and

will be capable of becoming PXE responders and TFTP servers to serve other machines on their respective subnets.



**NOTE: It is strongly recommended that you enable Peer-to-Peer PXE on All Adaptiva Client computers, and completely do away with PXE servers in your entire ConfigMgr environment.**

7. The remaining sections described below should be considered optional to enable P2P PXE
  - In the **Mac Exclusion List** section, add any client MAC addresses you would like to not PXE boot to a PXE enabled client.
  - In the **Task Sequence Variables** section, add any task sequence variables and values that OneSiteDownloader may read
  - In the **P2P PXE Server Workflow** section, specify a **Task Sequence Variable Workflow** that will execute on the PXE device to set Task Sequence variables
  - In the **PXE Approval Workflow**, specify an approval workflow to approve PXE requests. This can also be used to bypass F12 on required deployments
8. At the top of the editor, click the **Apply** button. The Progress Status section will indicate any failures. All boxes must be checked before PXE is available.



## Policy Bandwidth Management

### Overview

In many large ConfigMgr implementations, the servers hosting the Management Point (MP) role will reside in a datacenter as they provide a critical role for client management and should be reliable. In the case where there are many ConfigMgr clients located at remote sites, these clients will connect to an MP over the WAN to request policy, and by default, will do so every 60 minutes. Normally the amount of data transferred when a client checks for policy is nominal but consider the case where you are managing tens of thousands of clients located at many remote offices with slow WAN links. Each client will initiate an HTTP (or HTTPS) connection to its MP, and the MP will query the ConfigMgr database to see if there are any new policies for the client, then return the results. Considering the amount of policy checks being done by all of these clients in a given day, only a small fraction will return any actionable results such as a new package deployment or client setting change. The process unnecessarily consumes resources on the MP, the site database, and of course the WAN. The Policy Bandwidth Management feature of OneSite, also known as Policy Push, provides a solution which can dramatically reduce the frequency of these policy requests.

Due to OneSite's deep integration with ConfigMgr, it immediately detects policy changes for a given client when they are made. When the Policy Bandwidth Management feature is enabled, Adaptiva OneSite will instruct only the targeted clients to check for policy in real time. This feature allows administrators to increase their policy polling interval to the maximum value which is 24 hours. If there are no applicable policy changes for a given client within the 24 hours interval, the client will not attempt to check.

In addition to the WAN traffic reduction, this is a powerful feature for administrators because applicable policy changes are received by the client much sooner than if they had to wait for the standard Machine Policy Retrieval & Evaluation Cycle to start.

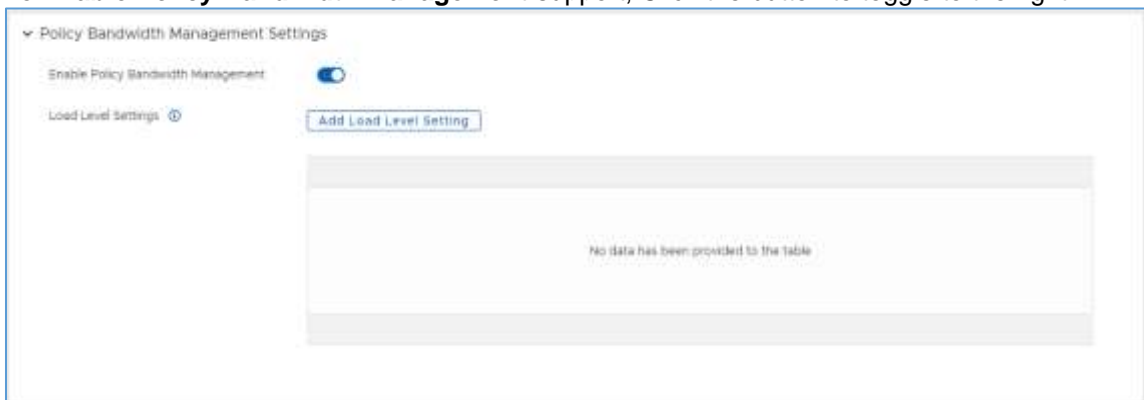
## Enabling Policy Bandwidth Management

### Using the Adaptiva Web Portal

1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Go to OneSite ConfigMgr Edition** or click **OneSite Anywhere, OneSite ConfigMgr Edition**
4. Click **Settings, Policy Bandwidth Management**



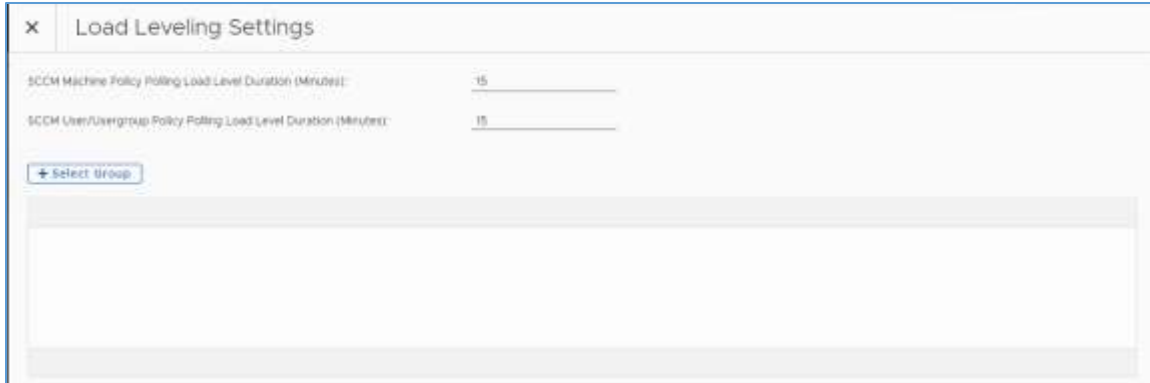
5. To **Enable Policy Bandwidth Management** support, Click the button to toggle to the right



By default, when a policy change is detected by the Adaptiva Server, it will immediately send a notification to applicable clients to check for policy. If Policy Bandwidth Management is enabled, and a policy change is applicable to many clients, an administrator may not want all of the clients to check at the same time. OneSite provides a mechanism to load level policy updates to targeted clients over a given duration. For example, if the Adaptiva Server needs to send a notification to

100 machines for a policy check, and the policy load level duration is set to 10 minutes, 10 machines will check for policy every minute until the 10 minutes has passed.

6. To create a new load level setting, click **Add Load Level Setting**



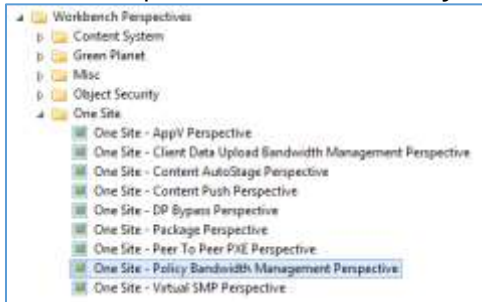
7. Modify the duration in minutes for each of the policy intervals
  - SCCM Machine Policy Polling Load Level Duration (Minutes)
  - SCCM User/Usergroup Policy Polling Load Level Duration (Minutes)

As an example, if the Adaptiva Server needs to send a notification to 100 machines for a policy check, and the policy load level duration is set to 10 minutes, 10 machines will check for policy every minute until the 10 minutes has passed.

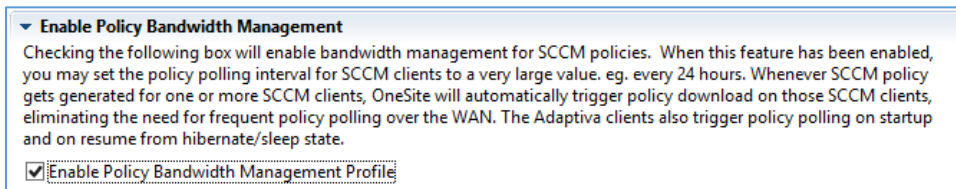
8. Click **+ Select Group** to select the Collection/Group that the Load Leveling settings will be applied to. Check the box next to each group to be targeted. Click on **Add To List**
9. Click on **Add**
10. Add additional Load Level Settings as required
11. Click **Save**

## Using the Adaptiva Workbench

1. Open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **One Site** folder and open the **One Site – Policy Bandwidth Management Perspective**.



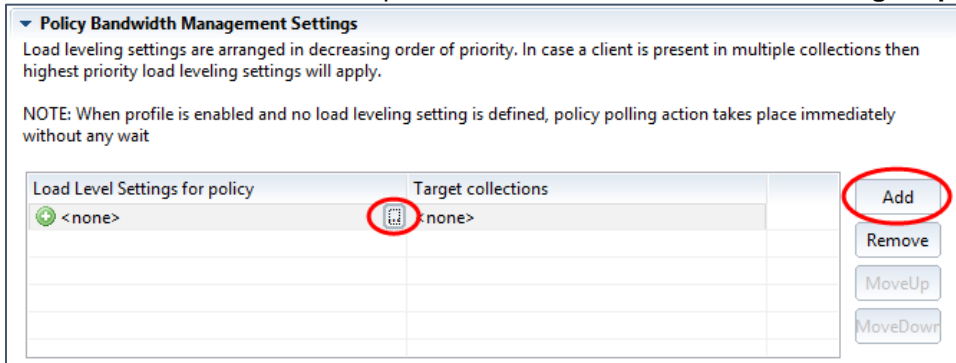
2. In the **Policy Bandwidth Management Profile** editor, in the **Enable Policy Bandwidth Management Profile** section, check the box next to **Enable Policy Bandwidth Management Profile**.



By default, when a policy change is detected by the Adaptiva Server, it will immediately send a notification to applicable clients to check for policy. If Policy Bandwidth Management is enabled, and a policy change is applicable to many clients, an administrator may not want all of the clients to check at the same time. OneSite provides a mechanism to load level policy updates to targeted clients over a given duration. For example, if the Adaptiva Server needs to send a notification to 100 machines for

a policy check, and the policy load level duration is set to 10 minutes, 10 machines will check for policy every minute until the 10 minutes has passed.

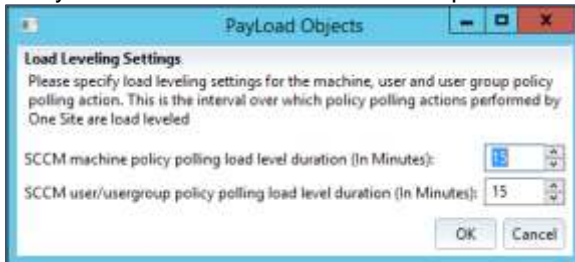
- To create a new load level setting, In the **Policy Bandwidth Management Settings** section, click the **Add** button then click the ellipses, ..., button in the **Load Level Setting for policy** column.



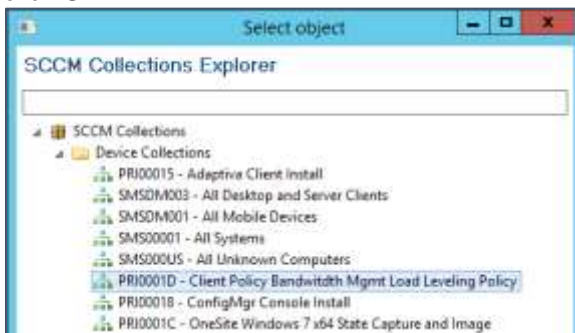
- In the **PayLoad Objects** dialog box, modify the duration in minutes for each of the policy intervals then click **OK**.

- SCCM machine policy polling load level duration (In Minutes)
- SCCM user/usergroup policy polling load level duration (In Minutes)

As an example, if the Adaptiva Server needs to send a notification to 100 machines for a policy check, and the policy load level duration is set to 10 minutes, 10 machines will check for policy every minute until the 10 minutes has passed.



- In the **Select object** dialog box, choose the collection to apply the load leveling settings, then click **OK**.



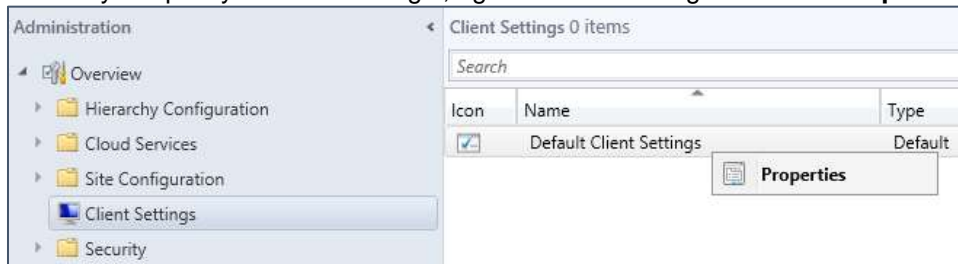
- Multiple entries can be added for load leveling settings for different target collections.

## Modifying ConfigMgr Client Policy Retrieval Settings

Now that Policy Bandwidth Management is enabled, the setting for how often ConfigMgr clients check for policy can be modified.

In ConfigMgr, client settings can be modified to apply to all clients assigned to the site, or a custom Client Device Settings policy can be created with a higher priority than the default and targeted to a collection. This might be desired in a test scenario.

1. In the ConfigMgr console, open the **Administration** workspace and select **Client Settings**. Select **Default Client Settings** to target all ConfigMgr clients or select **Create Custom Client Device Settings** to target a specific collection(s).
2. To modify the policy retrieval settings, right-click the setting and select **Properties**.



3. In the left pane, select **Client Policy** and in the right-pane, modify the **Client policy polling interval (minutes)** setting to the maximum value, which is **1440** minutes (24 hours).



4. Click **OK** to save the changes to the policy. Moving forward, all clients will check for policy once every 24 hours unless a change is applicable, when the Adaptiva Server will instruct clients to check for policy.

## Virtual SMP

### Overview

Adaptiva OneSite includes a feature called Virtual State Migration Points or Virtual SMP. The Virtual SMP offers an efficient alternative to the ConfigMgr State Migration Point role. Much like OneSite enables the elimination of secondary sites and distribution points, Virtual SMPs make use of the revolutionary OneSite Virtual SAN, the Caching File System, and Peer-to-Peer technologies to enable the elimination of State Migration Points from ConfigMgr environments.

Virtual SMP tasks are integrated directly into the SCCM Task Sequence UI for seamless administration and operation. Deep integration is also provided with SCCM Computer Associations, enabling the use of OneSite's Virtual SMP as a simple replacement for potentially hundreds of physical SMP servers.

More information can be found in the Adaptiva OneSite OSD User Guide.

### Enabling Virtual SMP

#### Using the Adaptiva Web Portal

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



4. Click **Settings, Virtual SMP**



5. To **Enable Virtual SMP** support, Click the button to toggle to the right

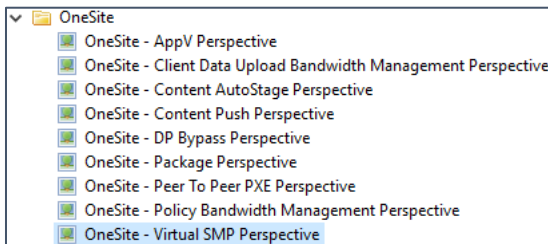


6. Click on **Save**

### Using the Adaptiva Workbench

To enable the Virtual SMP feature:

1. Open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **One Site** folder and open the **OneSite – Virtual SMP Perspective**.



2. To enable the Virtual SMP feature, check the box **Enable Virtual SMP On Specified Collections**.
3. In the **Target Collections** section, drag a collection of machines you want to serve as Virtual SMPs or check the box **Use All Adaptiva Clients**.




4. Click **Apply** to enable the Virtual SMP feature on the target systems. This will enable all targeted clients to participate as state store hosts for OneSite Virtual SMP.

# Client Settings

Client Settings (aka System Configurations) can be used to create configuration changes for a group of devices or globally for all client devices.

## Using the Adaptiva Web Portal

1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on the gear, , **Settings**, then select **Client Settings Policies**
4. To create a new policy, click on **+New**



In **General Settings**, complete the following:

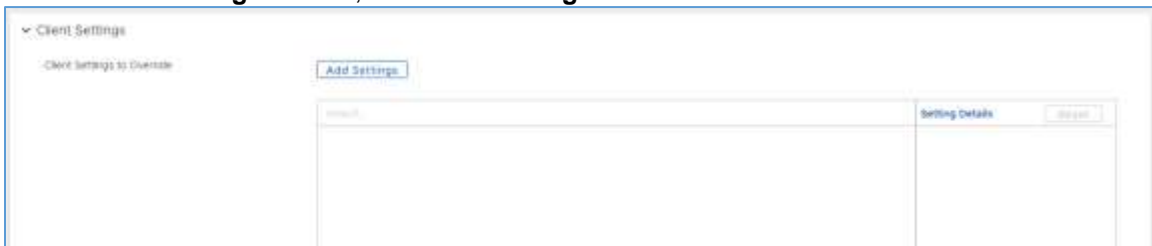
**Name:** Enter a descriptive name

**Description:** Enter a description

**Priority:** To ensure these settings apply to the target groups, set this value greater than 1

**Target Groups:** Click on Browse and check the box next to one or more collections / groups and click **Add to List**

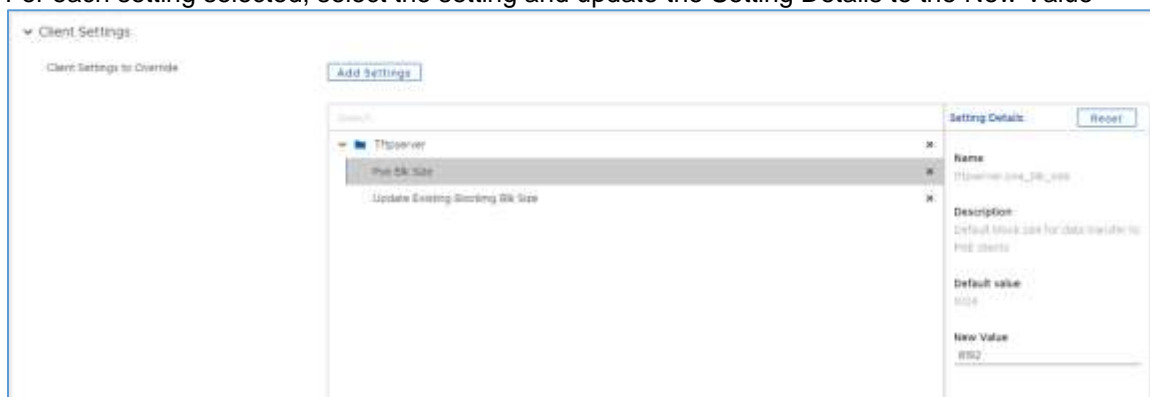
5. In the **Client Settings** section, click **Add Settings**



- The **Select Client Settings** page will be displayed



- Using the Search box, or expand individual categories, check the box next to each setting to customize  
For example, to change the TFTP Block Size when PXE booting, type in the Search box **PXE Blk Size** or expand **Tftpserver**. Check the box next to **Pxe Blk Size** and **Update Existing Booting Blk Size**  
Click OK
- For each setting selected, select the setting and update the Setting Details to the New Value



For example, to improve the speed of the TFTP transfer of the WinPE Boot image using PXE, Select **Pxe Blk Size** and enter **8192** in the **New Value** field. Select the **Update Existing Booting Blk Size** and enter **true** in the **New Value** field

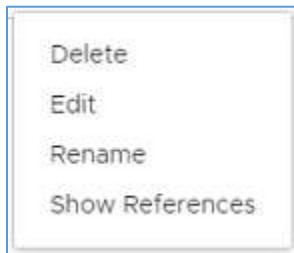
**NOTE:** The Name field contains the registry value name that can be found in *HKLM\Software\WOW6432Node\Adaptiva\client* (for 64-bit clients)

Click on **Reset** to change the value back to the default (this will blank the New Value field)

9. After all settings have been updated, click on **Save**. This will immediately distribute this policy to all target clients

## Using the Actions menu

For each Client Settings policy, hover over the policy and click on the ellipses, ..., to display the Actions menu



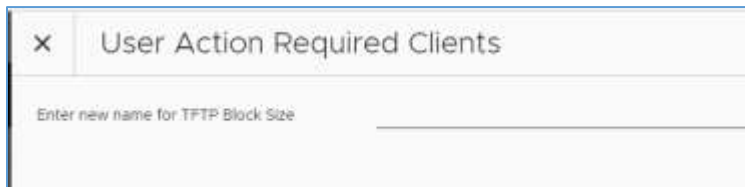
**NOTE:** The built-in Client Setting policies cannot be Edited or Deleted and those actions will be grayed out

### Edit

Click on Edit to open the Client Settings policy

### Rename

Click on Rename to change the name of the Client Settings policy



Enter the new name and click **Save**

### Delete

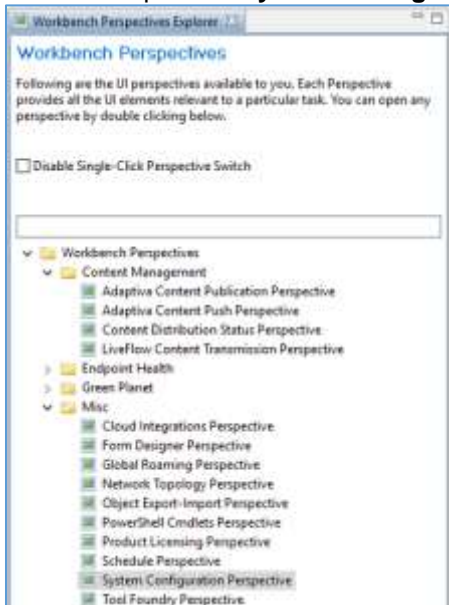
Click on **Delete** to delete the Client Settings policy

### References

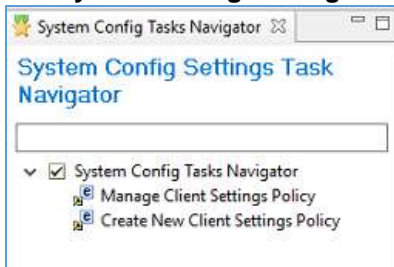
Click on **References** to show where the Client Settings policy is used

## Using the Adaptiva Workbench

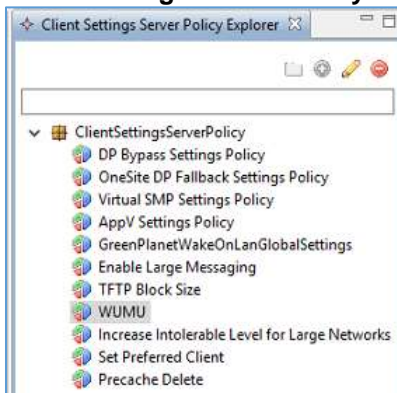
1. Open the Adaptiva Workbench and in the **Workbench Perspectives** pane, expand the **Misc** folder and open the **System Configuration Perspective**.



