
Adaptiva Platform Installation Guide

Updated: April 9, 2025

OneSite Anywhere

- Configuration Manager
- Intune
- Workspace ONE
- OneSite Patch
- OneSite Health
- OneSite Wake

Table of Contents

Legal Notices	4
Introduction	5
Deployment Planning – General	6
Adaptiva Platform Components	6
Adaptiva Server Hardware Requirements.....	6
Database Considerations.....	6
Firewall and Communication Ports	8
Antivirus Exceptions.....	8
Accounts and Permissions.....	10
Certificates for the Adaptiva OneSite Admin Portal.....	10
Deployment Planning – OneSite Anywhere	11
Design Considerations – OneSite Anywhere	11
Accounts and Permissions.....	11
Internet Access	11
Admin Portal Communications.....	12
HTTP Communications.....	12
Additional Planning – OneSite ConfigMgr Edition	14
Design Considerations - ConfigMgr	14
Accounts and Permissions.....	16
Additional Planning – OneSite for Workspace ONE.....	18
Design Considerations – Workspace ONE	18
Accounts and Permissions.....	19
Installation Prerequisites	20
Certificates	20
Database Reporting Account	20
SQL Express.....	20
SQL Express pre-installed	21
SQL permissions.....	22
Server Activation.....	23
App Registration	24
Workspace ONE	27
(Deprecated) Azure Storage	29
OneSite Platform Installation.....	38
Prerequisites.....	38
Prepare the Installation Files	38
Launch the Adaptiva Server Installer	39
Configure Installation Settings	40
Configure TLS Security Settings and Client Count	41
Integrate Third Party Products	42
Integrate an Existing Microsoft ConfigMgr Site	43
Specify Login Information for Accessing Site Server Files.....	46
Integrate with Workspace ONE.....	47
Options For Creating the Adaptiva SQL Database	47

Download and Install Free Microsoft SQL Express And Auto-create Adaptiva Database.....	48
Create The Adaptiva Database In An Existing SQL Server Instance.....	49
Create the Adaptiva Database In The Same SQL Instance As ConfigMgr	51
Read-Only SQL Login For Adaptiva Reporting	52
Completing the Installation.....	52
Adaptiva Client Installation on the Server	54
Server Installation Log	55
Create Silent Installation Answer file.....	55
Post-Install Instructions.....	57
Workbench Installation.....	61
Installing the License Key	63
(Optional) Post Installation Tasks	66
Client Installation.....	73
Upgrading	110
Server Upgrade.....	111
Client Upgrade	115
Uninstallation.....	120
OneSite Backup and Recovery	121
Overview.....	121
Prerequisites (ConfigMgr)	121
Scenarios.....	121
Backup.....	121
Restore	124
Appendix A: Communication Ports.....	126
List of All Adaptiva Ports	126
Communication Port and Flow Diagrams.....	127
Additional Firewall Rules.....	131
Appendix B: SPNs and Delegation.....	133
Create the SPNs	133
Delegate Kerberos authentication.....	134
Confirm the Configuration	134
Create the Linked Servers	134
Test the Linked Servers	135
Appendix C: Optional Configuration Activities	136

Legal Notices

The information in this document is proprietary and confidential to Adaptive Protocols, Inc. (Adaptiva) and provided to customers for their internal use only. No part of this document may be reproduced or redistributed in any form without the prior written consent of Adaptiva.

All information supplied here is subject to change without notice. Contact Adaptiva to request the latest OneSite specifications and designs.

Adaptiva reserves the right to amend the product(s) or information disclosed herein at any time without notice. Adaptiva does not assume any responsibility or liability arising out of the application or use of any product or service described herein, except as expressly agreed to in writing by Adaptiva.

Any brand and/or product names mentioned may be trademarks of their respective companies.

Corporate Headquarters

Kirkland, WA +1 (425) 823-4500

Copyright © 2022-2024 Adaptiva

Adaptive Protocols, Inc.

All Rights Reserved

E-mail

info@adaptiva.com

Website

www.adaptiva.com

Introduction

Adaptiva products are known for their simplicity and ease of installation. This guide explains how to install the Adaptiva Platform components, which includes the Adaptiva server service, management workbench and the Adaptiva Client agent. The installation is the same for all Adaptiva products since they are all built upon the Adaptiva Platform. The server setup process installs components shared between OneSite Anywhere, OneSite for ConfigMgr, OneSite for Intune, OneSite for Workspace ONE, OneSite Patch (formerly Autonomous Patch), OneSite Health (formerly Endpoint Health) and OneSite Wake (formerly Endpoint Wakeup); adding a valid license key will enable the features of the product(s). The Adaptiva Server will be installed first (which will include the Adaptiva Client on the server), followed by the workbench and finally, the endpoint devices.

The products also uninstall cleanly and leave no files or database entries behind.

Deployment Planning – General

The following sections detail architectural pre-requisites and recommendations for the deployment of Adaptiva.