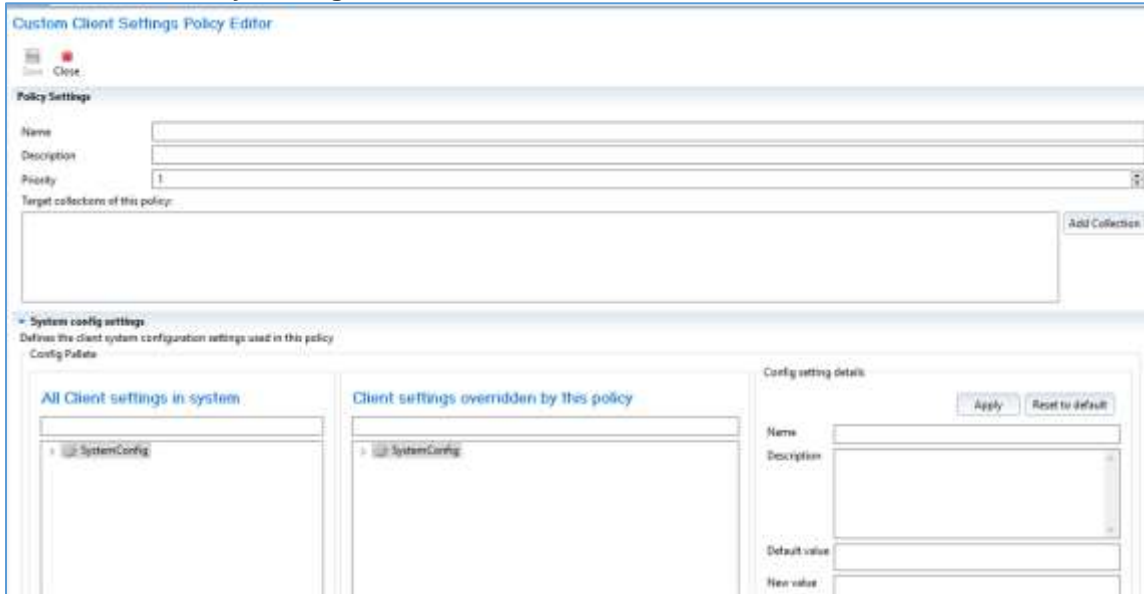
2. The **System Config Settings Task Navigator** will be displayed



3. Clicking on **Manage Client Settings Policy** will change the focus to the right-hand pane in the **Client Settings Server Policy Explorer**



- Clicking on **Create New Client Settings Policy** will open the **Custom Client Settings Policy Editor**. In the **Policy Settings** section:



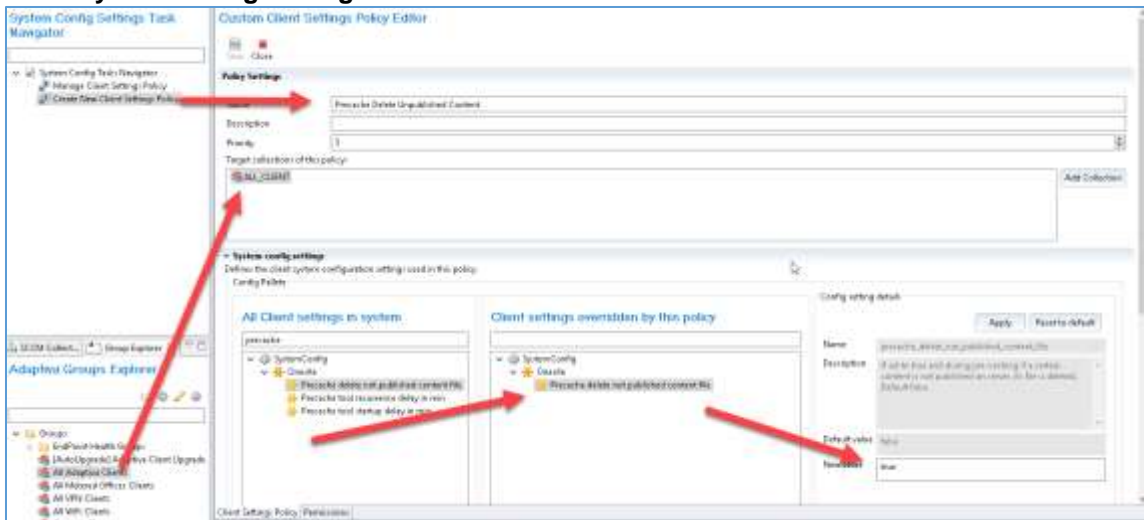
**Name:** Enter a descriptive name

**Description:** Enter a description

**Priority:** To ensure these settings apply to the target groups, set this value greater than 1

Click on **Add Collection** and select a ConfigMgr collection and click **OK**. Alternatively, right-click in the **Target collections of this policy** box and select **Add object** and select an Adaptiva group. Repeat for each target collection / group

- In the **System config setting** section:



- Using the Search box below **All Client settings in system**, or expand individual categories below **SystemConfig**, select the setting to customize and drag it on top of **SystemConfig** in the center pane

For example, to ensure content that is no longer published on the server is removed from the AdaptivaCache on the client, type in the Search box **precache** or expand **Onesite**. Drag **Precache delete non published content file** to **SystemConfig** in the center pane

- For each setting selected, select the setting and update the Config setting details New Value and click **Apply**



**IMPORTANT:** Be sure to click **Apply** after changing **EACH** setting

12. After all settings have been updated, click on **Save**. This will immediately distribute this policy to all target clients

## Client Settings Server Policy Explorer

The following actions are available in the explorer

### Icon bar

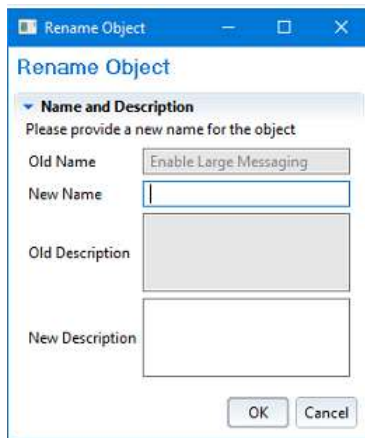
-  Select a custom Client Settings Server Policy and click the pencil icon to **Edit** the policy
-  Select a custom Client Settings Server Policy and click the reg icon to **Delete** the policy

### Delete

Click on **Delete** to delete the Client Settings policy

### Rename

Click on Rename to change the name of the Client Settings policy



The image shows a 'Rename Object' dialog box. It has a title bar with 'Rename Object' and standard window controls. The main area is titled 'Rename Object' and contains a section 'Name and Description' with a dropdown arrow. Below this, it says 'Please provide a new name for the object'. There are four input fields: 'Old Name' (containing 'Enable Large Messaging'), 'New Name' (empty), 'Old Description' (empty), and 'New Description' (empty). At the bottom right are 'OK' and 'Cancel' buttons.

Enter the new name and click **OK**. The Description can also be changed.

### Open in editor

Click on Open in editor to open the Client Settings policy

### Save as..

Click on Save as... to save the Client Settings policy to a new policy

### Export

Click on Export to open the Object Export Settings to export the Client Settings policy to a file or a linked server

### Show references

Click on Show references to show where the Client Settings policy is used

# Additional Configuration Items

## Event Notifications

xxx

## REST API Endpoints

Information about REST API Endpoints can be found in the Adaptiva Support Portal located here: [REST API Foundry User Guide – Adaptiva Support Portal](#)

Xxx this is currently restricted to Accenture Users

## Sensor Offline Cache

Xxx

This should be for Endpoint Inventory ONLY



# Dashboards

Dashboards are only available with the Adaptiva Web Portal.

Xxx

Written up here: [User Dashboards – Adaptiva Support Portal](#)


## Using the Legacy Dashboard Content Download Details

Xxx this should be replaced with Content\_Receipts

### Prerequisites

There is a prerequisite action that must be completed before this dashboard can be used. This only needs to be completed once.

**CAUTION: This change has the potential to impact database size and performance. It is recommended to target only a subset of devices**

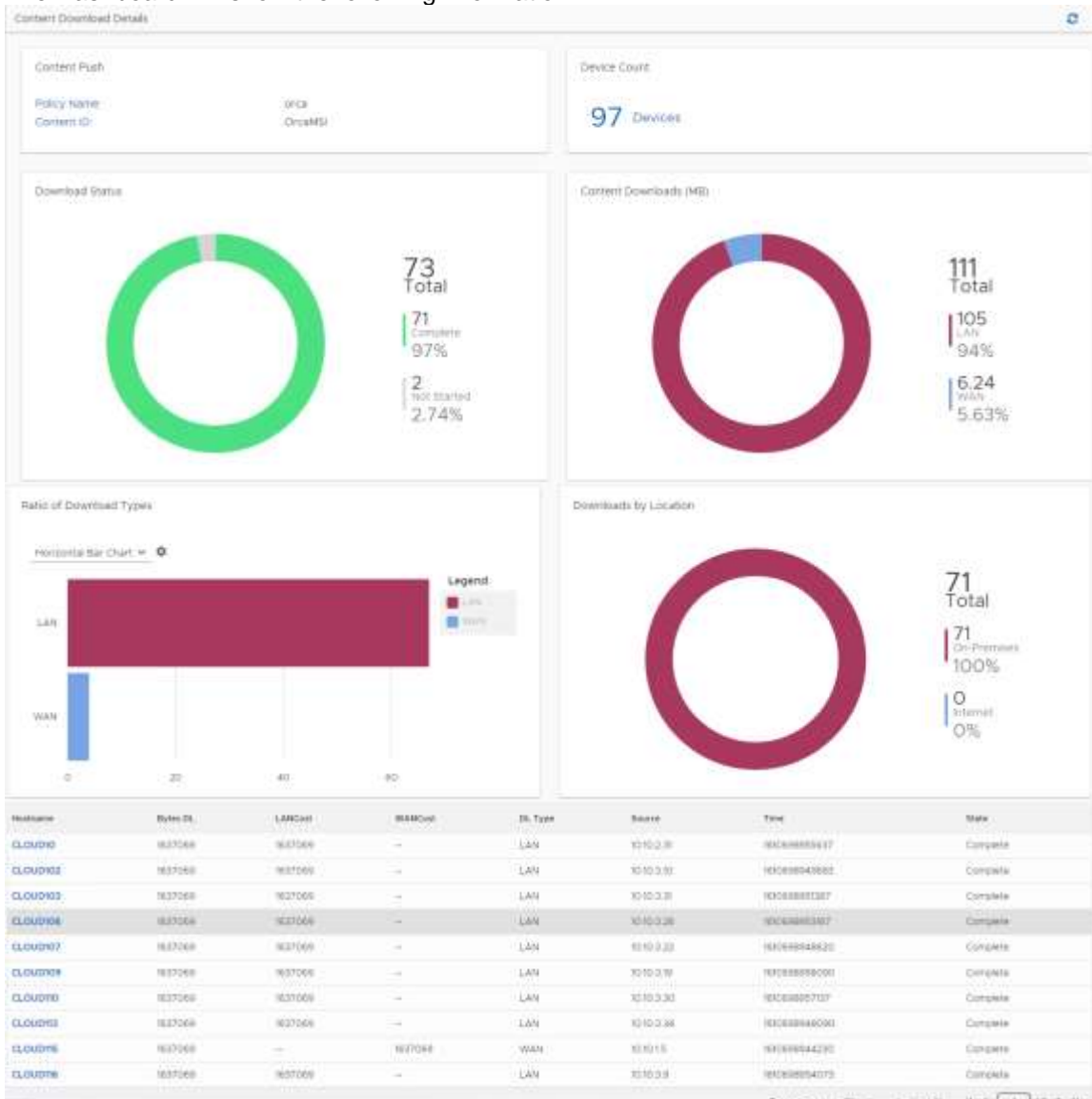
1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – `http[s]://AdaptivaServerFQDN[:port]`
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on the gear, , Settings, and then select **Client Settings Policies**
4. Click on **+New** to create a New Client Settings policy
5. Enter the following:  
Name: Enable Content Push Status Details  
Description:  
Priority: 2  
Target Groups: Groups -> select a group or collection  
Client Settings: ContentSystem -> Send Content Push Status : true
6. Click on **Save**

### Content Download Details

Content Download Details assumes a Content Push policy has been used to push content to a group of clients. To view the data, the content push policy must have run and the clients must have the setting enabled from the prerequisites.

1. From the Dashboards page, select **Legacy Dashboard**
2. Select on Content Download Details
3. Check the box next to the specific Content Push policy and click OK

4. The Dashboard will show the following information:



**Policy Name** – The name of the Content Push policy

**Content ID** – The list of ContentIDs that were included in the Content Push policy (currently, this will show the first Content ID)

**Device Count** – The total number of devices targeted

**Download Status** – The number of computers that have completed, are in progress, or not started the download

**Content Downloads (MB)** – The amount of MB that has been downloaded across the LAN, WAN, Internet

**Ratio of Download Types** – This shows a bar chart of the Content Downloads (MB) info. If there are multiple content IDs the amount downloaded will reflect the total size.

**Downloads by Location** – This shows the number of computers on-premises vs those on the internet that downloaded the content

**List of Computers** – This list shows all computers that have downloaded the content and where the content was downloaded from



# 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

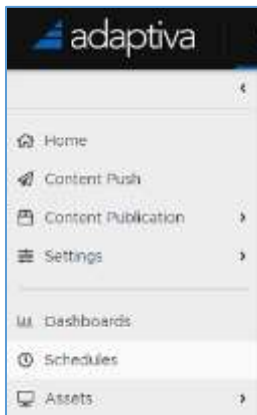
Last Saturday Of Every Month

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

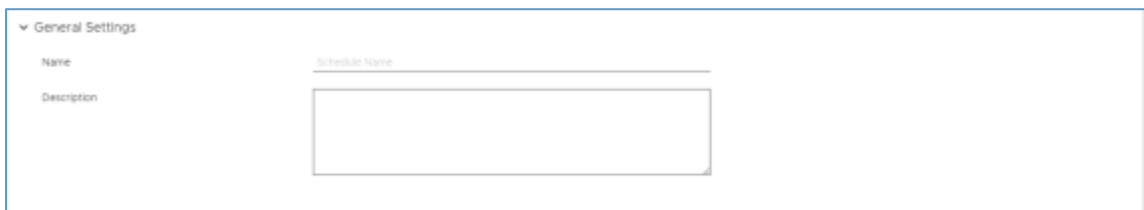
## Creating a Custom Schedule

### Using the Adaptiva Web Portal

1. Connect to the Adaptiva Web Portal using your web browser (except Internet Explorer) – `http[s]://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**

A screenshot of the 'General Settings' form in the Adaptiva web portal. The form is titled 'General Settings' and has two input fields: 'Name' and 'Description'. The 'Name' field is labeled 'Schedule Name' and the 'Description' field is a larger text area.

**Name** – Enter a descriptive name for the new schedule

**Description** – Enter a description

## Schedule Settings

**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

**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   ▾

**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

Day of the Week

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

Month By Date Setting ⓘ

Recurring Interval in Months

Day of Month

### Recurring Monthly By Last Day – Enter the Month interval

Month By Last Day Setting ⓘ

Recurring Interval in Months

**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

Day of the Week

Week of the Month

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  days

Override Duration  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

End 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**

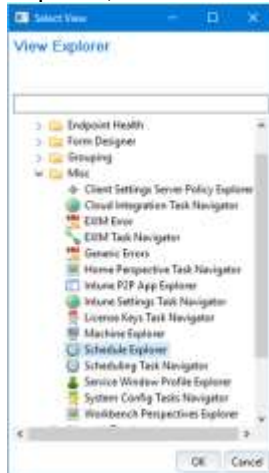
**Load Leveling Duration:** Select the Load level duration in days, hours, or minutes. The target list of devices will be balanced across the time interval

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

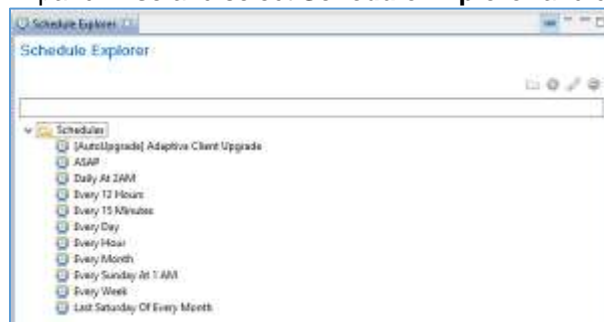
5. Click **Save**

## Using the Adaptiva Workbench

1. There is no Schedule Perspective, but there is a Schedule Editor. To open the Schedule Explorer, select the View menu, then Manage Views



2. Expand **Misc** and select **Schedule Explorer** and click **OK**



3. Select Schedules and click the green + to create a new Schedule

**Schedule Editor**

Save SaveAs Close

**Basic Information**  
Basic Information for this Schedule.

Name

Description

**Schedule Type**  
Schedule Type determines when and how often the Schedule is run

ASAP  
 Non Recurring  
 Recurring Interval  
 Recurring By Day  
 Recurring By Week  
 Recurring Monthly By Date  
 Recurring Monthly By Last Day  
 Recurring Monthly By Day Of The We

**Start/End Time**  
The Start time specifies when the schedule will begin firing. If the Start time has already passed then it will fire immediately, subject to service window constraints.

Use Server Time Zone       Enable End Time

**Start Time**      **End Time**

5 : 13 : 5 PM      5 : 13 : 6 PM

August 2020      August 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						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					

**Constraints**  
If a Service Window Constraint is specified, the Schedule will only run within the provided range.

Service Window Constraints Status: Not Applied      Add      Remove

Schedule Editor | Permissions

**Name** – Enter a descriptive name for the new schedule

**Description** – Enter a description

**Schedule Type** – Select a Schedule 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 Settings**

Please enter a number of days, hours or minutes as the Schedule Interval.

Recurrence Interval  days



**Recurring By Day** – Check the day of the week

▼ **Day Settings**  
 The Schedule will fire at the start time on the specified days of the week.

Days of the Week: Sun Mon Tue Wed Thu Fri Sat

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

▼ **Week Settings**  
 This Schedule will occur once every X weeks on the specified day of the week.

Recur Interval In Weeks:   
 Day of the Week:

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

▼ **Month By Date Settings**  
 This Schedule will occur once every X months, on or after the specified date.

Recur Interval In Months:   
 Day of Month:

**Recurring Monthly By Last Day** – Enter the Month interval

▼ **Month By Last Day Settings**  
 This Schedule will occur once every X months on the last day of the month.

Recur Interval In Months:

**Recurring Monthly By Day Of The Week** – Enter the Month interval for a specific day and week of the month. Check the box **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**  
 This Schedule will occur once every X months on the Yth day of the week on the Zth week of the month.

Recur Interval In Months:   
 Day of the Week:   
 Week of the month:   Last week of the month

**Start/End Time** – The Start and optional End of the schedule

**Use Server TimeZone** – Check this box to use the time zone of the Adaptiva server

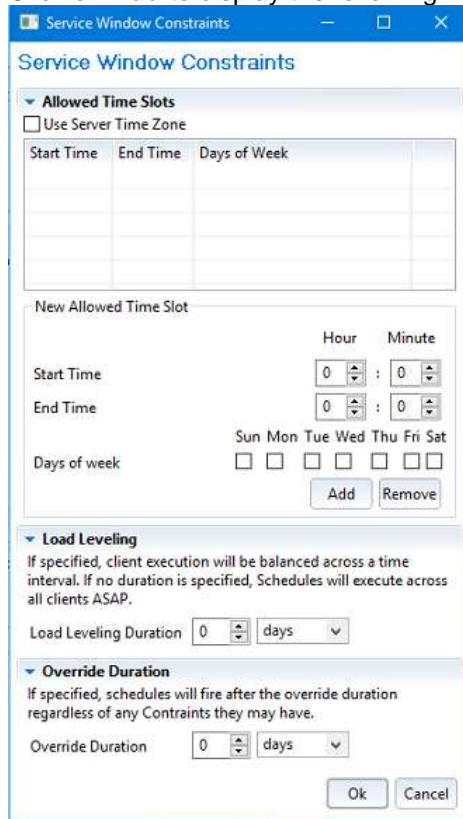
**Enabled End Time** – Check this box, if available, to end the schedule on this date

Select the time using Hour, Minute and Second spinners

Select the Month and the Year

Select the date in the month

**Constraints** – Create additional constraints for this schedule, including load leveling  
Click on **Add** to display the following:



**Service Window Constraints**

Use Server Time Zone

Start Time	End Time	Days of Week

**New Allowed Time Slot**

Start Time: Hour: 0 Minute: 0

End Time: Hour: 0 Minute: 0

Days of week: Sun Mon Tue Wed Thu Fri Sat

**Load Leveling**

If specified, client execution will be balanced across a time interval. If no duration is specified, Schedules will execute across all clients ASAP.

Load Leveling Duration: 0 days

**Override Duration**

If specified, schedules will fire after the override duration regardless of any Constraints they may have.

Override Duration: 0 days

**Use Server Time Zone** – Check this box to use the time zone of the Adaptiva server

**New Allowed Time Slot** – Enter the Start Time, End Time using the 24-hour clock and select the days of the week the schedule is allowed to run.

Then click **Add**

To delete an existing time slot, select the time and click **Remove**

**Load Leveling** – 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

Click **OK**

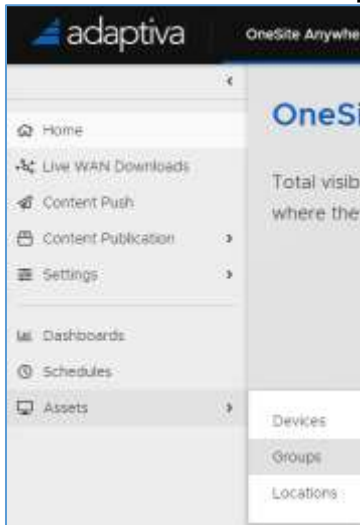
4. Click **Save**

# Adaptiva Groups

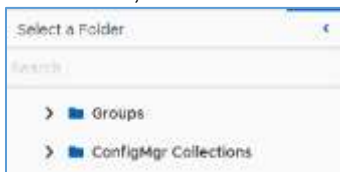
## Using the Adaptiva Web Portal

### Creating a Group

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



4. This will open the Groups page showing all groups and if integrated with ConfigMgr, ConfigMgr collections. When integrated with ConfigMgr, the collections and groups will display together. To only see the Adaptiva Groups, select the Groups folder on the left or to see only the ConfigMgr Collections, select that folder in the left pane.



5. Click on **+ New** to create new Adaptiva Group

### General Settings

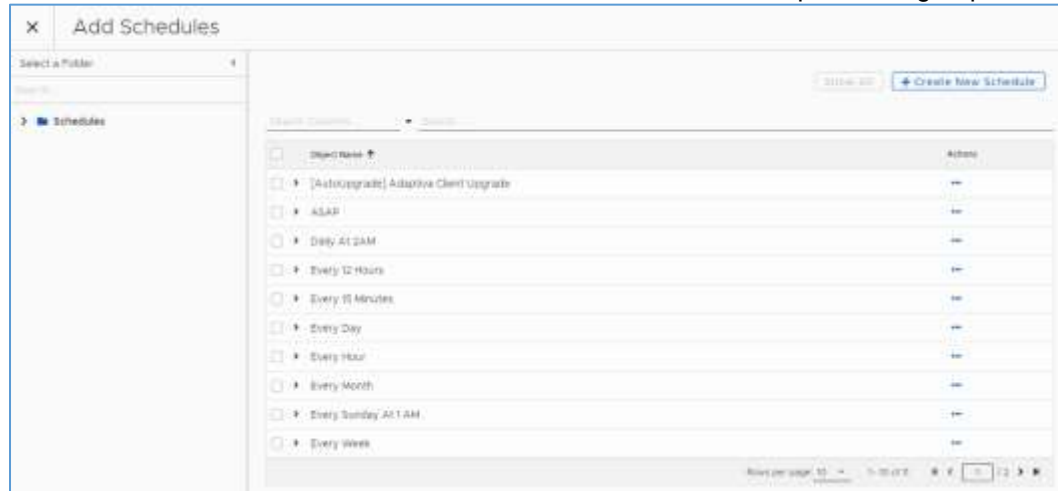


The screenshot shows the 'General Settings' form for creating a new Adaptiva Group. The form is titled 'General Settings' and has a dropdown arrow on the left. It contains the following fields and controls:

- Name:** A text input field with the placeholder text 'Group Name'.
- Description:** A larger text area for entering a description.
- Evaluation Schedules:** A section with a plus icon and a link to 'Add Schedules'.
- BROWSE:** A button located at the bottom right of the form.

- **Name** – Enter a name to identify the group.
- **Description** – This text field allows you to add a description for the group (optional).

- **Evaluation Schedules** – Click on Browse to select a schedule to update the group.



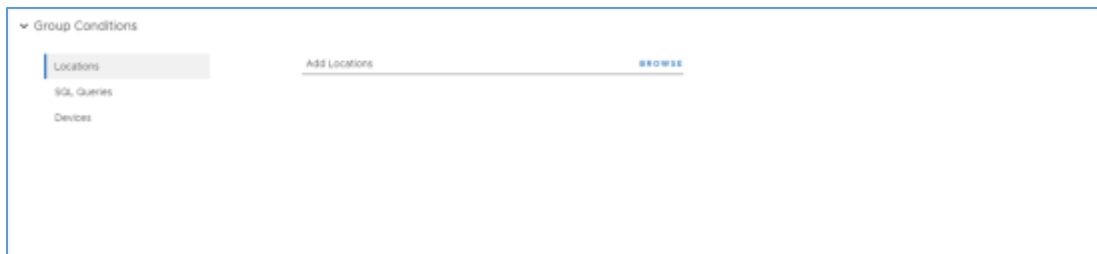
ASAP and non-recurring schedules run once and are not repeated.

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 start on March 31st at 5pm, April 30th at 5pm and so on.

1. Check one or more boxes next to the desired schedule(s) or click **+Create Server Object** to create a new Schedule
2. Click **Add to List** to return to the Create Group page

### Group Conditions



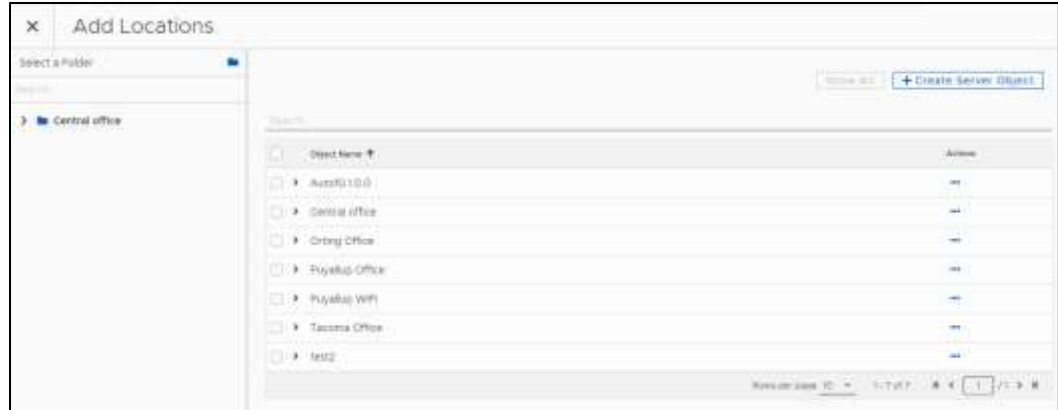
There are 3 different conditions that be selected:

- **Locations** – Create a Group based on a Location
- **SQL Queries** – Create a Group based on a SQL Query
- **Devices** – Create a Group based on a list of devices

See below for the actions required for each condition

#### Locations

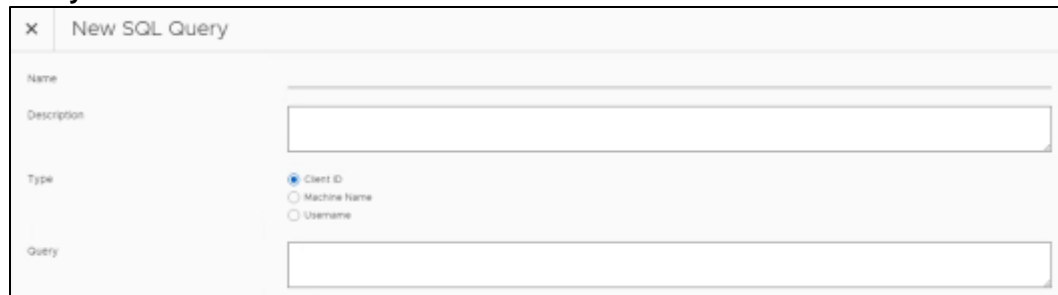
1. To create a group based on one or more Locations select **Locations** and then click **Browse**



2. Check one or more boxes next to the desired schedule(s) or click **+Create Server Object** to create a new Location
3. Click **Add to List** to return to the Group Conditions page

### SQL Queries

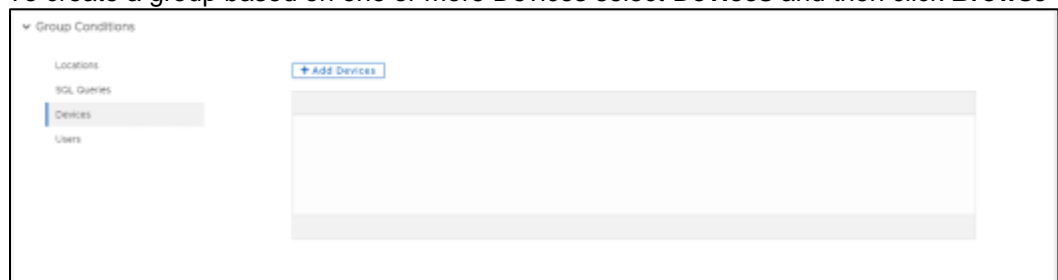
1. To create a group based on a SQL Query select **SQL Queries** and then click **+ Add Query**



2. Enter the **Name** of the query.
3. Enter an optional **Description** for the query
4. Select the **Type** of field that will be returned as the first field. Client ID, Machine Name, User Name
5. Enter the **Query**
6. Click **Add Query** to return to the Group Conditions page

### Locations

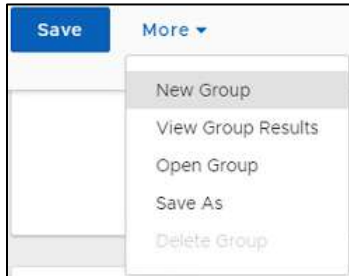
1. To create a group based on one or more Devices select **Devices** and then click **Browse**



2. Click on **+ Add Devices** to get the list of devices
3. Check one or more boxes next to the desired device(s)
4. Click **Add to List** to return to the Group Conditions page
7. Click on **Save**

## Additional Options

Clicking on More will display another menu



- **New Group** – Create a New Group
- **View Group Results** – Display the results of the group created
- **Open Group** – Open the Group created so the Group conditions can be changed
- **Save As** – Save the Group as a new name
- **Delete Group** – Deletes the current Group

## Using the Adaptiva Workbench

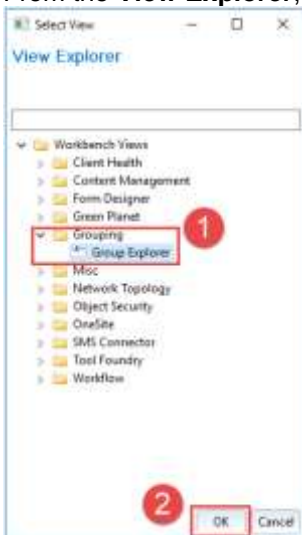
Primarily throughout OneSite, you will use ConfigMgr collections to identify which machines a policy or workflow should apply. However, there are times where it may be more advantageous to create groups of computers based on information gathered from the Adaptiva Client. A prime example of this would be to create groups based on the offices defined in the Adaptiva platform.

To create an Adaptiva group, please perform the following:

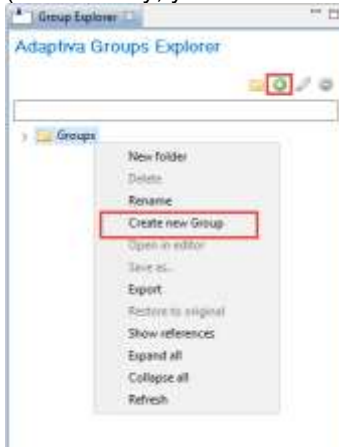
1. From the top left click on **Manage Views** icon as shown below:



2. From the **View Explorer**, expand **Grouping**, select **Group Explorer**, and click **OK**



3. In the **Adaptiva Groups Explorer**, right-click on the **Groups** and select on **Create New Group** (alternatively, you can also use the **+** sign to create a new group).



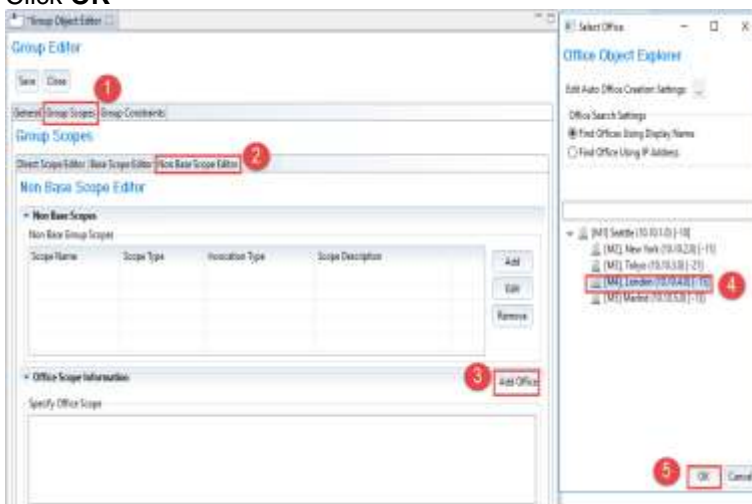
4. In the **Group Object Editor**, on the **General** tab, input the **Group Name** for the group you want to create.



## Creating a Group Based on Office

In this step we will discuss on how to include the clients to be part of the group.

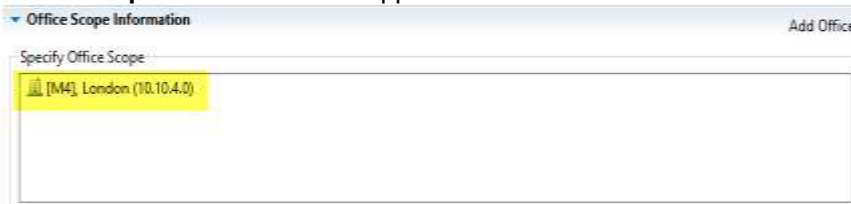
1. First, by directly selecting the entire office so that all the clients in the office will be part of the group. To do this, select the **Group Scopes** tab
2. Select the **Non Base Scope Editor** tab
3. To select an office, click on **Add Office**
4. The **Office Object Explorer** window will appear, then select the office that is going to part of the group
5. Click **OK**



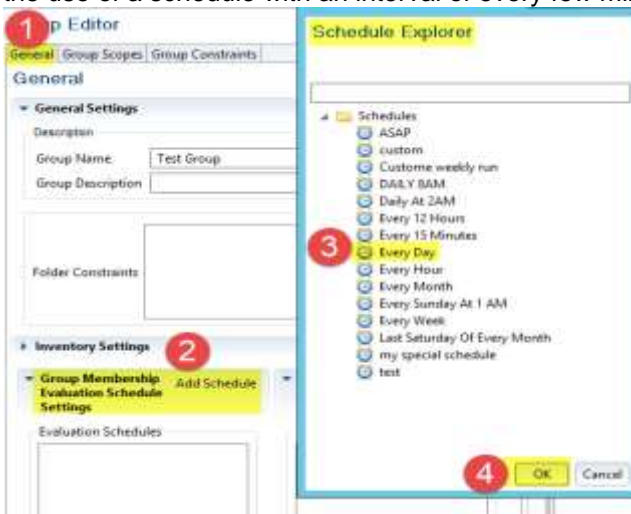
You can select multiple offices to be part of the group and add the offices later once the group gets created.

**NOTE: Only the clients that are part of the office(s) selected will be part of the group. Suppose you are targeting a parent Office that had multiple child offices, and only the Parent office is selected, then only the parent office clients will be part of the group.**

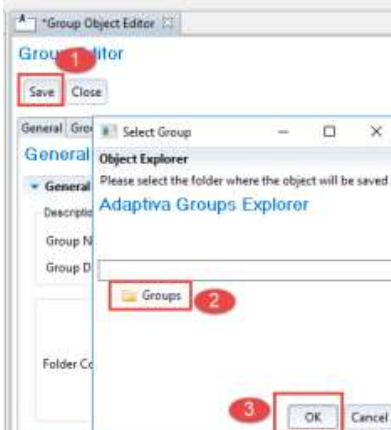
- Office Scope Information will appear like below.



- Adding a schedule will update the group membership, based on the interval specified. If any new clients appear in the office, then those clients will become part of the group when the schedule triggers. As shown below, click on **General** tab and if you scroll down a little you will notice **Group Membership Evaluation Schedule Settings** and next to it click on **Add Schedule**.
- From the **Schedule Explorer** window, select the schedule and then click **OK**. It is better to avoid the use of a schedule with an interval of every few minutes to reduce the load on the server.



- Save the group by clicking on **Save** on the **Group Editor**. The **Adaptiva Groups Explorer** window will appear, select the **Groups** folder, and click **OK**.

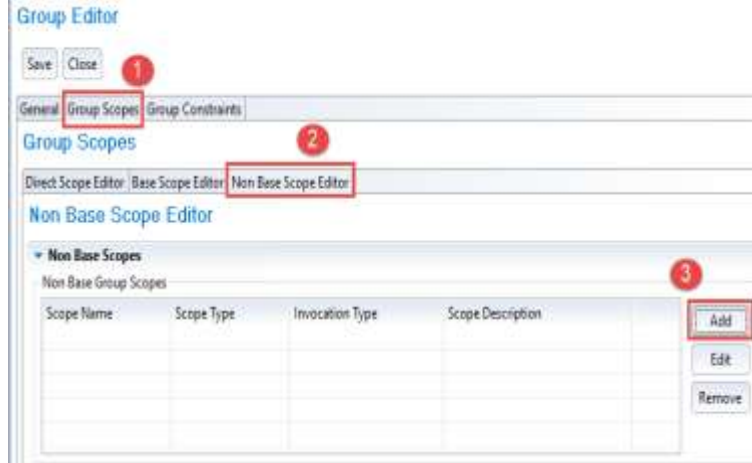




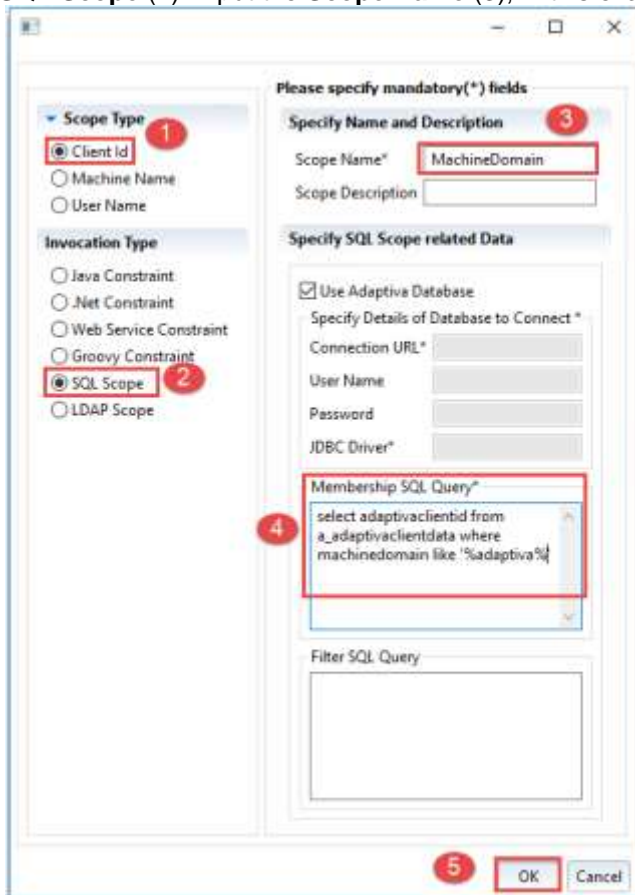
## Creating a Group Based on SQL Query

In this step we will discuss how to add Adaptiva clients to a group based on a SQL Query.

1. These are the same steps as above. Provide the group name in the general tab and now go to the **Group Scopes** tab (1), **Non Base Scope Editor** tab (2), and then click on **Add** (3).



2. In the dialog box that opens, select the **Scope Type** as **Client Id** (1) and **Invocation Type** as **SQL Scope** (2). Input the **Scope Name** (3), in this example, it is named *MachineDomain*.



**NOTE:** All other Invocation Types are under development and should not be used at this time.

3. Write your own query, test in the SQL Management Studio, and copy that query in **Membership SQL Query** (4).

Sample Queries that can be used:

- i. To list the ConfigMgr Client machines that are not on the correct client version. Below query lists the Adaptiva client id's that are not on ConfigMgr Client version 5.00.8577.1005 and with version Null

```
Select adaptivaclientid
from a_Adaptivaclientdata a
inner join on v_r_system b on a.machinename=b.name0
where (b.client_Version0 != '5.00.8577.1005' OR
b.client_Version0 is NULL)
```

- ii. To list the Adaptiva clients that are not on the current installed version.

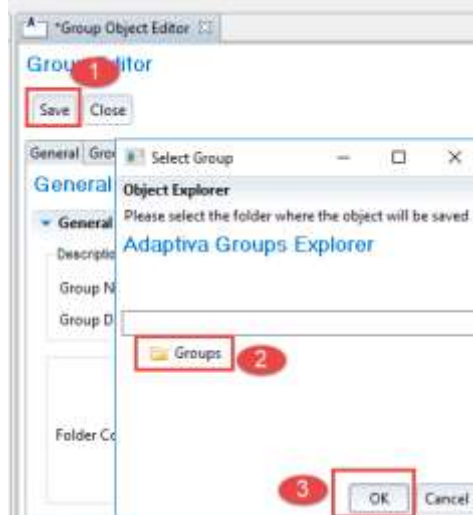
```
Select adaptivaclientid
from a_Adaptivaclientdata
where adaptivaclientversion != '5.5.669.0'
```

- iii. To list the Adaptiva client IDs if we want to license a particular set of machines based on AD Site.

```
Select adaptivaclientid
from a_Adaptivaclientdata
where ADSITE like '%adaptiva%'
```

Please observe the queries that we use all return *adaptivaclientid*, the reason for that is we selected the **Scope Type** to be **Client Id**.