Adaptiva Platform Components

There are 4 main components to the Adaptiva platform:

- Adaptiva Server Component
- SQL Database – while not an Adaptiva component, it is required
- Adaptiva Workbench Component
- Adaptiva Client Component

Adaptiva Server Hardware Requirements

The following details the minimum server hardware requirements for installing the Adaptiva Server component.

Component	Minimum Requirement
Operating System	Windows Server 2016 Standard or Datacenter Edition and above.
Processor	Single Quad-core Xeon Processor
RAM	32GB
Memory Allocation for the Adaptiva Server	0 to 5,000 clients – 2048 MB 5,001 to 10,000 clients – 3072 MB 10,001 to 19,999 – 5120 MB 20,000 to 49,999 – 6144 MB 50,000 and above - 8192 MB Recommendation: When integrated with Configuration Manager and Endpoint Protection is enabled, double the above values.
Storage	Installation Files – 1.5GB (for Server, Client, & Workbench) Logging – 5GB for default logging retention

Database Considerations

The Adaptiva server requires its own SQL Server database. The Adaptiva database can be hosted on the same database server as the Configuration Manager database or a stand-alone, free version of SQL Server, SQL Server Express, can be used. If hosting with the Configuration Manager database, be aware of the licensing requirements. If SQL Server Express is chosen, it can be pre-installed, or select it during installation, where it will be automatically downloaded and installed on the server. Using SQL Server Express will suffice for most but the largest environments.

See the section below on [Choosing the SQL Edition](#) to understand the implications of using SQL Express.

The Adaptiva database can be hosted on a local installation or in a SQL Server AlwaysOn Availability Group on remote servers.

SQL Requirements

Component	Requirement
SQL Server Version	SQL Server 2022: Express, Standard, Enterprise SQL Server 2019: Express, Standard, Enterprise SQL Server 2017: Express, Standard, Enterprise SQL Server 2016 SP2: Express, Standard, Enterprise IMPORTANT: The Database Compatibility Level must be SQL 2016 (130) or newer

Database Sizing	Base Database size is 5GB plus a storage allocation equal to approximately 200KB per managed device. When using OneSite Health or OneSite Patch, Storage allocation per managed device is approximately 2.5MB per each solution. NOTE: SQL Server Express Edition will support up to approximately 2000 devices.
Memory	Server should have a minimum of 64GB of RAM. OneSite Patch requires a minimum SQL Server memory configuration of 8GB.
Disk infrastructure	Recommended: SSD or NVMe drives for the database files.
Local Security Policy	Network security: Restrict NTLM: Incoming NTLM traffic must be set to Allow all when using a domain account for the Adaptiva reporting account used with the Adaptiva OneSite Admin Portal.

Choosing the SQL Edition

Using SQL Server Standard Edition is recommended.

Enterprise Edition is required if High Availability will be used.

SQL Server Express Edition can be used in all but the largest environments, except when using OneSite Patch. The following lists the main limitations of the Express Edition. A large environment would be those with 50,000 devices or more.

- No Built-In Scheduled Backups (work around available)
- Maximum Memory - 1410MB
- Database Size Limit – 10GB
- Maximum Number of Cores – 1 socket, up to 8 Cores
- No High Availability
- SQL Server Reporting Services (SSRS) is only available with SQL Express with Advanced Services

For a full list, reference: <https://www.microsoft.com/en-us/sql-server/sql-server-2022-comparison>

Choosing SQL Server Express Edition

When choosing SQL Server Express Edition, it can be downloaded and installed as part of the installation. Having the Adaptiva Server Setup perform the installation of SQL Server Express Edition does bring with it the following considerations:

- With build 8.3 and later, the Installer will download and install SQL Server 2022 Express Edition.
- Installer will not install SQL Server Management Studio
- Installer will configure all necessary settings. If SQL Server Express Edition is installed manually, additional configuration is required – reference the table below.
- Installer will name the instance **AdaptivaSQL**.

SQLEXPR_x64_ENU.exe can be pre-downloaded and placed in the specified download folder. For build 8.3 and later, the file size must match exactly 279,293,816 bytes (version 2022) for the AdaptivaServerSetup to install it.

When choosing to install SQL Server Express Edition prior to the installation of Adaptiva, there are a few steps that must be completed to ensure that it will work correctly.

Configuration	Steps to Implement
TCP/IP connections must be enabled	<ol style="list-style-type: none"> 1. Open SQL Server 20## Configuration Manager 2. Expand SQL Server Network Configuration (not 32-bit), and select Protocols for MSSQLSERVER or the Instance name used 3. Enable TCP/IP if not already 4. Shared Memory should also be enabled, while Named Pipes can stay Disabled
Enable SQL Server Browser	<ol style="list-style-type: none"> 5. Select SQL Server Services 6. Right-click SQL Server Browser and select Properties 7. Confirm the Log on as setting is set for the Built-in account: Local Service 8. Click on Start
Grant Local System account Sysadmin role.	<ol style="list-style-type: none"> 9. Install SQL Server Management Studio

Permissions can be reduced after installation	10. If the account does not exist under Security, Logins run the following T-SQL command: <pre>CREATE LOGIN [NT AUTHORITY\SYSTEM] FROM WINDOWS WITH DEFAULT_DATABASE=[master], DEFAULT_LANGUAGE=[us_english]; ALTER SERVER ROLE [sysadmin] ADD MEMBER [NT AUTHORITY\SYSTEM];</pre>
-----------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

SQL Licensing

Appropriate SQL licenses must be purchased unless SQL Server Express will be used. Always consult with a Microsoft licensing specialist to ensure the proper licenses have been purchased.