4. Click **OK** (5)
5. Now add a **Schedule** as shown previously and click on **Save** (1). After clicking on save you will get **Adaptiva Groups Explorer** window, now select **Groups** (2), and click **OK** (3).



# (Optional) Post Installation Activities

Please review the links below for additional activities that may be useful

Description	Knowledgebase Article
Speed up content and policy delivery by enabling Large UDP messaging. If you have upgraded from versions prior to 7.0.854 this is <b>STRONGLY</b> recommended. Large messaging is enabled by default for all builds from 854 and later	<a href="#">How-to: Enable UDP v2 Large Messaging – Adaptiva Support Portal</a>
Operating System Deployments: After installing the Adaptiva client, wait for the license before continuing the task sequence	<a href="#">Task Sequence - Wait for Adaptiva Client to get an ID – Adaptiva Support Portal</a>
Operating System Deployments: Getting the boot image faster by increasing the block size.	<a href="#">How-To: Set the Boot Image TFTP Block Size – Adaptiva Support Portal</a>
Operating System Deployments: Using the PXE Approval Workflow to ensure the correct boot image is used.	<a href="#">How-To: Define a Preferred Boot Image for PXE – Adaptiva Support Portal</a>
Content Push Policy optimization techniques	<a href="#">How-To: Optimize "All Clients" targeted IntelliStage Content Push Policies – Adaptiva Support Portal</a>
Perform administrative functions and tests on remote machines. For example, <b>Get logs, Check PXE</b> , Get the RVP, Restart the Client, etc.	<a href="#">Administration: Adaptiva Administration Tool (AAT) – Adaptiva Support Portal</a>
Clients not communicating with the server? Use the UDPPortChecker tool to determine which port or ports is blocked.	<a href="#">How-To: Check that the required ports for Adaptiva are open? – Adaptiva Support Portal</a>
Create a Custom Security Role	<a href="#">How-To: Create a Custom Security Role with Limited Set of Perspectives – Adaptiva Support Portal</a>
Viewing Adaptiva Status Messages in the ConfigMgr console	<a href="#">How-To: View Adaptiva Status Message Descriptions – Adaptiva Support Portal</a>

# Cache Migration Tool

## Overview

The Adaptiva OneSite Cache Migration Tool is designed to convert and copy content that is published in Adaptiva OneSite but cached in non-Adaptiva form (such as a ConfigMgr Distribution Point), into the local Adaptiva Client cache. This alleviates the need to download content a second time for use in the Adaptiva Peer-to-Peer network.

The Cache Migration Tool can convert and copy content from the following locations:

- ConfigMgr 2012/Current Branch distribution point
- 1E Nomad™ client cache
- ConfigMgr client cache
- Altiris™ Notification Servers, Altiris™ Package Servers, Altiris™ Clients

## How It Works

When the Cache Migration Tool is executed on an Adaptiva client, the following steps are performed:

- The client java component (JAR file) is extracted and put into the **external** folder under the Adaptiva Client installation folder.
- The Adaptiva Client service is restarted.
- For each item in the cache a message is sent to the Adaptiva Server to see if that package is published in Adaptiva OneSite.
- The server responds with a message to either Convert (if the package is published in Adaptiva) or Abort. If the response is Convert, the content is converted and stored in the Adaptiva Client cache of the machine it is run on. If the response is Abort, the log file can be examined for the reason the content could not be migrated.
- After all packages have been checked, the client JAR file is removed from the **external** folder.
- The Adaptiva Client service is restarted.
- Approximately 1 minute after the client has restarted, the OneSitePreCacheClient component lets the Adaptiva Server know that the newly converted content is available from this client in the Adaptiva P2P network.

## Prerequisites

- The Adaptiva Client must be installed on the machine where the Cache Migration Tool is executed, and enough disk space should be available to accommodate the content.
- The Cache Migration Tool should be executed with administrative rights.

## Tool Location

The Adaptiva Cache Migration Tool is included in the Adaptiva OneSite download source, in the **\Tools** folder, and is named **CacheMigrationTool.exe**.

## Using the Cache Migration Tool

The tool can be distributed via a ConfigMgr package with an associated program or executed via command line.

CacheMigrationTool.exe -<source> [-parameter1] [-parameter2]

## Command Line Parameters

Parameter	Description
<b>Content Source</b>	
-dp2012	Used to migrate content from a Distribution Point where Adaptiva is connected to an ConfigMgr 2012/Current Branch site.
-nomad	Used to migrate content from a 1E Nomad™ client cache.
-sccmclient	Used to migrate content from a ConfigMgr client cache.
-altirispackageserver	Used to migrate content from an Altiris™ package server.
-altirisclient	Used to migrate content from an Altiris™ client.
<b>Additional Parameters</b>	
-p2p <#>	Used to replicate migrated content to other peers in the local office. The # value represents the number of clients where the content should be replicated. This parameter requires that a source parameter be used.  Ex: CacheMigrationTool.exe -dp2012 -p2p 3
-delete	Used to delete migrated content from the source cache.  <b>NOTE: This option can only be used with the -nomad, -sccmclient, -altirispackageserver, -altirisclient parameters.</b>  Ex: CacheMigrationTool.exe -sccmclient -delete
-regenerate	Used to regenerate previously migrated content from all contents found and deletes an earlier generated copy. This parameter requires that a source parameter be used.  <b>NOTE: This option is generally not required and solves a specified case for fixing contents generated by the Cache Migration Tool prior to version 4.5.632.</b>  Ex: CacheMigrationTool.exe -dp2007 -regenerate
-revalidate	Used to validate all existing content files in the Adaptiva Client cache. Once executed, the tool will verify the hash is correct for all content and remove any invalid or partial content.  <b>NOTE: This option can be run independently and does not require that a source parameter be used.</b>  Ex: CacheMigrationTool.exe -revalidate

## Migrating from an Altiris™ Notification Server

Cache migration is now supported from Altiris™ Notification Servers, Altiris™ Package Servers, and Altiris™ Clients.



Contact Adaptiva support (support@adaptiva.com) to obtain an OBEX file that contains an automated workflow which will import all Altiris™ Software Releases into ConfigMgr Applications, and automatically publish them in Adaptiva.

See the table above for the command line parameters used to migrate content from Altiris™ Package Servers and Altiris™ clients.

## Logging

When the cache migration executes on a client, the following logs document the process:

Log File	Location	Purpose
<b>Client</b>		
CacheMigrationTool.log	<AdaptivaClientInstallPath>\Logs	Documents the execution activity of the Cache Migration Tool.
CacheMigrationClient.log	<AdaptivaClientInstallPath>\Logs\componentlogs	Tracks the activity of the Cache Migration Tool as it works with the local content.
<b>Server</b>		
Adaptiva.log	<AdaptivaServerInstallPath>\Logs\	Displays the communication from the client running the Cache Migration Tool as well as the validation of each item being migrated.

# Appendix A: Adaptiva Logs

Xxx

## Server Logs

Log File Name	Log File Description
<b>Default Folder: &lt;drive&gt;\Program Files\Adaptiva\AdaptivaServer\logs</b>	
adaptiva.err	Records any errors during the running of the AdaptivaClient service
adaptiva.log	Records almost all data regarding AdaptivaClient service
AdaptivaNativeUtils.log	AdaptivaServer to windows access logging
AdaptivaServerNativeUtils.log	AdaptivaServer to windows access logging
AdaptivaService.log	AdaptivaServer service start/stop logging
AdaptiveProtocolTransport.log	AdaptivaServer data transfers using Adaptive Protocol
messagingMonitor.log	Logs all RVP advertisements
NtlmAuth.log	Logs communications using NTLM
sqlMonitor.log	Monitors the size of specific tables
VCDiff.log	Use of Visual C++
<b>Default Folder: &lt;drive&gt;\Program Files\Adaptiva\AdaptivaServer\logs\ComponentLogs</b>	
BlobServer.log	Logs the creation of blobs for Office 365 update content
ByteLevelP2PPublisher.log	Logs the Bob ranges when using Byte Level publishing for Office 365 update content
RelayDetailed.log	Detailed logging for Relay connectivity and Security protocols on HTTP. RelayDetailed are the previous HttpTransport, Security, and Relay logs combined into one file. This includes detailed error messages with stack traces as well as verbose logging for tracing requests end to end.
RelaySimple.log	Provides an overview of handshakes and HTTP messaging from a more conceptual standpoint. Instead of logging through the train of classes and method executions involved in the process, it is intended simply to say the handshake completed successfully. It can be used to confirm that the system is working as intended, or that something broke and the detailed logs may need digging through.
Utils.log	Logs communication to ConfigMgr Site Control File

## Client Logs

Log File Name	Log File Description
<b>Default Folder: C:\Program Files (x86)\Adaptiva\AdaptivaClient\logs</b>	
adaptiva.err	Records any errors during the running of the AdaptivaClient service
adaptiva.log	Records almost all data regarding AdaptivaClient service
AdaptivaNativeUtils.log	AdaptivaClient to windows access logging
AdaptivaRemoteInstallLog.log	Intune application content download and install logs
AdaptivaService.log	AdaptivaClient service start/stop logging
AdaptivaServiceRestart.log	AdaptivaServiceRestart.exe logging, used mostly by AdaptivaClient Setup during install or upgrades

AdaptiveProtocolTransport.log	AdaptivaClient data transfers using Adaptive Protocol
jvmhook.log	For developer use only, this log will only be used by Adaptiva Support
messagingMonitor.log	Logs all RVP advertisements
OneSiteProvider.log	Logs activity of the ConfigMgr Client and the Adaptiva Client ACP and vice-versa for 32-bit OSes
OneSiteProvider64.log	Logs activity of the ConfigMgr Client and the Adaptiva Client ACP and vice-versa for 64-bit OSes
sqlMonitor.log	Call to SQL logging
<b>Default Folder: C:\Program Files (x86)\Adaptiva\AdaptivaClient\logs\componentLogs</b>	
ActionExec.log	Logs activity for action executions
ARPDDiscovery.log	Not used
BlobSystem.log	Logs for internal system used for blob downloads
BulkMessaging.log	Logs activity related to extremely fast new P2P messaging system
CacheMigrationClient.log	Records activity of the cache migration tool
ChildJvm.log	Logs activity for child VMs created for scan executions
CHSClient.log	Records activity of the Client health modules
ClientInfo.log	Client registration with server and Client IP address in use for communication logging
Configuration.log	Client system configurations changes logging
ContentCache.log	AdaptivaClient cache state logging
ContentDeleter.log	Logs activities of Adaptiva Client content deletion
ContentDownload.log	Logs all content downloads
ContentLockManager.log	Logs activity related to P2P locking done during content downloads
ContentPush.log	Content pre-staging/push logging
ContentUnpack.log	Content unpacking logging
ContentUpload.log	Content uploads from client to client
DataFlow.log	Datapipe logs
EVM.log	Evolve VM generic logs
FileDeletion.log	Logs all Adaptiva file deletion requests (non-content)
GPClient.log	Green Planet client logging
HttpTransport.log	Client HTTP transport logs. HttpTransport is used when client binds to Adaptiva Server URL
InternetPeer.log	Contains details about communication for an internet client. It can be a pure internet or split internet client. This contains details about behaviors and protocols for internet client.
Inventory.log	AdaptivaClient inventory collection and reporting logging
LargeMsgTransport.log	Logs related to AdaptiveTransport for messages
License.log	Records the status of the client license
Locking.log	General concurrent locking logs
MemoryCache.log	Logs related to CachedHashMap
MemoryManager.log	Current client memory state and changes logging
Messaging.log	Messaging ports start and stop logging
NetworkLocation.log	Contains details about current network location for this client. It can be one of these (ON_PREMISES,ON_PREMISES_SPLIT,INTERNET,FORCED_TUNNEL_VPN,SPLIT_TUNNEL_VPN,UNKNOWN)



ObjectDeployment.log	Adaptiva object deployment system logs
OEMManager.log	Logs related to 3rdParty OEM integrations (e.g. VMware)
OfficeLockManager.log	Logs related to Office level locking used in advanced functions. (e.g. in IntelliStage)
OneSiteDownload.log	ConfigMgr client ACP invocation and downloads logging
OneSitePreCache.log	Content pre-caching logging
P2PDiscovery.log	Logs related to P2P discovery
P2PStore.log	Logs related to client's local P2P store
PolicyManager.log	Policy operations and processing logging
PXE.log	Records PXE service availability and communication
RegIPC.log	Logs activity related to IPC using windows registry
RelayDetailed.log	Detailed logging for Relay connectivity and Security protocols on HTTP. RelayDetailed are the previous HttpTransport, Security, and Relay logs combined into one file. This includes detailed error messages with stack traces as well as verbose logging for tracing requests end to end.
RelaySimple.log	Provides an overview of handshakes and HTTP messaging from a more conceptual standpoint. Instead of logging through the train of classes and method executions involved in the process, it is intended simply to say the handshake completed successfully. It can be used to confirm that the system is working as intended, or that something broke and the detailed logs may need digging through.
RemediationExec.log	Logs related to execution of remediations on the client
RemoteWorkflowExecution.log	Logging for remote workflow execution using tool foundry
RVPOSDSupporter.log	Records RVP content requests for clients executing OSD
RVPState.log	Displays RVP state for the local subnet
SCCMClient.log	Records interactions with the local ConfigMgr client
SCCMDataUpload.log	ConfigMgr client data upload management logging
SCCMPolicyPolling.log	ConfigMgr client policy polling management logging
Scheduler.log	AdaptivaClient scheduler
Security.log	Records the updating of ACLs
SentRecvMsg.log	Logs all messaging between client-server and client-client
ServerLocator.log	Logs activity related to server binding, connectivity
SmallMsgTransport.log	Logs related to small UDP messages
SQLAccess.log	Logs local client database activity
Startup.log	Startup and shutdown logging for AdaptivaClient
TFTP.log	Records TFTP communications for boot image file delivery during PXE boot
Utils.log	Generic utility logs
VirtualSMP.log	Logs virtual state migration point activities
WiFi.log	WiFi office transition logging
WOL.log	Logs related to any Wake On LAN activity
WorkflowSystem.log	Any workflow related logs
<b>Default Folder: C:\Program Files (x86)\Adaptiva\AdaptivaClient\logs\workflowlogs</b>	
WorkflowName.log	All Client workflows execution logging

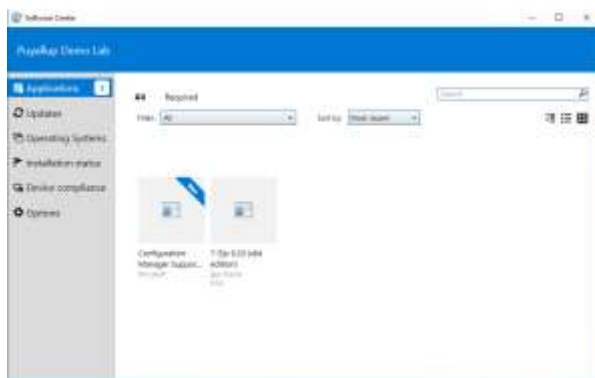
# Appendix B: Installing the App – What Does the User See?

## ConfigMgr

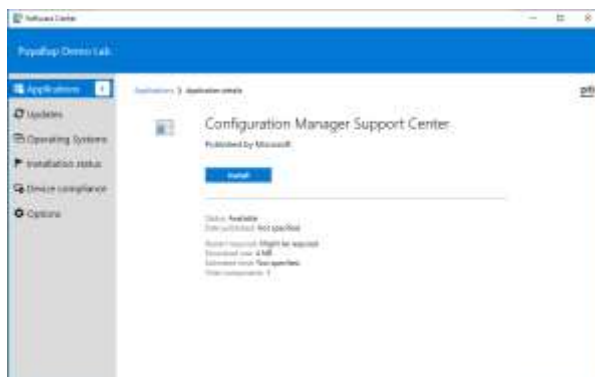
ConfigMgr can deploy several different types of content. Packages, Applications, Software Updates, and Task Sequences which can include all of those plus driver packages and OS images or upgrades. Adaptiva can download all these content types. How ConfigMgr determines if a download is required is different for Applications and Software Updates then for the rest.

Content must be deployed (or advertised) to a client device by that device being in a collection. When the collection membership changes, Adaptiva, if Policy Bandwidth management has been enabled, will notify the clients they need to request a machine policy refresh. Otherwise, clients will check in at their policy polling interval (default is every 60 minutes).

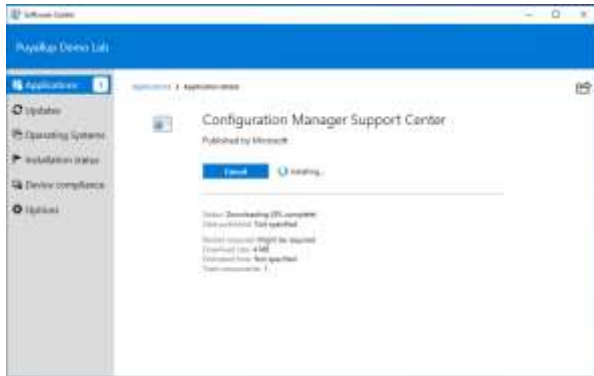
If the deployment was set to Required, then the client will be notified to begin download immediately after the policy becomes available. If the deployment was set to Available, then the end-user will be able to initiate the installation at their leisure by selecting the app in Software Center.



Selecting the app to install will display additional information



Click on **Install** to initiate the download and installation of the application



For applications, they have a detection method to determine if the application is already installed. That will be run first. If it is found that the application is not installed, only then will the content be downloaded. For software updates, they will only show up in Software Center if they are applicable to be installed on the machine. For packages and task sequences, they will display in Software Center if the computer is in the collection that has the package or TS deployed.

Let's look at the logs that are used during this process.

## Tracing the installation in the logs

It is important to understand what is happening in the logs if there is a problem during deployment so that it can be traced back to find a solution.

The following documentation can be used for additional information on the ConfigMgr processes:

Applications: <https://docs.microsoft.com/en-us/mem/configmgr/apps/understand/app-deployment-technical-reference>

Software Updates: <https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/troubleshoot-software-update-deployments>

When troubleshooting an application or package deployment, the following information is helpful:

Package ID: When deploying an application, the Package ID can be obtained from the Monitoring workspace, Distribution Status, Content Status

For Applications, also obtain:

Content ID: Look in the Deployment Types tab of the Application

For this example:

Package ID: PUY0000E

Content ID: Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2

1. For application deployments, start with AppDiscovery.log in C:\Windows\CCM\Logs to confirm the detected application needs to be downloaded. Search for the Content ID. The Content ID is highlighted in **yellow**. If the application is already installed, then nothing will be downloaded.

```
Entering ExecQueryAsync for query "select * from CCM_AppDeliveryType where
(AppDeliveryTypeId = "ScopeId_D0D32342-8317-43E5-A7F0-
659C31121CBF/DeploymentType_1d74b65c-bba1-4035-9e08-fddf80efc75d" AND Revision = 2)"
Performing detection of app deployment type Configuration Manager Support Center -
Windows Installer (*.msi file) (ScopeId_D0D32342-8317-43E5-A7F0-
659C31121CBF/DeploymentType_1d74b65c-bba1-4035-9e08-fddf80efc75d, revision 2) for system.
+++ MSI application not discovered [MSI Product Code: {79C523EC-042E-420F-83FB-
4CDB6B85CE15}, MSI Product version: ]
+++ Did not detect app deployment type Configuration Manager Support Center - Windows
Installer (*.msi file) (ScopeId_D0D32342-8317-43E5-A7F0-
659C31121CBF/DeploymentType_1d74b65c-bba1-4035-9e08-fddf80efc75d, revision 2) for system.
```

ActionType - **Install will use Content Id:** Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2 + Content Version: 1 for AppDT "Configuration Manager Support Center - Windows Installer (\*.msi file)" [ScopeId\_D0D32342-8317-43E5-A7F0-659C31121CBF/DeploymentType\_1d74b65c-bba1-4035-9e08-fddf80efc75d], Revision - 2

For Packages, open ExecMgr.log and search for the Package ID

Requesting content from CAS for package PUY00019 version 2

Successfully created a content request handle {C546A5B5-CC0F-4C4D-8AD4-4EEC5F72068C} for the package PUY00019 version 2

2. Open ContentTransferManager.log. For each content download request, a unique Job ID is assigned by the Content Transfer Manager (CTM). Search for the Content ID (for applications) or Package ID (for packages). The CTM Job ID is highlighted in blue. CTM will request the content location from CAS. If the CAS returns a Distribution Point, the download request will go forward. If no DP is returned, the CTM job will be suspended.

Persisted locations for CTM job {82B363D5-3655-4A72-B2A1-4066BAB0EEFD}:

(BOUNDARYGROUP) http://dpname.domain.com/SMS\_DP\_SMSPKG\$/Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2.1

(BOUNDARYGROUP) http://dpname.domain.com/NOCERT\_SMS\_DP\_SMSPKG\$/Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2.1 (BOUNDARYGROUP)

https://Dpname.domain.com/CMTOKENAUTH\_SMS\_DP\_SMSPKG\$/Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2.1

3. CTM then looks for registered download providers. If OneSite is registered, there will be a reference to AdaptivaOneSite

CCTMJob::TryNextProvider - Modifying provider to 'AdaptivaOneSite' with CLSID '{6822CB84-DBAF-4431-8EDC-42C0BCFE7E3F}'

Calling ACP with ICcmAlternateDownloadProvider interface.

4. The request now goes to Adaptiva. Those logs can be found in C:\Program Files (x86)\Adaptiva\AdaptivaClient\Logs. The first Adaptiva log will be the OneSiteProvider.log (OneSiteProvider64.log on 64-bit machines). Search for the Content ID/Package ID or the CTM Job ID. If the Content ID/Package ID, listed as Content id, and CTM Job ID, listed as Notify data are present in OneSiteProvider.log, it means Adaptiva OneSite has successfully received the Content download request from the ConfigMgr client. Also, notice the Local path. This will be where the unpacked contents will be copied to.

DownloadContent(): 794: Line: 0: Entry OneSiteProvider.cpp

DownloadContent(): 794: Line: 28: Content id: Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2 OneSiteProvider.cpp

DownloadContent(): 794: Line: 44: Remote path:

http://dpname.domain.com/SMS\_DP\_SMSPKG\$/Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2.1 OneSiteProvider.cpp

DownloadContent(): 794: Line: 52: Local path: C:\WINDOWS\ccmcache\d\y OneSiteProvider.cpp

DownloadContent(): 794: Line: 68: Notify data: {82B363D5-3655-4A72-B2A1-4066BAB0EEFD} OneSiteProvider.cpp

5. Back in the ContentTransferManager.log, CTM will then initiate the content download request to the Data Transfer Service (DTS), which will be handed off to Adaptiva. Copy the DTS Job ID, in olive

CTM job {82B363D5-3655-4A72-B2A1-4066BAB0EEFD} (corresponding DTS job {6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}) started download from

'http://dpname.domain.com/SMS\_DP\_SMSPKG\$/Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2.1' for full content download.

6. Next, the request can be found in OneSiteDownload.log in the componentlogs folder. Search this log for the DTS Job ID

INFO - DownloadContent is received in OneSiteMessage for jobID [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}] - OneSiteContentDownloader - TID=128, ReceivingTask: Sender Id = [/127.0.0.1]

INFO - No OneSiteJob is found for JobID [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}] - OneSiteContentDownloader - TID=128, ReceivingTask: Sender Id = [/127.0.0.1]

7. Then, Notice that Adaptiva has created a New Request to download the content. We can also see the Package ID being referenced. This is highlighted in gray with the full Adaptiva Content ID

INFO - OneSiteJob's status is updated to STATUS\_NEW\_REQUEST for jobID [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], SccmContentID [Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2],

SccmContentVersion [1] - OneSiteContentDownloader - TID=128, ReceivingTask: Sender Id = [/127.0.0.1]

INFO - Created OneSiteJob for JobID [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}] from OneSiteMessage [OneSiteJob [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], NotificationData [{82B363D5-3655-4A72-B2A1-4066BAB0EEFD}] status [0], SccmContentID [Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2], SccmContentVersion [1], LocalPath [C:\WINDOWS\ccmcache\dy], RemotePath [http://dpname.domain.com/SMS\_DP\_SMSPKG\$/Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2.1], NotifyEndPoint [direct:CTMDTSReply], SccmTimedOut [2419200], SccmChunkSize(bytes) [52224], SccmFlags [4195590], SccmProviderData [AdaptivaGlobalSettings], SccmPackageData [<Data>APP</Data>] and status [STATUS\_NEW\_REQUEST] and SccmNotifyErrorOccurred [false] - OneSiteContentDownloader - TID=128, ReceivingTask: Sender Id = [/127.0.0.1]

INFO - Successfully Sent OneSiteContentRequest message for JobID [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}] and AdaptivaContentID [App\$Content\_efb1c4db\_01fd\_4cc3\_972e\_62f62bd652a2] and SccmContentRequestedVersion [1] - OneSiteContentDownloader - TID=128, ReceivingTask: Sender Id = [/127.0.0.1]

INFO - Notify Progress to SCCM Client for JobID [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}] SCCM ContentId [Content\_efb1c4db-01fd-4cc3-972e-62f62bd652a2], SCCM Content Version [1], NotificationData [{82B363D5-3655-4A72-B2A1-4066BAB0EEFD}], TotalBytes [0], BytesTransferred [0], TotalFiles [0], FilesTransferred [0] - OneSiteContentDownloader - TID=128, ReceivingTask: Sender Id = [/127.0.0.1]

INFO - Using AdaptivaContentID: App\$PUY0000E\$16779293, for JobID: {6117DCB7-FF18-CB4B-0DCD-A1743F0EA112} - OneSiteContentDownloader - TID=131, ConsumerTask: Sender Id = [0], Retry Level : 0

8. Open ContentDownload.log and search for the DTS Job ID. The DTS Job ID is used to create the Session ID. Also, notice the Adaptiva Content ID.

INFO - Invoking downloadContent for session : OneSite\${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112} and contents : [App\$PUY0000E\$16779293] - ContentDownloader - TID=131, ConsumerTask: Sender Id = [0], Retry Level : 0

INFO - Write locks acquired for for session : OneSite\${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112} and contents : [App\$PUY0000E\$16779293] - ContentDownloader - TID=131, ConsumerTask: Sender Id = [0], Retry Level : 0

INFO - Cleared lan/wan cost content session: OneSite\${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112} - ContentDownloader - TID=131, ConsumerTask: Sender Id = [0], Retry Level : 0

INFO - Added content name mapping: Adaptiva content for contentId [App\$PUY0000E\$16779293], ID: App\$PUY0000E\$16779293 - ContentDownloader - TID=131, ConsumerTask: Sender Id = [0], Retry Level : 0

9. The download starts. Notice the Network Location Type.

INFO - **Started download** for : App\$PUY0000E\$16779293 - ContentDownloader - TID=131, ConsumerTask: Sender Id = [0], Retry Level : 0

INFO - Write locks released for for session : OneSite\${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112} and contents : [App\$PUY0000E\$16779293] - ContentDownloader - TID=131, ConsumerTask: Sender Id = [0], Retry Level : 0

INFO - ContentPublicationData: [ Content Version: 5, isExpedited: false, isEncrypted: false, isCompressed: true, SizeOfLatestVersion: 4883879, SizeOfOldVersion: 0, SizeOfDiff: 0, SizeOfUnpackedVersion: 5230592, TotalUnpackedFilesCount: 1, RepublishedContent: true, publishedUnchanged: false, actualFileName: null, isLocalContent: false, Nh: false], GlobalContentVersion: 1], ContentFriendlyName: Adaptiva content for contentId [App\$PUY0000E\$16779293]], ContentTypeFlags: 8]], ContentDownloadSettings [120;false;false;false;com.adaptiva.transport.BGTransport;34750;com.adaptiva.transport.FGTransport;34760;360000;360000;2419200000;false] - StateTransitionProtocol - TID=133, STP-SessionHandle=[OneSite\${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], Content Id=[App\$PUY0000E\$16779293]

INFO - **Current network location type: [ON PREMISES]** - StateTransitionProtocol - TID=133, STP-SessionHandle=[OneSite\${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], Content Id=[App\$PUY0000E\$16779293]

```
INFO - Download preference: Download preferences: LocalOffice: true, Internet peers:
false, CDN: false, ParentOfficeHierarchy: true, for LocationType: ON PREMISES -
ContentSystemUtils - TID=133, STP-SessionHandle=[OneSite${6117DCB7-FF18-CB4B-0DCD-
A1743F0EA112}], Content Id=[App$PUY0000E$16779293]
```

10. Open the log SentRecvMsg.log, the normal election process is held, does anyone have this content? Highlight or filter the Adaptiva Content ID

```
INFO - Attempting to send (WiFi): Receiver ID: -1, Receiver IP: null, MsgLen: 643,
Correlation ID = 604182 port: 34329, transport:
com.adaptiva.transport.WiFiUDPTransport@5d8af3, Message :Name of the message:
P2PDiscoveryRequest, Sender ID: 12, Receiver ID: 1, Queue ID: 1, CORRELATION ID: 0,
ORIGINAL CORRELATION ID: 0, ORIGINAL RECEIVER ID: 1, REPLY TO: 1, REPLY TO IP: null, IS
REPLY: false, PREF TRANSPORT: 0, RECV TRANSPORT: 2, Attribute count: 23Attribute names
and their values: Name: RequestID ,Value: 51539607553; Name: NoOfConditions ,Value: 4;
Name: FieldID0 ,Value: 1; Name: Operator0 ,Value: 1; Name: Value0 ,Value: Content; Name:
CaseInsensitive0 ,Value: 1; Name: FieldID1 ,Value: 2; Name: Operator1 ,Value: 1; Name:
Value1 ,Value: App$PUY0000E$16779293; Name: CaseInsensitivel ,Value: 1; Name: FieldID2
,Value: 3; Name: Operator2 ,Value: 1; Name: Value2 ,Value: 5; Name: CaseInsensitive2
,Value: 1; Name: FieldID3 ,Value: 4; Name: Operator3 ,Value: 4; Name: Value3 ,Value: 0;
Name: CaseInsensitive3 ,Value: 1; Name: MaxResponses ,Value: 4; Name: SpreadDuration
,Value: 4000; Name: NewVersion ,Value: ; Name: _SERVER_GUID_ ,Value: 8efe3c8a-9aac-11ea-
97f0-00155d0a1e8a; Name: _WiFi_ ,Value: ; - SendingThread - TID=133, SendingThread:
[Receiver Id= -1]
```

**NOTE: This is in a WiFi-configured Location. In a wired/Default-configured Location, it would read:**

```
INFO - Attempting to send (Broadcast): Receiver ID: -1, Receiver IP:
null,...
```

11. Now back in ContentDownload, filter on **Content download progress**. Notice where it is downloading from. It might be across the LAN or across the WAN (filter on AN\$), it might be across the INternet or from the CDN (filter on INT\$ or CDN\$).

```
INFO - Content download progress percentage notification. ContentId
:App$PUY0000E$16779293, Content version: 5, Current download type: 0, percentage: 0,
download source: WAN$10.151.2.51, Lan download(in bytes): 0, Wan download(in bytes): 1024
- StateTransitionProtocol - TID=33, Polling Thread
```

```
INFO - Content download progress percentage notification. ContentId
:App$PUY0000E$16779293, Content version: 5, Current download type: 0, percentage: 100,
download source: WAN$10.151.2.51, Lan download(in bytes): 0, Wan download(in bytes):
4883879 - StateTransitionProtocol - TID=33, Polling Thread
```

12. Finally, ContentDownload marks the download as complete and releases the RVP locks

```
INFO - Content Download Completed called for Content Id: App$PUY0000E$16779293.. Content
Version : 5..Status Code : 0.. String message :null - ContentDownloader - TID=133, STP-
SessionHandle=[OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], Content
Id=[App$PUY0000E$16779293]
```

```
INFO - release/cancel locks in case they were held and not released - ContentDownloader -
TID=133, STP-SessionHandle=[OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], Content
Id=[App$PUY0000E$16779293]
```

13. The downloaded content is checked against its hash which it gets from the Adaptiva server.

```
INFO - Verifying content : C:\AdaptivaCache\App$PUY0000E$16779293.5.content, Content Id :
App$PUY0000E$16779293, Content version : 5, Diff : false - ContentDownloader - TID=133,
STP-SessionHandle=[OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], Content
Id=[App$PUY0000E$16779293]
```

```
INFO - Computing hash for file: C:\AdaptivaCache\App$PUY0000E$16779293.5.content -
ContentSystemUtils - TID=133, STP-SessionHandle=[OneSite${6117DCB7-FF18-CB4B-0DCD-
A1743F0EA112}], Content Id=[App$PUY0000E$16779293]
```

```
INFO - Verified secure hash for content : App$PUY0000E$16779293 - ContentDownloader -
TID=133, STP-SessionHandle=[OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], Content
Id=[App$PUY0000E$16779293]
```

14. It then unpacks the content to the ccmcache folder that was specified in OneSiteProvider[64].

```
INFO - Unpacking content for session : OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112} -
ContentDownloader - TID=133, STP-SessionHandle=[OneSite${6117DCB7-FF18-CB4B-0DCD-
A1743F0EA112}], Content Id=[App$PUY0000E$16779293]
```

```
INFO - Content unpacking successful for session : OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112} - ContentDownloader - TID=133, STP-SessionHandle=[OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], Content Id=[App$PUY0000E$16779293]
```

```
INFO - set LastUnpackedFolderPath in contentState to: C:\WINDOWS\ccmcache\dy\, taken from session : OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112} - ContentDownloader - TID=133, STP-SessionHandle=[OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], Content Id=[App$PUY0000E$16779293]
```

- Then the completed download request notification is shown. This status is then sent to the OneSiteDownload.log

```
INFO - Content download completed for content ID : App$PUY0000E$16779293, for session handle : OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112} - ContentDownloader - TID=133, STP-SessionHandle=[OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}], Content Id=[App$PUY0000E$16779293]
```

```
INFO - Sending notification: NotificationEvent ::
<NotificationType:ContentDownloadProgress><NotificationQualifier:OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}><Value:[Ljava.lang.String;@1b940bc - ContentSystemNotificationSender - TID=8, AdaptivaTimer - SystemLifetimeManager. ExecutingTask-ContentSystemNotificationSender$ContentNotificationSenderTask
```

- And back in OneSiteDownload.log we see the receipt of the notification and where the content was unpacked to and then sending the notification back to CTM:

```
INFO - ContentDownloadCompleted notification is received by OneSiteContentDownloader for SessionId [OneSite${6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}] - OneSiteContentDownloader - TID=8, AdaptivaTimer - SystemLifetimeManager. ExecutingTask-ContentSystemNotificationSender$ContentNotificationSenderTask
```

```
INFO - Content download Result status is [0] and statusMessage [c:\windows\ccmcache\dy ] for jobID [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}] - OneSiteContentDownloader - TID=8, AdaptivaTimer - SystemLifetimeManager. ExecutingTask-ContentSystemNotificationSender$ContentNotificationSenderTask
```

```
INFO - Content is successfully downloaded for SCCM ContentID [Content_efb1c4db-01fd-4cc3-972e-62f62bd652a2], SCCM Content Version [1] for JobID [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}] - OneSiteContentDownloader - TID=8, AdaptivaTimer - SystemLifetimeManager. ExecutingTask-ContentSystemNotificationSender$ContentNotificationSenderTask
```

```
INFO - Notify Success to SCCM Client for JobID [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}] and NotificationData [{82B363D5-3655-4A72-B2A1-4066BAB0EEFD}], SCCM ContentId [Content_efb1c4db-01fd-4cc3-972e-62f62bd652a2], SCCM Content Version [1] - OneSiteContentDownloader - TID=8, AdaptivaTimer - SystemLifetimeManager. ExecutingTask-ContentSystemNotificationSender$ContentNotificationSenderTask
```

```
INFO - OneSiteJob's status is updated from [STATUS_CONTENT_DOWNLOAD_STARTED] to STATUS_DOWNLOAD_SUCCESSFULLY_COMPLETED for jobID [{6117DCB7-FF18-CB4B-0DCD-A1743F0EA112}] SccmContentID [Content_efb1c4db-01fd-4cc3-972e-62f62bd652a2], SccmContentVersion [1] - OneSiteContentDownloader - TID=8, AdaptivaTimer - SystemLifetimeManager. ExecutingTask-ContentSystemNotificationSender$ContentNotificationSenderTask
```

- Back in ContentTransferManager.log, ConfigMgr receives the download status:

```
CTM job {82B363D5-3655-4A72-B2A1-4066BAB0EEFD} successfully processed download completion.
```

- ConfigMgr will check the content against its hash. This can be seen in the CAS.log

```
Download completed for content Content_efb1c4db-01fd-4cc3-972e-62f62bd652a2.1 under context System
Computed hash: 0F4B041F96809359ABEA2F13196A84A8B99D3EC31C42E5C1C92E91DB57A0D465
Hash verification succeeded for content Content_efb1c4db-01fd-4cc3-972e-62f62bd652a2.1 downloaded under context System
```

- For applications, in AppEnforce.log, the installation command can then be seen and the exit code result from the installation. For this, the Deployment Type name is required.

```
+++ Starting Install enforcement for App DT "Configuration Manager Support Center - Windows Installer (*.msi file)" ApplicationDeliveryType - ScopeId_DOD32342-8317-43E5-A7F0-659C31121CBF/DeploymentType_1d74b65c-bba1-4035-9e08-fddf80efc75d, Revision - 2, ContentPath - C:\WINDOWS\ccmcache\dy, Execution Context - System
```

```

Performing detection of app deployment type Configuration Manager Support Center -
Windows Installer (*.msi file) (ScopeId_D0D32342-8317-43E5-A7F0-
659C31121CBF/DeploymentType_1d74b65c-bba1-4035-9e08-fddf80efc75d, revision 2) for system.
+++ MSI application not discovered [MSI Product Code: {79C523EC-042E-420F-83FB-
4CDB6B85CE15}, MSI Product version: ]
App enforcement environment:
Context: Machine
Command line: msiexec /i "supportcenterinstaller.msi" /qn
Content path: C:\WINDOWS\ccmcache\dy Working directory:
Prepared working directory: C:\WINDOWS\ccmcache\dy
Found executable file msiexec with complete path C:\WINDOWS\system32\msiexec.exe
Prepared command line: "C:\WINDOWS\system32\msiexec.exe" /i
"supportcenterinstaller.msi" /qn /qn
Valid MSI Package path = C:\WINDOWS\ccmcache\dy\supportcenterinstaller.msi
Process 7396 terminated with exitcode: 0

```

For packages, that will be in ExecMgr.log, continue to use the Package ID

```

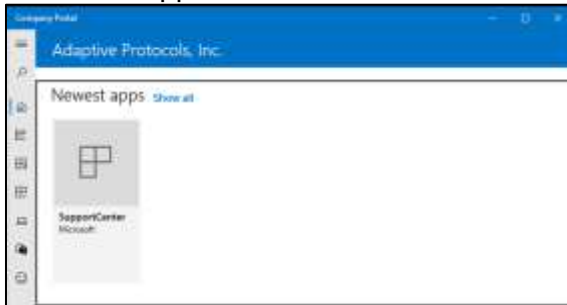
Execution Request for advert package PUY00019 program Install Per System state change
from Ready to NotifyExecution
Successfully selected content location C:\WINDOWS\ccmcache\e7
Executing program as a script
Successfully prepared command line "C:\WINDOWS\ccmcache\e7\ChromeSetup.exe"
Command line = "C:\WINDOWS\ccmcache\e7\ChromeSetup.exe", Working Directory =
C:\WINDOWS\ccmcache\e7\
Running "C:\WINDOWS\ccmcache\e7\ChromeSetup.exe" with 32bitLauncher
Created Process for the passed command line
Raised Program Started Event for Ad:PUY20003, Package:PUY00019, Program: Install Per
System
Program exit code 0

```

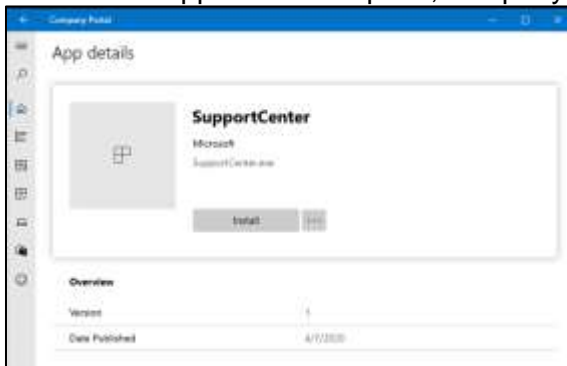
## Intune

When the app created is targeted as Available to a group of user accounts, the Company Portal is then used to request the installation of the app.

1. Log into the device with your Azure AD Account
  2. Open the Company Portal
- Notice the app created earlier is now listed under **Newest apps**

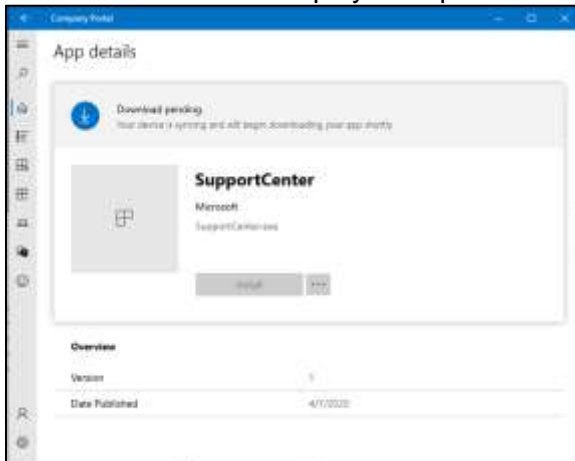


3. Click on the app. The description, company information, etc. is visible to the end-user.





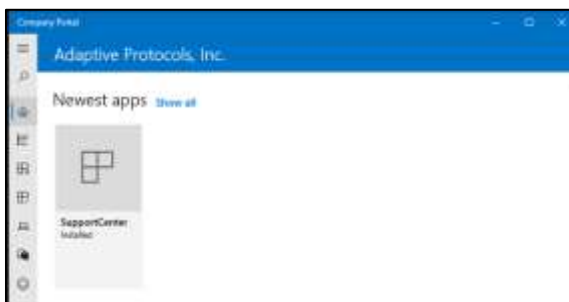
- Click on **Install**. The display will update to show Download pending



- Toast notifications will also be displayed



- When the installation has completed



## Tracing the installation in the logs

It is important to understand what is happening in the logs if there is a problem during deployment so that it can be traced back to find a solution.

The following documentation can be used for additional information:

<https://docs.microsoft.com/en-us/mem/intune/apps/troubleshoot-app-install>

- The first communication is with the Intune Management Extension. The **IntuneManagementExtension.log** is found here:

C:\ProgramData\Microsoft\IntuneManagementExtension\Logs

It will be helpful to have the name of the app

The managed client will check in about every hour.

[Proxy Poller] Proxy polling thread starts.

Or if this is an Available deployment, the user clicks on the app to install

[Win32App] Received the signal.

## 2. The policy for the app is retrieved from Intune

```
[Win32App] ----- application poller
starts. -----
Get policies = [{"Id":"04f1566f-966f-4213-95d7-7f3bb5887ec4", "Name":"SupportCenter", "DetectionRule":[{"DetectionType":1, "DetectionText":{"ProductCode":{"79C523EC-042E-420F-83FB-4CDB6B85CE15"},"ProductVersion":null, "ProductVersionOperator":""}}, {"Version":1, "Intent":1, "InstallCommandLine":"SupportCenter.exe -i", "UninstallCommandLine":"SupportCenter.exe -u", "RequirementRules":{"RequiredOSArchitecture":3, "MinimumFreeDiskSpaceInMB":null, "MinimumWindows10BuildNumber":{"10.0.14393"}, "MinimumMemoryInMB":null, "MinimumNumberOfProcessors":null, "MinimumCpuSpeed":null, "RunAs32Bit":false}, "ExtendedRequirementRules":{"InstallEx":{"RunAs":1, "RequiresLogon":true, "InstallProgramVisibility":3, "MaxRetries":3, "RetryIntervalInMinutes":5, "MaxRunTimeInMinutes":60, "DeviceRestartBehavior":1}, "ReturnCodes":[{"ReturnCode":0, "Type":1}, {"ReturnCode":1707, "Type":1}, {"ReturnCode":3010, "Type":2}, {"ReturnCode":1641, "Type":3}, {"ReturnCode":1618, "Type":4}], "AvailableAppEnforcement":0, "SetUpFilePath":"SupportCenter.exe", "ToastState":0, "Targeted":1, "FlatDependencies":null, "MetadataVersion":3, "RelationVersion":0, "RebootEx":{"GracePeriod":-1, "Countdown":-1, "Snooze":-1}, "InstallBehavior":0, "StartDeadlineEx":{"TimeFormat":"","StartTime":"","Date":62135596800000}, "Deadline":"","Date":62135596800000}, "TargetType":0, "RemoveUserData":false, "DOPriority":1}]
[Win32App] ExecManager: processing targeted app (name='SupportCenter', id='04f1566f-966f-4213-95d7-7f3bb5887ec4') with intent=1 for user session 0
```

## 3. We see the deployment starting. The detection rule is evaluated to determine if the app is already installed and should this content even be download? Notice the app was not detected as installed

```
[Win32App] ===Step=== Detection rules
[Win32App] Completed detectionManager SideCarProductCodeDetectionManager,
applicationDetectedByCurrentRule: False
```

### Requirements are checked

```
[Win32App] ===Step=== Check applicability
[Win32App] applicationRequirementMetadata.RequiredOSArchitecture is 0 or 3, skip check.
[Win32App] applicationRequirementMetadata. expected version: 10.0.14393, client version:
10.0.18362, applicability: Applicable.
```

### The Requirements are met, so download the content – this is the 80KB .intunewin file

```
[AppStatusMgr] downloadTime is 1/1/0001 12:00:00 AM
[Win32App] ===Step=== Download
[Win32App] Downloading app on session 0. App: 04f1566f-966f-4213-95d7-7f3bb5887ec4
[Win32App] DownloadType = 2, DownloadUrl = http://swda02.manage.microsoft.com/da30d15a-2bb8-4bd7-8c57-e415d1006c7d/72605fa4-d998-4608-b95c-338aff4ce11c/5367031b-38ab-4985-b28c-3e34ced5fce2.intunewin.bin
[Win32App] Downloaded file size 80,337.00
[Win32App] Start unzipping.
[Win32App] Unzipping file on session 0 from C:\Program Files (x86)\Microsoft Intune Management Extension\Content\Staging\04f1566f-966f-4213-95d7-7f3bb5887ec4_1\04f1566f-966f-4213-95d7-7f3bb5887ec4_1.zip to C:\Windows\IMECache\04f1566f-966f-4213-95d7-7f3bb5887ec4_1
```

It was downloaded successfully, now run the command line. This is the command line provided in Intune. It will trigger the download from Adaptiva.

```
[Win32App] ===Step=== ExecuteWithRetry
[Win32App] ===Step=== InstallBehavior RegularWin32App, Intent 1, UninstallCommandLine
SupportCenter.exe -u
SupportCenter.exe -i
[Win32App] SetCurrentDirectory: C:\Windows\IMECache\04f1566f-966f-4213-95d7-7f3bb5887ec4_1
[Win32App] Launch Win32AppInstaller in machine session
[StatusService] Saved AppInstallStatusReport for user <user guid> for app 04f1566f-4213-95d7-7f3bb5887ec4 in the StatusServiceReports registry.
[Win32App] Installer process timeout milliseconds: 3600000.
```

## 4. This will now invoke Adaptiva to locate and download the content.

### Let's finish with this log

```
[Win32App] Installation is done, collecting result
[Win32App] lpExitCode 0
[Win32App] lpExitCode is defined as Success
```

### Validate it was installed per the Detection rules

```
[Win32App] ===Step=== Detection rules after Execution
[Win32App] Completed detectionManager SideCarProductCodeDetectionManager,
applicationDetectedByCurrentRule: True
```

### The staging folder is cleaned up

```
Cleaning up staged content C:\Windows\IMECache\04f1566f-966f-4213-95d7-7f3bb5887ec4_1
```

### The download time is calculated, and the content is kept in the cache

```
[AppStatusMgr] downloadTime is
[Win32App] app result (id = 04f1566f-966f-4213-95d7-7f3bb5887ec4, version = 1) is
different from cached one, save to cache.
[Win32App] ----- application poller
stopped. -----
```

- When Adaptiva takes over, start with the following log:

#### AdaptivaRemoteInstallLog.log

It is also important to know the content id. This will be IntuneP2PApp\$<appname>. It is highlighted in pink. It can be used to filter the various logs as well

```
INFO: Beginning Adaptiva Remote Install.
INFO: Found: 1000: 1242 bytes
DEBUG: Downloading content [IntuneP2PApp$SupportCenter] to parent folder
[C:\Windows\temp\SupportCenter\IntuneP2PApp$SupportCenter]
```

Note on the path listed as parent folder: I directed the install to this folder, by default content will be extracted to C:\AdaptivaCache\\_sadaptiva\\_UnpackedContents\IntuneP2PApp\$<app name>

```
SessionId: {7A9A7AB-724E-1D5A-50A5-548949CE74E5}
```

- The SessionID triggers **RemoteWorkflowExecution.log**. It is another good field to filter on. It is highlighted in yellow

```
INFO - Giving request to request handler, SessionId: {7A9A7AB-724E-1D5A-50A5-548949CE74E5} - RemoteWorkflowExecutionManager - TID=284, ConsumerTask: Sender Id = [-2],
Retry Level : 0
```

- Recall, when we looked at the Storage container after Generating the P2P App. The location is highlighted in blue.

```
INFO - Name of the message: RemoteWorkflowRequest, Sender ID: -2, Receiver ID: -2, Queue
ID: 1, CORRELATION ID: 2, ORIGINAL CORRELATION ID: 0, ORIGINAL RECEIVER ID: 1, REPLY TO:
1, REPLY TO IP: /127.0.0.1, IS REPLY: false, TRANSPORT: 0, Attribute count: 34Attribute
names and their values: Name: Count ,Value: 15; Name: ID ,Value: {7A9A7AB-724E-1D5A-50A5-548949CE74E5};
Name: P0 ,Value: ContentId; Name: P1 ,Value: Folder; Name: P10 ,Value:
UseWakeOnLAN; Name: P11 ,Value: WaitForCompletion; Name: P12 ,Value:
FireWindowsEventOnProgress; Name: P13 ,Value: FireWindowsEventOnCompletion; Name: P14
,Value: ContentPubDataText; Name: P2 ,Value: FailoverToCDN; Name: P3 ,Value: CDNUrls;
Name: P4 ,Value: FileName; Name: P5 ,Value: SHA256; Name: P6 ,Value: DownloadPriority;
Name: P7 ,Value: LocalTimeout; Name: P8 ,Value: RemoteTimeout; Name: P9 ,Value:
TotalTimeout; Name: PW ,Value: <encrypted>; Name: V0 ,Value:
IntuneP2PApp$24SupportCenter; Name: V1 ,Value:
C:\Windows\temp\SupportCenter\IntuneP2PApp$24SupportCenter; Name: V10 ,Value: false;
Name: V11 ,Value: true; Name: V12 ,Value: false; Name: V13 ,Value: false; Name: V14
,Value: <encrypted>; Name: V2 ,Value: true; Name: V3 ,Value:
https://storageaccount.blob.core.windows.net/container/E9DEC27C-7858-11EA-8080-00155D0A1E42/IntuneP2PApp$24SupportCenter.1.content?sv=2019-02-02$26ss=bfqt$26srt=sco$26sp=rlp$26se=<SASend>$26st=<SASstart>$26spr=https$26sig=<SAS>;
Name: V4 ,Value: ; Name: V5 ,Value: ; Name: V6 ,Value: 255; Name: V7 ,Value: 60; Name: V8
,Value: 180; Name: V9 ,Value: 604800; Name: WF ,Value: OneSiteContentDownloadCDN; -
RemoteWorkflowExecutionManager - TID=284, ConsumerTask: Sender Id = [-2], Retry Level : 0
INFO - Successfully launched workflow: OneSiteContentDownloadCDN, intance id:1, for
request Id: {7A9A7AB-724E-1D5A-50A5-548949CE74E5} -
RemoteWorkflowExecutionManager$RemoteExecutionRequestHandler - TID=285, Thread=265
```

- This triggers the workflow **OneSiteContentDownloadCDN** to start. Open that log from workflowlogs

```
Prop: Start1.CDNUrls, TEXT, Old: none, New:
https://storageaccount.blob.core.windows.net/container/E9DBC27C-7858-11EA-8080-00155D0A1E42/IntuneP2PApp$SupportCenter.1.content?sv=2019-02-02&ss=bfqt&srt=sco&sp=rlp&se=<SASend>&st=<SASstart>&spr=https&sig=<SAS>
Prop: Start1.ContentID, TEXT, Old: none, New: IntuneP2PApp$SupportCenter
Prop: SessionGUID.GUID, TEXT, Old: none, New: dd12d63c-7a21-11ea-8d88-00155d0a1e52
Prop: CDNContentDownload.SessionHandle, TEXT, Old: none, New: OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52
```

- The download is then handed off to **ContentDownload.log** in componentlogs with a Session id which can be filtered on as well. It is highlighted in green.

```
INFO - Content publication data request sent to server: IntuneP2PApp$SupportCenter -
ContentDownloader - TID=286, Pooled Thread -
com.adaptiva.workflow.model.LauncherRunnable@13a4578
INFO - Invoking downloadContent for session : OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52 and contents : [IntuneP2PApp$SupportCenter] - ContentDownloader - TID=286, Pooled Thread - com.adaptiva.workflow.model.LauncherRunnable@13a4578
INFO - Write locks acquired for for session : OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52 and contents : [IntuneP2PApp$SupportCenter] - ContentDownloader - TID=286, Pooled Thread - com.adaptiva.workflow.model.LauncherRunnable@13a4578
INFO - Starting download for : IntuneP2PApp$SupportCenter - ContentDownloader - TID=286, Pooled Thread - com.adaptiva.workflow.model.LauncherRunnable@13a4578
```

- In **SentRecvMsg.log**, the normal election process is held, does anyone have this content?

```
INFO - Attempting to send (Broadcast): Receiver ID: -1, Receiver IP: null, MsgLen: 644, Correlation ID = 1586408948351 port: 34329, transport:
com.adaptiva.transport.BroadcastTransport@121304c, Message :Name of the message:
P2PDiscoveryRequest, Sender ID: 4, Receiver ID: 1, Queue ID: 1, CORRELATION ID: 0, ORIGINAL CORRELATION ID: 0, ORIGINAL RECEIVER ID: 1, REPLY TO: 1, REPLY TO IP: null, IS REPLY: false, TRANSPORT: 0, Attribute count: 22Attribute names and their values: Name: RequestID ,Value: 17179869185; Name: NoOfConditions ,Value: 4; Name: FieldID0 ,Value: 1; Name: Operator0 ,Value: 1; Name: Value0 ,Value: Content; Name: CaseInsensitive0 ,Value: 1; Name: FieldID1 ,Value: 2; Name: Operator1 ,Value: 1; Name: Value1 ,Value: IntuneP2PApp$SupportCenter; Name: CaseInsensitive1 ,Value: 1; Name: FieldID2 ,Value: 3; Name: Operator2 ,Value: 1; Name: Value2 ,Value: 1; Name: CaseInsensitive2 ,Value: 1; Name: FieldID3 ,Value: 4; Name: Operator3 ,Value: 4; Name: Value3 ,Value: 0; Name: CaseInsensitive3 ,Value: 1; Name: MaxResponses ,Value: 4; Name: SpreadDuration ,Value: 4000; Name: NewVersion ,Value: ; Name: _SERVER_GUID_ ,Value: 7e90219e-75fa-11ea-bf70-00155d0a1e42; - SendingThread - TID=77, SendingThread: [Receiver Id= -1]
```

- In **ContentDownload** we can see that download starts. Communication will go back and forth with **RemoteWorkflowExecution.log**. It figures out it has to download from Azure storage instead of a peer or a parent office.

```
INFO - CDNDownloadProtocol started for content Id : IntuneP2PApp$SupportCenter content version : 1 - CDNDownloadProtocol - TID=297, STP-SessionHandle=[OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52], Content Id=[IntuneP2PApp$SupportCenter]
INFO - ServerAssistedDiscoveryProtocolOutput : [ Status: 15, StatusString:
USE CDN AS_SOURCE, Priority: -1, WAN Transport: null, WAN Transport String: null] -
StateTransitionProtocol - TID=297, STP-SessionHandle=[OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52], Content Id=[IntuneP2PApp$SupportCenter]
```

- Now filter **ContentDownload** on **Content download progress**. Notice where it is downloading from. It might be across the LAN or across the WAN, it might be across the INternet or from the CDN.

```
INFO - Content download progress percentage notification. ContentId
:IntuneP2PApp$SupportCenter, Content version: 1, Current download type: 0, percentage:
44, download source: CDN$https://storageaccount.blob.core.windows.net/container/E9DBC27C-7858-11EA-8080-00155D0A1E42/IntuneP2PApp$SupportCenter.1.content?sv=2019-02-02&ss=bfqt&srt=sco&sp=rlp&se=<SASend>&st=<SASstart>&spr=https&sig=<SAS>, Lan download(in bytes): 0, Wan download(in bytes): 2341888 - StateTransitionProtocol - TID=321,
CDNDownloadPollingThread
INFO - Content download progress percentage notification. ContentId
:IntuneP2PApp$SupportCenter, Content version: 1, Current download type: 0, percentage:
100, download source:
CDN$https://storageaccount.blob.core.windows.net/container/E9DBC27C-7858-11EA-8080-00155D0A1E42/IntuneP2PApp$SupportCenter.1.content?sv=2019-02-02&ss=bfqt&srt=sco&sp=rlp&se=<SASend>&st=<SASstart>&spr=https&sig=<SAS>, Lan download(in
```

bytes): 0, Wan download(in bytes): 5231835 - StateTransitionProtocol - TID=314, CNDNDownloadThread [OneSiteIntune\$dd12d63c-7a21-11ea-8d88-00155d0a1e52]

- Once the content is downloaded, its hash is checked and then unpacked

```
INFO - Marked unpacking start for handle: OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52 - ContentUnpacker - TID=297, STP-SessionHandle=[OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52], Content Id=[IntuneP2PApp$SupportCenter]
INFO - Content unpacking successful for session : OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52 - ContentDownloader - TID=297, STP-SessionHandle=[OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52], Content Id=[IntuneP2PApp$SupportCenter]
```

- Finally, ContentDownload marks the download as complete and releases the RVP locks

```
INFO - Content download completed for content ID : IntuneP2PApp$SupportCenter, for session handle : OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52 - ContentDownloader - TID=297, STP-SessionHandle=[OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52], Content Id=[IntuneP2PApp$SupportCenter]
INFO - Released write lock for session : OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52 - ContentDownloader - TID=297, STP-SessionHandle=[OneSiteIntune$dd12d63c-7a21-11ea-8d88-00155d0a1e52], Content Id=[IntuneP2PApp$SupportCenter]
```

- Now, in **AdaptivaRemoteInstallLog.log**, with the download completed and unpacked, run the command line to perform the installation and get the installation status

```
DEBUG: Executing commandLine [C:\Windows\system32\msiexec.exe /i supportcenterinstaller.msi /qn /log C:\Windows\temp\Install_SupportCenter.log] in directory [C:\Windows\temp\SupportCenter\IntuneP2PApp$SupportCenter\]
INFO: Application install completed with code: 0
INFO: Returning status 0
INFO: Execution completed for content: IntuneP2PApp$SupportCenter. Result: 0
```

## Workspace ONE

When the app created is targeted as On Demand to an assignment group, the VMWare Workspace ONE app (HUB app) or web-based App catalog is used to request the installation of the app. When the application assignment is set to Auto, the installation will happen automatically based on the assignment configuration.

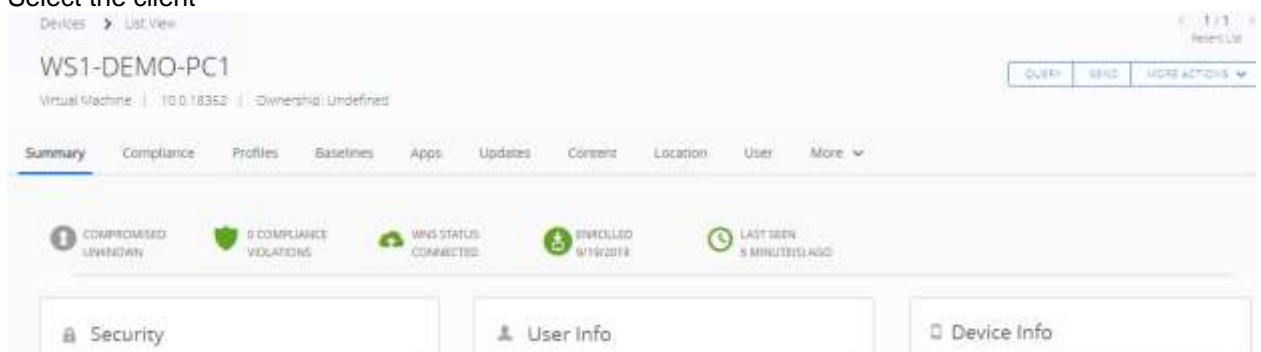
### Accessing the VMWare Airwatch catalog

Clients can see which apps have been assigned to them by accessing the catalog in their web browser

The challenge is the client must know their Encrypted UID

To find a client's Encrypted UID:

- In the Workspace ONE UEM console, select Devices, List View
- Select the client

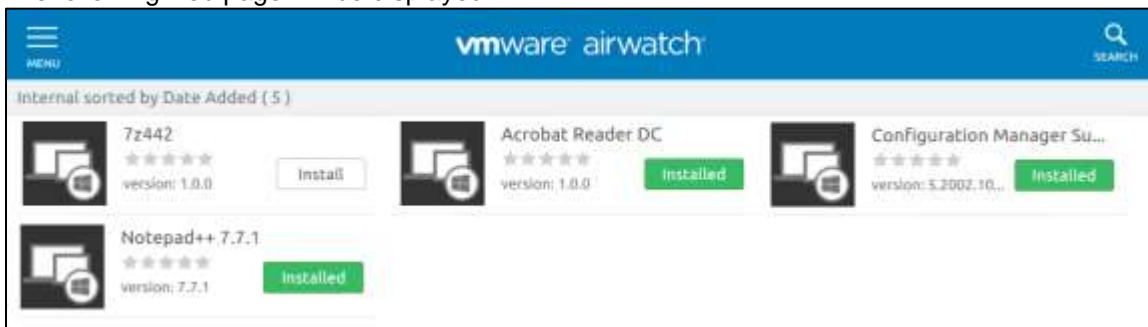


- In the Device Info section, look for UDID. This is the client's Encrypted UID

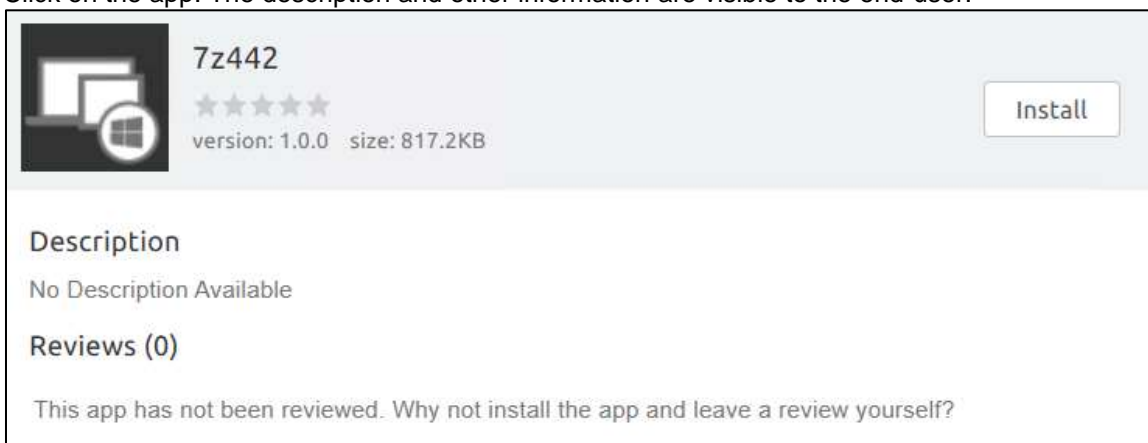
To open the catalog

- Open a web browser

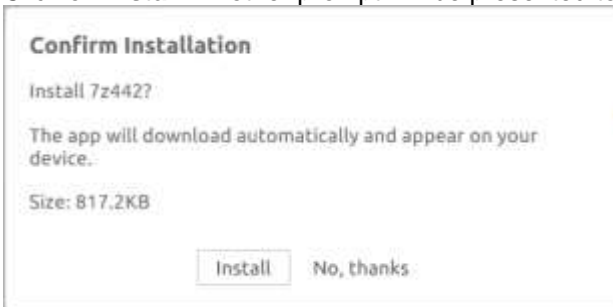
- In the address bar enter the following URL:  
<https://ds800.airwatchportals.com/Catalog/ViewCatalog/<clientEncryptedUID>/WinRT?type=Internal>
- The following web page will be displayed



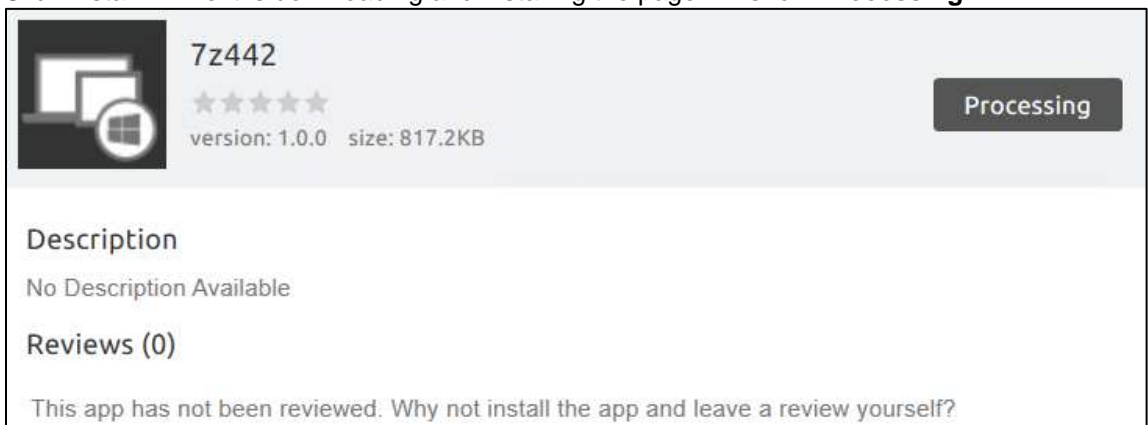
- Click on the app. The description and other information are visible to the end-user.



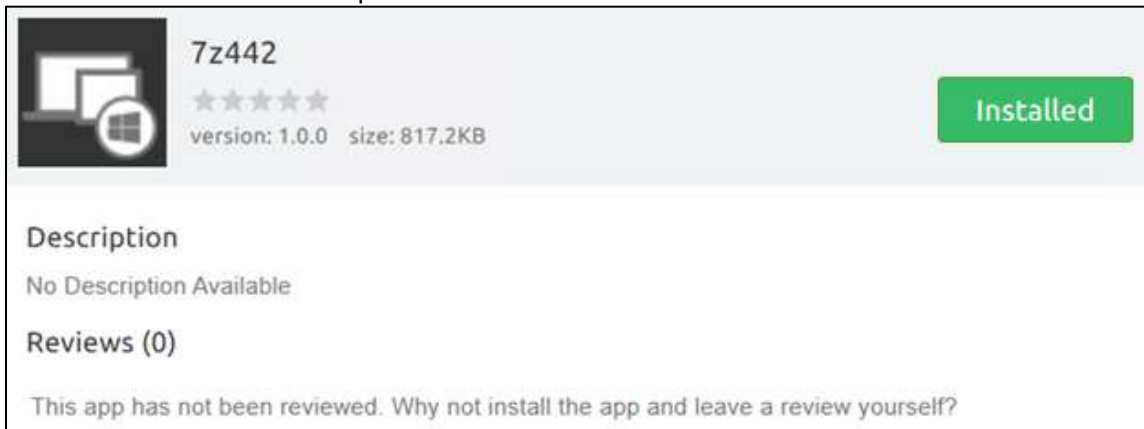
- Click on **Install**. Another prompt will be presented to ensure you want to install the app.



- Click Install. While it is downloading and installing the page will show **Processing**



7. When the installation has completed



### Tracing the installation in the logs

It is important to understand what is happening in the logs if there is a problem during deployment so that it can be traced back to find a solution.

The following documentation can be used for additional information:

<https://techzone.vmware.com/troubleshooting-windows-10-vmware-workspace-one-operational-tutorial#968024>

The first communication is with the AirWatch Management Extension. The AirWatch MDM agent records its information in the registry.

You need to start with the Name of the app and then get the Identity ID

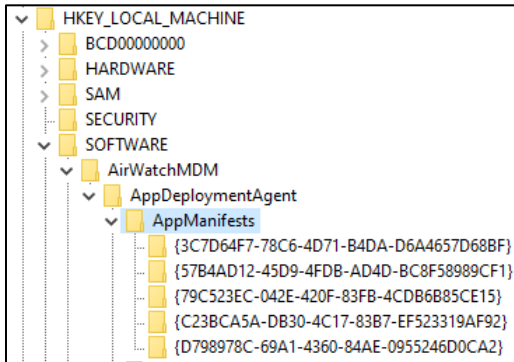
1. The Identity ID can be obtained in the Adaptiva Workbench or by searching the registry
  - a. In the Adaptiva Workbench, Open the Content Distribution Status Perspective
  - b. Expand VMware Contents

#### Content Explorer



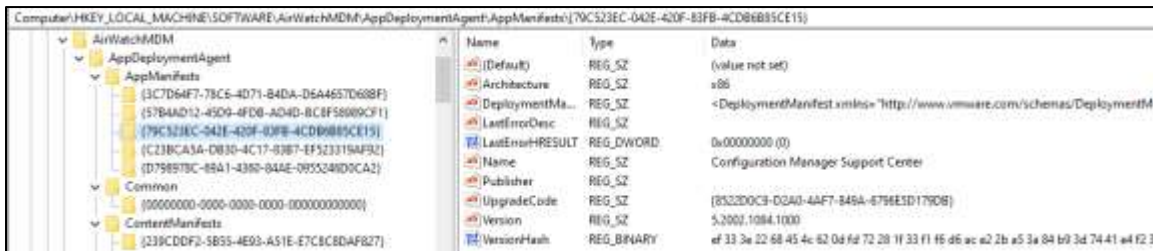
- c. Notice the GUID after the executable that was used to create the App in Workspace ONE. This is the Identity ID. For my example, the GUID is B4E1F138-B2D3-45BC-88E1-037B4BC08AA6

- Open the registry and browse to  
HKLM\Software\AirWatchMDM\AppDeploymentAgent\AppManifests



Use the Identity ID GUID to find the app manifest. Notice the GUID for my example is not listed. It is under a different GUID.

**NOTE:** It is possible that a different ID was used. If the GUID is not listed, search through the manifests GUIDs for your app. The Identity ID GUID may be different when an MSI is used to create the app



- If your app is not there, then the AirWatch MDM client has not received the policy yet. Force a sync with Workspace ONE by following these steps:
  - Click on **Start, Settings** (the gear icon), **Accounts, Access work or school**
  - Select **Connected to Workspace ONE MDM** and click **Info**
  - Under Device sync status, click **Sync**
  - Wait for synchronization to be completed
- Get the Key GUID for the app. In the example above, the GUID is: {79C523EC-042E-420F-83FB-4CDB6B85CE15}
- Copy the data from DeploymentManifestXML and paste it into Notepad, or better something that will automatically reformat the text for XML



The DeploymentManifestXML data will provide the information on how to install/uninstall/detect the app being installed

```
<Requirements>
  <Condition>DevicePowerLevel >=0</Condition>
  <Condition>PhysicalMemory >=0</Condition>
  <Condition>AvailPhysMem >=0</Condition>
  <Condition>SystemDriveFreeDiskSpace >=0</Condition>
</Requirements>
<Dependencies />
<Deploy>
  <Method Id="install" Type="EXEC">
    <Key Name="RetryCount">3</Key>
    <Key Name="RetryInterval">300</Key>
    <Key Name="ForceReboot">>false</Key>
    <Key Name="PerformReboot">>false</Key>
    <Key Name="UseElevatedToken">True</Key>
    <Key Name="MaxExecuteTimeout">3600</Key>
    <Key Name="CommandLine">msiexec /i "supportcenterinstaller.msi" /qn</Key>
    <Key Name="CheckExitCode">>true</Key>
    <Key Name="SuccessExitCodeList">0</Key>
    <Key Name="RebootExitCodeList">1641</Key>
  </Method>
  <Method Id="uninstall" Type="EXEC">
    <Key Name="RetryCount">3</Key>
    <Key Name="RetryInterval">300</Key>
    <Key Name="ForceReboot">>false</Key>
    <Key Name="PerformReboot">>false</Key>
    <Key Name="UseElevatedToken">True</Key>
    <Key Name="MaxExecuteTimeout">3600</Key>
    <Key Name="CommandLine">MSIEXEC /x "supportcenterinstaller.msi" /qn</Key>
  </Method>
  <Method Id="detect" Type="CONDITION">
    <Condition>PRODUCTCODE</Condition>
  </Method>
</Deploy>
```

- Now expand ContentManifests and select the GUID to get information as to where the content will be obtained from



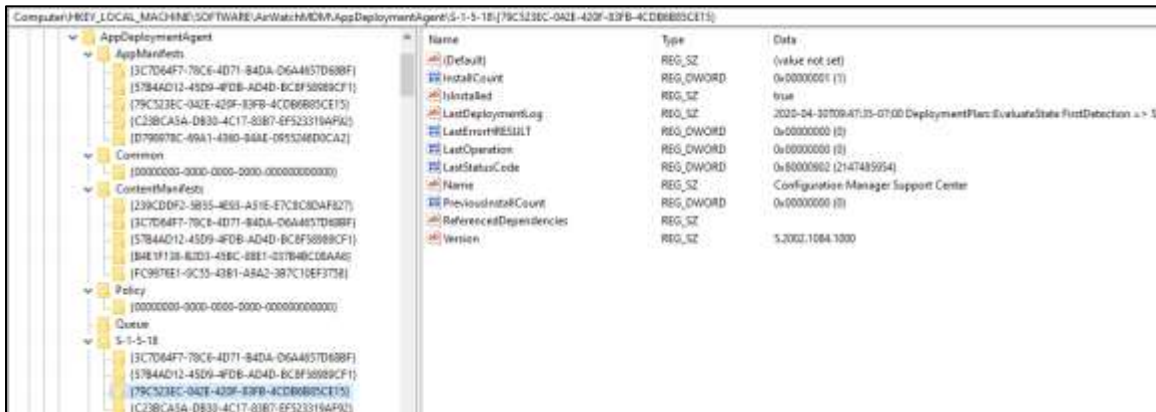
- Copy the data from ContentManifestXML and paste it into Notepad, or better something that will automatically reformat the text for XML

The ContentManifestXML data will provide the information on where the content will be downloaded from. Notice the **Type="P2P"**

```
<ContentManifest xmlns="http://www.snow.com/schemas/ContentManifest/1">
  <Identity Id="{b4e1f138-b2d3-45bc-8be1-037b4b08aa6}" />
  <Content>
    <Content LocalName="supportcenterinstaller.msi" SHA256="5D758A062CFD9F988489051B538A53862A48827B6A2457E44A619C18B9AD47D4" FileSize="5230592">
      <Source Type="CDN">
        <a href="https://CDN002.amazonaws.com/onB00.airwatchportals.com/12074/Apps/b4e1f138-b2d3-45bc-8be1-037b4b08aa6.msi?Token=at-1589264354-xxx-1589351654">https://CDN002.amazonaws.com/onB00.airwatchportals.com/12074/Apps/b4e1f138-b2d3-45bc-8be1-037b4b08aa6.msi?Token=at-1589264354-xxx-1589351654</a>
      </Source>
      <Source Type="APN">
        <a href="https://s0001.airwatchportals.com/DeviceServices/public/obj/b4e1f138-b2d3-45bc-8be1-037b4b08aa6/DeviceHandler_obj/obj?e=McQ6VwITTYQvaby02C3Z">https://s0001.airwatchportals.com/DeviceServices/public/obj/b4e1f138-b2d3-45bc-8be1-037b4b08aa6/DeviceHandler_obj/obj?e=McQ6VwITTYQvaby02C3Z</a>
      </Source>
      <Source Type="P2P">
        <a href="http://www.snow.com/schemas/ContentManifest/1">http://www.snow.com/schemas/ContentManifest/1</a>
      </Source>
    </Content>
  </Content>
</ContentManifest>
```

- If the app is installing as the System, look under S-1-5-18

If the app is installing under the user's context, then look under the SID for the user



- Select the GUID for the app and select the LastDeploymentLog value. Copy the data to Notepad. This data is not in XML format
- We see the deployment starting. The detection rule is evaluated to determine if the app is already installed and should this content even be download? Notice the app was not detected as installed

```
DeploymentPlan::EvaluateState FirstDetection => STATE_INPROGRESS
DetectionExecItem::Execute: Running Conditional detection {79C523EC-042E-420F-83FB-4CDB6B85CE15}
ConditionEvalExecItem::Execute: Evaluate (PRODUCTCODE) FAILURE. {79C523EC-042E-420F-83FB-4CDB6B85CE15} TargetSID: S-1-5-18
DeploymentPlan::OnAfterExecution FirstDetection => STATE_FALSE
DeploymentPlan::EvaluateState FirstDetection - IsInstalled => false
```

- Requirements and dependencies are checked

```
DeploymentPlan::EvaluateState CheckReferenceCount => STATE_INPROGRESS
RefCountEvalExecItem::Execute2: {79C523EC-042E-420F-83FB-4CDB6B85CE15} INSTALL,
Dependency: 0, Dependency Counting: 1
RefCountEvalExecItem::Execute2: {79C523EC-042E-420F-83FB-4CDB6B85CE15} - Target SID: S-1-5-18
RefCountEvalExecItem::Execute2 Original State --> Installed: 0, RefCount: 0,
UserInstalled: 0, OverrideUserInstall: 0
RefCountEvalExecItem::DependencyAction: Reset registered dependencies.
RefCountEvalExecItem::Execute2: Incrementing InstallCount to 1.
RefCountEvalExecItem::Execute2 New State --> RefCount: 1, UserInstalled: 0,
OverrideUserInstall: 0
DeploymentPlan::OnAfterExecution CheckReferenceCount => STATE_TRUE
DeploymentPlan::EvaluateState RequirementsEvaluation => STATE_INPROGRESS
ConditionEvalExecItem::Execute: Evaluate (DevicePowerLevel >=0) SUCCESS. {79C523EC-042E-420F-83FB-4CDB6B85CE15} TargetSID: S-1-5-18
ConditionEvalExecItem::Execute: Evaluate (PhysicalMemory >=0) SUCCESS. {79C523EC-042E-420F-83FB-4CDB6B85CE15} TargetSID: S-1-5-18
ConditionEvalExecItem::Execute: Evaluate (AvailPhysMem >=0) SUCCESS. {79C523EC-042E-420F-83FB-4CDB6B85CE15} TargetSID: S-1-5-18
ConditionEvalExecItem::Execute: Evaluate (SystemDriveFreeDiskSpace >=0) SUCCESS. {79C523EC-042E-420F-83FB-4CDB6B85CE15} TargetSID: S-1-5-18
DeploymentPlan::OnAfterExecution RequirementsEvaluation => STATE_TRUE
DeploymentPlan::EvaluateState Dependencies => STATE_INPROGRESS
DeploymentPlan::EvaluateState Dependencies => STATE_TRUE
DeploymentPlan::EvaluateState SanitizeCache => STATE_INPROGRESS
DeploymentPlan::EvaluateState CacheConsistency => STATE_UNSTARTED
DeploymentPlan::OnAfterExecution SanitizeCache => STATE_TRUE
DeploymentPlan::EvaluateState CacheConsistency => STATE_INPROGRESS
DeploymentPlan::OnAfterExecution CacheConsistency => STATE_FALSE
```

12. Requirements have been met and there were no dependencies, so download the content

Notice the Transport is P2P. This will now hand over the Content Delivery process to the Adaptiva client.

```
DeploymentPlan::EvaluateState DownloadContent => STATE_INPROGRESS
DeploymentPlan::EvaluateState SanitizeCache => STATE_UNSTARTED
DownloadExecItem::ResolveDownloaderPlugin: Transport: P2P
DownloadExecItem::Execute: Download started...
RunAdaptivaTransferLoop: [+0] Add URL:
https://CDNUS02.awmdm.com/cn800.airwatchportals.com/12074/Apps/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6.msi?token=st=1588264954~exp=1588351654~acl=/*~hmac=437a59c5085bce8b2b3f90a4e6cfc76b6431debc963f6788babf2f95b3196
RunAdaptivaTransferLoop: [+0] Add URL:
https://ds800.airwatchportals.com/DeviceServices/publicblob/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6/BlobHandler.pblob?s=MsCMeVwPTY5vxby5ZC%2bjVq4QfrmpQCXfEFPzfD7MURqoXvybx3iV53%2bKK%40wqVKL1X4NyreyDfq0PuHC6HPiIA%3d%3d
RunAdaptivaTransferLoop: [+0] Download starts. ContentId=b4e1f138-b2d3-45bc-88e1-037b4bc08aa6. FileName=supportcenterinstaller.msi
RunAdaptivaTransferLoop: [+0] |--- Content download progress 0 of 5230592 bytes. ContentId=b4e1f138-b2d3-45bc-88e1-037b4bc08aa6. DownloadSource=Unknown(Unknown)
RunAdaptivaTransferLoop: [+90] |--- Content download progress 3072 of 5230592 bytes. ContentId=b4e1f138-b2d3-45bc-88e1-037b4bc08aa6. DownloadSource=WAN(10.75.11.5)
RunAdaptivaTransferLoop: [+90] Download progress 3072 of 5230592 bytes
RunAdaptivaTransferLoop: [+93] |--- Content download progress 5230592 of 5230592 bytes. ContentId=b4e1f138-b2d3-45bc-88e1-037b4bc08aa6. DownloadSource=WAN(10.75.11.5)
RunAdaptivaTransferLoop: [+93] Download progress 5230592 of 5230592 bytes
RunAdaptivaTransferLoop: [+93] Download job completed for 1 contents.
AdaptivaDownload: Download is completed successfully.
DownloadExecItem::Execute: Download request completed in 93/sec
DeploymentPlan::OnAfterExecution DownloadContent => STATE_TRUE
```

13. When the AirWatch MDM agent hands over to Adaptiva we can also see the download happening there. Start with the **RemoteWorkflowExecution.log** in c:\program files (x86)\Adaptiva\AdaptivaClient\Logs\ComponentLogs

```
INFO - Name of the message: RemoteWorkflowRequest, Sender ID: -2, Receiver ID: -2, Queue ID: 1, CORRELATION ID: 2, ORIGINAL CORRELATION ID: 0, ORIGINAL RECEIVER ID: 1, REPLY TO: 1, REPLY TO IP: /127.0.0.1, IS REPLY: false, TRANSPORT: 0, Attribute count: 15Attribute names and their values: Name: Count ,Value: 6; Name: ID ,Value: {466A964-1650-75F5-7EEF-10DC3D2466FF}; Name: P0 ,Value: ContentID; Name: P1 ,Value: Folder; Name: P2 ,Value: FailoverToCDN; Name: P3 ,Value: FileName; Name: P4 ,Value: SHA256; Name: P5 ,Value: CDNUrls; Name: V0 ,Value: b4e1f138-b2d3-45bc-88e1-037b4bc08aa6; Name: V1 ,Value: C:\ProgramData\AirWatchMDM\AppDeploymentCache\{B4E1F138-B2D3-45BC-88E1-037B4BC08AA6}\; Name: V2 ,Value: true; Name: V3 ,Value: supportcenterinstaller.msi; Name: V4 ,Value: 5d758a062cfd9f8bb48b051b53ba53862a4bb27b6ae657e44a619c1eb9ab67d6; Name: V5 ,Value: https://CDNUS02.awmdm.com/cn800.airwatchportals.com/12074/Apps/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6.msi?token=st=1588264954~exp=1588351654~acl=/*~hmac=437a59c5085bce8b2b3f90a4e6cfc76b6431debc963f6788babf2f95b3196$3Chttps://ds800.airwatchportals.com/DeviceServices/publicblob/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6/BlobHandler.pblob?s=MsCMeVwPTY5vxby5ZC%2bjVq4QfrmpQCXfEFPzfD7MURqoXvybx3iV53%2bKK%40wqVKL1X4NyreyDfq0PuHC6HPiIA%3d%3d; Name: WF ,Value: vmwareInitiateContentDownload; - RemoteWorkflowExecutionManager - TID=6332, ConsumerTask: Sender Id = [-2], Retry Level : 0
```

14. This will trigger the workflow vmwareInitiateContentDownload to start. Open that log from workflowlogs

```
Prop: Start1.WorkflowInstanceId, WHOLE NUMBER, Old: None, New: 16
Prop: Start1.SHA256, TEXT, Old: None, New: <secure hash>
Prop: Start1.FailoverToCDN, BOOLEAN, Old: false, New: true
Prop: Start1.FileName, TEXT, Old: None, New: supportcenterinstaller.msi
Prop: Start1.ContentID, TEXT, Old: None, New: b4e1f138-b2d3-45bc-88e1-037b4bc08aa6
Prop: Start1.Folder, TEXT, Old: None, New: C:\ProgramData\AirWatchMDM\AppDeploymentCache\{B4E1F138-B2D3-45BC-88E1-037B4BC08AA6}\
Prop: Start1.CDNUrls, TEXT, Old: None, New: https://CDNUS02.awmdm.com/cn800.airwatchportals.com/12074/Apps/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6.msi?token=st=1588264954~exp=1588351654~acl=/*~hmac=437a59c5085bce8b2b3f90a4e6cfc76b6431debc963f6788babf2f95b3196<https://ds800.airwatchportals.com/DeviceServices/publicblob/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6/BlobHandler.pblob?s=MsCMeVwPTY5vxby5ZC%2bjVq4QfrmpQCXfEFPzfD7MURqoXvybx3iV53%2bKK%40wqVKL1X4NyreyDfq0PuHC6HPiIA%3d%3d
```

15. The download is then handed off to ContentDownload.log in componentlogs with a Session id which can be filtered on as well. It is highlighted in green.

```

INFO - Input URL
[https://CDNUS02.awmdm.com/cn800.airwatchportals.com/12074/Apps/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6.msi?token=st=1588264954~exp=1588351654~acl=/*~hmac=437a59c5085bce8b2b3f90a4e6cfcdc76b6431debc963f6788babf2f95b3196] used as it is - HttpDirectDownloadClient -
TID=6334, Pooled Thread - com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - Input URL [https://ds800.airwatchportals.com/DeviceServices/publicblob/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6/BlobHandler.pblob?s=MsCMeVwPTY5vxby5ZC%2bjVq4QfrmpQCXfEEPzfd7MURqoXvybx3iV53%2bKK%40wqVKL1X4NyreyDfq0PuHC6HPiIA%3d%3d], changed to
[https://ds800.airwatchportals.com/DeviceServices/publicblob/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6/BlobHandler.pblob?s=MsCMeVwPTY5vxby5ZC%252bjVq4QfrmpQCXfEEPzfd7MURqoXvybx3iV53%252bKK%2540wqVKL1X4NyreyDfq0PuHC6HPiIA%253d%253d] - HttpDirectDownloadClient -
TID=6334, Pooled Thread - com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - ServerLess mode FALSE - ContentDownloader - TID=6334, Pooled Thread -
com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - Content publication data request sent to server: b4e1f138-b2d3-45bc-88e1-037b4bc08aa6 - ContentDownloader - TID=6334, Pooled Thread -
com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - Cached ContentPublicationData for: b4e1f138-b2d3-45bc-88e1-037b4bc08aa6 - ContentDownloader - TID=6334, Pooled Thread -
com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - Invoking downloadContent for session : VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede and contents : [b4e1f138-b2d3-45bc-88e1-037b4bc08aa6, ] - ContentDownloader - TID=6334, Pooled Thread - com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - Write locks acquired for for session : VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede and contents : [b4e1f138-b2d3-45bc-88e1-037b4bc08aa6, ] - ContentDownloader - TID=6334, Pooled Thread - com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - Cleared lan/wan cost content session: VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede - ContentDownloader - TID=6334, Pooled Thread -
com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - Added content name mapping: supportcenterinstaller.msi_b4e1f138-b2d3-45bc-88e1-037b4bc08aa6, ID: b4e1f138-b2d3-45bc-88e1-037b4bc08aa6 - ContentDownloader - TID=6334, Pooled Thread - com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - Content download transaction log created for session : VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede - ContentDownloader - TID=6334, Pooled Thread -
com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - Download content flag is set to TRUE. Stored session is VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede - ContentDownloader - TID=6334, Pooled Thread -
com.adaptiva.workflow.model.LauncherRunnable@c39107
INFO - Starting download for : b4e1f138-b2d3-45bc-88e1-037b4bc08aa6 - ContentDownloader - TID=6334, Pooled Thread - com.adaptiva.workflow.model.LauncherRunnable@c39107

```

16. In SentRecvMsg.log, the normal election process is held, does anyone have this content? If no one has the content, the client will request the content from the parent office. If no one has the content, the request will go up to the Central Office where a client will download the content from the CDN. If the Office is configured to allow Direct CDN Download, then the elected client in the remote office will download from the CDN.

```

INFO - Attempting to send (Broadcast): Receiver ID: -1, Receiver IP: null, MsgLen: 645, Correlation ID = 2256 port: 34329, transport:
com.adaptiva.transport.BroadcastTransport@1576090, Message :Name of the message:
P2PDiscoveryRequest, Sender ID: 3, Receiver ID: 1, Queue ID: 1, CORRELATION ID: 0, ORIGINAL CORRELATION ID: 0, ORIGINAL RECEIVER ID: 1, REPLY TO: 1, REPLY TO IP: null, IS REPLY: false, TRANSPORT: 0, Attribute count: 22Attribute names and their values: Name: RequestID ,Value: 12884901935; Name: NoOfConditions ,Value: 4; Name: FieldID0 ,Value: 1; Name: Operator0 ,Value: 1; Name: Value0 ,Value: Content; Name: CaseInsensitive0 ,Value: 1; Name: FieldID1 ,Value: 2; Name: Operator1 ,Value: 1; Name: Value1 ,Value: b4e1f138-b2d3-45bc-88e1-037b4bc08aa6; Name: CaseInsensitive1 ,Value: 1; Name: FieldID2 ,Value: 3; Name: Operator2 ,Value: 1; Name: Value2 ,Value: 1; Name: CaseInsensitive2 ,Value: 1; Name: FieldID3 ,Value: 4; Name: Operator3 ,Value: 4; Name: Value3 ,Value: 0; Name: CaseInsensitive3 ,Value: 1; Name: MaxResponses ,Value: 4; Name: SpreadDuration ,Value: 4000; Name: NewVersion ,Value: ; Name: _SERVER_GUID_ ,Value: cdb31551-de31-11e9-8df3-00155d0a1ee7; - SendingThread - TID=111, SendingThread: [Receiver Id= -1]

```

17. In ContentDownload we can see the download start. Communication will go back and forth with RemoteWorkflowExecution.log. It figures out it has to download from VMware CDN storage instead of a peer or a parent office.

```
INFO - RemoteDownloadProtocol started for content Id : b4e1f138-b2d3-45bc-88e1-037b4bc08aa6 content version : 1 - RemoteDownloadProtocol - TID=6344, STP-SessionHandle=[VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede], Content Id=[b4e1f138-b2d3-45bc-88e1-037b4bc08aa6]
```

18. Now filter ContentDownload on **CDN\$** or **INT\$**, if the content is coming from the internet, or **AN\$** to see if the content is coming from the LAN or WAN. Unless the Adaptiva office is configured to download from the CDN, the clients will always download from another Adaptiva client either on the LAN or at the parent office across the WAN. These are the entries from the client downloading from a client in the parent office

```
INFO - Content download progress percentage notification. ContentId : b4e1f138-b2d3-45bc-88e1-037b4bc08aa6, Content version: 1, Current download type: 0, percentage: 0, download source: WAN$10.75.11.5, Lan download(in bytes): 0, Wan download(in bytes): 3072 - StateTransitionProtocol - TID=32, Polling Thread
INFO - Content download progress percentage notification. ContentId : b4e1f138-b2d3-45bc-88e1-037b4bc08aa6, Content version: 1, Current download type: 0, percentage: 100, download source: WAN$10.75.11.5, Lan download(in bytes): 0, Wan download(in bytes): 5230592 - StateTransitionProtocol - TID=32, Polling Thread
This is what the client in the parent office is doing
INFO - Content download progress percentage notification. ContentId : b4e1f138-b2d3-45bc-88e1-037b4bc08aa6, Content version: 1, Current download type: 0, percentage: 15, download source: CDN$https://CDNUS02.awmdm.com/cn800.airwatchportals.com/12074/Apps/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6.msi?token=st=1588264954~exp=1588351654~acl=/*~hmac=437a59c5085bce8b2b3f90a4e6cfcfdc76b6431debc963f6788babf2f95b3196, Lan download(in bytes): 0, Wan download(in bytes): 829440 - StateTransitionProtocol - TID=119885, CDNDownloadPollingThread
INFO - Content download progress percentage notification. ContentId : b4e1f138-b2d3-45bc-88e1-037b4bc08aa6, Content version: 1, Current download type: 0, percentage: 99, download source: CDN$https://CDNUS02.awmdm.com/cn800.airwatchportals.com/12074/Apps/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6.msi?token=st=1588264954~exp=1588351654~acl=/*~hmac=437a59c5085bce8b2b3f90a4e6cfcfdc76b6431debc963f6788babf2f95b3196, Lan download(in bytes): 0, Wan download(in bytes): 5212160 - StateTransitionProtocol - TID=119885, CDNDownloadPollingThread
INFO - Content download progress percentage notification. ContentId : b4e1f138-b2d3-45bc-88e1-037b4bc08aa6, Content version: 1, Current download type: 0, percentage: 100, download source: CDN$https://CDNUS02.awmdm.com/cn800.airwatchportals.com/12074/Apps/b4e1f138-b2d3-45bc-88e1-037b4bc08aa6.msi?token=st=1588264954~exp=1588351654~acl=/*~hmac=437a59c5085bce8b2b3f90a4e6cfcfdc76b6431debc963f6788babf2f95b3196, Lan download(in bytes): 0, Wan download(in bytes): 5230592 - StateTransitionProtocol - TID=119881, CDNDownloadThread [-10#b4e1f138-b2d3-45bc-88e1-037b4bc08aa6#1#false]
```

19. Once the content is downloaded, its hash is checked and then unpacked

```
INFO - Unpacking transaction log created for session : VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede - ContentDownloader - TID=6344, STP-SessionHandle=[VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede], Content Id=[b4e1f138-b2d3-45bc-88e1-037b4bc08aa6]
INFO - Unpacking content for session : VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede - ContentDownloader - TID=6344, STP-SessionHandle=[VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede], Content Id=[b4e1f138-b2d3-45bc-88e1-037b4bc08aa6]
INFO - Content unpacking successful for session : VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede - ContentDownloader - TID=6344, STP-SessionHandle=[VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede], Content Id=[b4e1f138-b2d3-45bc-88e1-037b4bc08aa6]
```

20. Finally, ContentDownload marks the download as complete and releases the RVP locks

```
INFO - Content download completed for content ID : b4e1f138-b2d3-45bc-88e1-037b4bc08aa6, for session handle : VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede - ContentDownloader - TID=6344, STP-SessionHandle=[VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede], Content Id=[b4e1f138-b2d3-45bc-88e1-037b4bc08aa6]
INFO - Released write lock for session : VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede - ContentDownloader - TID=6344, STP-SessionHandle=[VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede], Content Id=[b4e1f138-b2d3-45bc-88e1-037b4bc08aa6]
INFO - Released write lock for content : b4e1f138-b2d3-45bc-88e1-037b4bc08aa6 - ContentDownloader - TID=6344, STP-SessionHandle=[VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede], Content Id=[b4e1f138-b2d3-45bc-88e1-037b4bc08aa6]
```

21. The content is not only downloaded to the AdaptivaCache folder but to the AirWatchMDM AppDeploymentCache. This is visible in the ContentUpack.log

```
INFO - Copied file to: C:\ProgramData\AirWatchMDM\AppDeploymentCache\{B4E1F138-B2D3-45BC-88E1-037B4BC08AA6}\supportcenterinstaller.msi - ContentUnpacker - TID=6344, STP-
```

```
SessionHandle=[VMware$4b646f7c-8b02-11ea-8c16-00155d0a1ede], Content Id=[b4e1f138-b2d3-45bc-88e1-037b4bc08aa6]
```

22. Back in the AirWatch MDM log from the registry we can see AirWatch checking the contents that were placed into the cache

```
DeploymentPlan::EvaluateState SanitizeCache => STATE_INPROGRESS
DeploymentPlan::EvaluateState CacheConsistency => STATE_UNSTARTED
DeploymentPlan::OnAfterExecution SanitizeCache => STATE_TRUE
DeploymentPlan::EvaluateState CacheConsistency => STATE_INPROGRESS
CacheConsistencyExecItem::Execute: Cache is consistent. Download not needed.
DeploymentPlan::OnAfterExecution CacheConsistency => STATE_TRUE
DeploymentPlan::EvaluateState Transform => STATE_INPROGRESS
TransformCacheExecItem::Execute: Running cache transformation action
TransformCacheExecItem::Execute: Cache transformation complete.
DeploymentPlan::OnAfterExecution Transform => STATE_TRUE
```

23. Now that AirWatch MDM has confirmed the downloaded content, it will execute the command line that was provided in the app config

```
DeploymentPlan::EvaluateState ExecDeployment => STATE_INPROGRESS
DeploymentPlan::EvaluateState Executing now. Time: 2020-04-30T09:49:11-07:00
Execute: Running 'msiexec /i "supportcenterinstaller.msi" /qn'
Execute: Exec completed, ExitCode=0 (success code)
DeploymentPlan::OnAfterExecution ExecDeployment => STATE_TRUE
```

24. Since the installation returned success, the application is checked against the detection method to confirm it was installed

```
DeploymentPlan::EvaluateState FinalDetection => STATE_INPROGRESS
DetectionExecItem::Execute: Running Conditional detection {79C523EC-042E-420F-83FB-4CDB6B85CE15}
ConditionEvalExecItem::Execute: Evaluate(PRODUCTCODE) SUCCESS. {79C523EC-042E-420F-83FB-4CDB6B85CE15} TargetSID: S-1-5-18
DeploymentPlan::OnAfterExecution FinalDetection => STATE_TRUE
DeploymentPlan::EvaluateState FinalDetection - IsInstalled => true
DeploymentManager::OnStopExecutingEvent: Status code is: 80000902
```

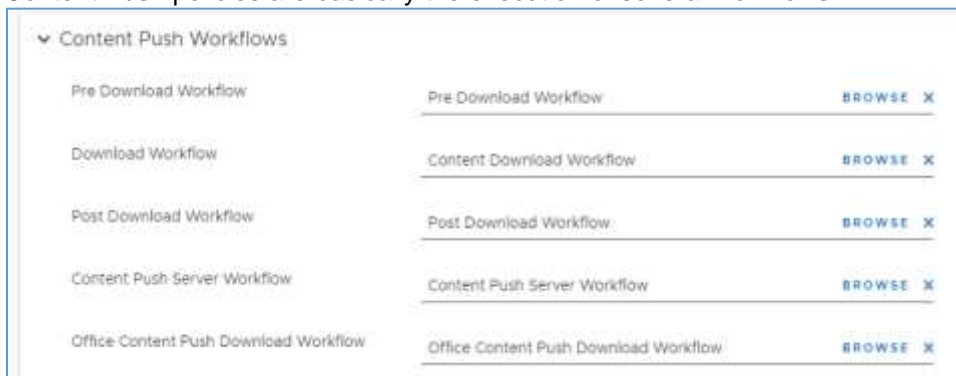
## Adaptiva Content

Adaptiva content is deployed to client devices using a content push policy. The content can be distributed, unpacked and executed, if desired, or any combination of the three. Users cannot request the content. Everything is run based on the defined schedule or executed by the administrator.

### Tracing the installation in the logs

It is important to understand what is happening in the logs if there is a problem during deployment so that it can be traced back to find a solution.

Content Push policies are basically the execution of several workflows.

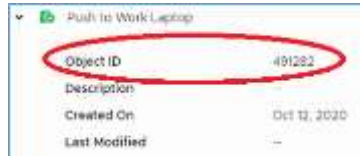


These were defined in the Content Push section

From a logging perspective the client will receive the policy assignment which will be logged in the Default Policy Assignment Client Workflow log showing which policy is being run.

After the content has been successfully downloaded, a post-download workflow will run. This workflow will execute the command line that was entered in the Content Push Policy

1. Obtain the Content Push Object ID, or the Policy ID, so that it can be traced on the client computer. The Content ID is also needed.
  - a. In the Adaptiva Web Portal, select the ellipses, ..., **More, Adaptiva Content, Content Push**. Click on the > next to the Content Push policy. The Policy ID needed is the Object ID.



In the Adaptiva Workbench, open the **OneSite – Content Push Perspective** and open the Content Push policy. Click on the Permissions tab to get the Policy ID



- b. To get the Content ID, in the Adaptiva Web Portal, select the ellipses, ..., **More, Adaptiva Content, Manage Content**. Click on the > next to the content item. The Adaptiva Content ID is what is needed.



In the Adaptiva Workbench, open the **Adaptiva Content Publication Perspective** to reach the Adaptiva Content Explorer. Right-click on the specific package and select **Edit Content Details** to get the Content ID



For this example, the Policy ID is: 491282. The Content ID being downloaded is TEST001

2. SentRecvMsg.log will show the policy being received after the Content Push policy is executed either by its schedule or manually.

```
INFO - Sender ID: 0. Correlation ID = 1600877735039 . message :Name of the message:
PolicyAssignment, Sender ID: 0, Receiver ID: 14, Queue ID: 1, CORRELATION ID:
1600877735039, ORIGINAL CORRELATION ID: 0, ORIGINAL RECEIVER ID: 1, REPLY TO: 1, REPLY TO
IP: /0.0.0.0, IS REPLY: false, PREF TRANSPORT: 0, RECV TRANSPORT: 5, Attribute count:
2Attribute names and their values: Name: PolicyID ,Value: 491282; Name: PolicyVer ,Value:
1; - ReceivingTask - TID=43161, ReceivingTask: Sender Id = [/0.0.0.0]
```

3. ContentDownload.log will then show the policy and workflows being downloaded

```
INFO - Write locks acquired for for session : ContentPush$491282$TEST001 and contents :
[TEST001] - ContentDownloader - TID=43175, Pooled Thread -
com.adaptiva.workflow.model.LauncherRunnable@3dc322
```

4. In SentRecvMsg.log The normal election process will be held to determine if this content is available on the subnet locally, or if it will need to be retrieved from the parent office, an internet-based peer or from the CDN.

**NOTE: When the client is on the internet, it will be treated as if it is in a Wi-Fi location/office**

```
INFO - Attempting to send (WiFi): Receiver ID: -1, Receiver IP: null, MsgLen: 636,
Correlation ID = 1600312622839 port: 34329, transport:
com.adaptiva.transport.WifiUDPTransport@1df276f, Message :Name of the message:
P2PDiscoveryRequest, Sender ID: 14, Receiver ID: 1, Queue ID: 1, CORRELATION ID: 0,
ORIGINAL CORRELATION ID: 0, ORIGINAL RECEIVER ID: 1, REPLY TO: 1, REPLY TO IP: null, IS
REPLY: false, PREF TRANSPORT: 0, RECV TRANSPORT: 2, Attribute count: 23Attribute names
and their values: Name: RequestID ,Value: 60129542145; Name: NoOfConditions ,Value: 4;
Name: FieldID0 ,Value: 1; Name: Operator0 ,Value: 1; Name: Value0 ,Value: Content; Name:
CaseInsensitive0 ,Value: 1; Name: FieldID1 ,Value: 2; Name: Operator1 ,Value: 1; Name:
Value1 ,Value: TEST001; Name: CaseInsensitive1 ,Value: 1; Name: FieldID2 ,Value: 3; Name:
Operator2 ,Value: 1; Name: Value2 ,Value: 2; Name: CaseInsensitive2 ,Value: 1; Name:
FieldID3 ,Value: 4; Name: Operator3 ,Value: 4; Name: Value3 ,Value: 0; Name:
CaseInsensitive3 ,Value: 1; Name: MaxResponses ,Value: 4; Name: SpreadDuration ,Value:
4000; Name: NewVersion ,Value: ; Name: _SERVER_GUID_ ,Value: 8efe3c8a-9aac-11ea-97f0-
00155d0ale8a; Name: _WiFi_ ,Value: ; - SendingThread - TID=130, SendingThread: [Receiver
Id= -1]
```

5. In ContentDownload we can see the download start.

```
INFO - Starting download for : TEST001 - ContentDownloader - TID=43175, Pooled Thread -
com.adaptiva.workflow.model.LauncherRunnable@3dc322
```

6. Now filter ContentDownload on **CDN\$** or **INT\$**, if the content is coming from the internet, or **AN\$** to see if the content is coming from the LAN or WAN.

```
INFO - Content download progress percentage notification. ContentId : TEST001, Content
version: 2, Current download type: 0, percentage: 100, download source:
CDN$https://storageaccount.blob.core.windows.net/container/Adaptiva/TEST001/79CF08D9-
11AE-17AF-4E2E-2AB068D4405A/TEST001.2.content, Lan download(in bytes): 0, Wan download(in
bytes): 589824 - StateTransitionProtocol - TID=43266, CDNDownloadThread
[ContentPush$491282$TEST001]
```

7. Once the content is downloaded, its hash is checked and then unpacked. Notice it is unpacked to the location specified in the Content Push policy

```
INFO - Unpacking content for session : ContentPush$491282$TEST001 - ContentDownloader -
TID=43179, STP-SessionHandle=[ContentPush$491282$TEST001], Content Id=[TEST001]
set LastUnpackedFolderPath in contentState to: C:\Windows\TEMP\unpackedContent, taken from session :
ContentPush$491282$TEST001 - ContentDownloader - TID=43179, STP-
SessionHandle=[ContentPush$491282$TEST001], Content Id=[TEST001]
INFO - Content unpacking successful for session : ContentPush$491282$TEST001 -
ContentDownloader - TID=43179, STP-SessionHandle=[ContentPush$491282$TEST001], Content
Id=[TEST001]
```

8. Finally, ContentDownload marks the download as complete and releases the RVP locks.

```
INFO - Content download completed for content ID : TEST001, for session handle : ContentPush$491282$TEST001 -
ContentDownloader - TID=43179, STP-SessionHandle=[ContentPush$491282$TEST001], Content Id=[TEST001]
INFO - Released write lock for session : ContentPush$491282$TEST001 - ContentDownloader - TID=43179, STP-
SessionHandle=[ContentPush$491282$TEST001], Content Id=[TEST001] INFO -
```

9. After the content has been unpacked, the post download workflow will execute the command line

Post Download Workflow #####\_####

```
Prop: CmdShell1.Command, TEXT, Old: none, New: C:\Windows\system32\msiexec.exe /i Orca-
x86_en-us.msi /qn /log C:\Windows\temp\Install_Orca.log
Exec: Starting: Start1.Try1.MainTry1.If2.True2.CmdShell1
```

10. If there is logging with the execution, that can then be monitored