Firewall and Communication Ports

As a network application facilitating activity between server and clients, as well as between clients and other clients, certain ports must be open or allowed to enable communication. For a list of required ports, refer to [Appendix A: Communication Ports](#) at the bottom of this document or the file **AdaptivaPortDetail.pdf** in the product download source.

The ports listed should be excluded from any network filtering or intervening network security devices to prevent a disruption in network communication. Adaptiva setup creates Windows Firewall rules in the currently connected profile for these ports automatically when installed. If ports are customized which are used by the Adaptiva server, client, or workbench, or use other firewalls or security software between the server, workbench or clients, then these ports must be manually configured as rules or exceptions in the firewall to enable the necessary communication.

Antivirus Exceptions

Adaptiva OneSite acquires content directly from the site server content library, and therefore, we follow the Microsoft recommendation that Antivirus scanning should be performed on the package source files. However, Adaptiva folders themselves should be excluded from scanning to prevent a degradation in performance. All Adaptiva content that is distributed uses a secure hash to ensure content is not tampered with, corrupted in transit, or when stored.

NOTE: The folders listed below are the parent folders. Ensure all subfolders are included in the exclusion.

Folder Exclusions

Adaptiva Server Exclusions

Description	Folder Exclusion
Server Installation Folder	<path>\Adaptiva\AdaptivaServer
Adaptiva Content Library (if different from the default location)	The location in which the Adaptiva content library will be located
Client Installation Folder	<path>\Adaptiva\AdaptivaClient

Client Exclusions (Client and Server Operating Systems)

Description	Folder Exclusion
Client Installation Folder	C:\Program Files\Adaptiva (Default) When using AdaptivaClientSetup32.exe on 64-bit operating systems the path will be: C:\Program Files (x86)\Adaptiva (or custom location)
Adaptiva Content Cache	\AdaptivaCache (exists at the root of every fixed logical drive by default)

ConfigMgr Exclusions (Client and Server Operating Systems)

If using Adaptiva OneSite with ConfigMgr, the following exclusions should already be in place and are being provided here for completeness:

Description	Folder Exclusions
ConfigMgr Client Folder Exclusions	%windir%\CCM*.sdf %windir%\CCM\Logs %windir%\CCM\ServiceData %windir%\CCM\Cache %windir%\CCM\Setup It is also recommended to exclude the following for the Windows Update agent %windir%\SoftwareDistribution*

Intune Exclusions

If using Adaptiva OneSite with Intune, the following exclusions should already be in place and are being provided here for completeness:

Description	Folder Exclusions
Intune Management Extension Exclusions	C:\program files (x86)\Microsoft Intune Management Extension\Content %windir%\IMECache

Process Exclusions

Some Security Administrators would prefer to exclude processes rather than folders. Process exclusions are necessary only if aggressive antivirus programs consider the executables to be a high-risk process. See the tables below.

Adaptiva Server Exclusions

Description	Process Exclusion
Server Service	<path>\Adaptiva\AdaptivaServer\bin\AdaptivaServerService.exe <path>\Adaptiva\AdaptivaServer\cloud-ui\node-adaptiva.exe <path>\Adaptiva\AdaptivaServer\cloud-ui\nginx-html\nginx-adaptiva.exe
Client Service	<path>\Adaptiva\AdaptivaClient\bin\AdaptivaAIT.exe <path>\Adaptiva\AdaptivaClient\bin\AdaptivaClientService.exe <path>\Adaptiva\AdaptivaClient\bin\AdaptivaUserPortal.exe <path>\Adaptiva\AdaptivaClient\bin\OneSiteClient64.exe

Client Exclusions (Client and Server Operating Systems)

Description	Process Exclusion
Client Service	C:\Program Files\Adaptiva\AdaptivaClient\bin\AdaptivaAIT.exe C:\Program Files\Adaptiva\AdaptivaClient\bin\AdaptivaClientService.exe C:\Program Files\Adaptiva\AdaptivaClient\bin\AdaptivaUserPortal.exe C:\Program Files\Adaptiva\AdaptivaClient\bin\OneSiteClient.exe C:\Program Files\Adaptiva\AdaptivaClient\bin\OneSiteClient64.exe C:\Program Files\Adaptiva\AdaptivaClient\bin\amd64\OneSiteDownloader.exe

ConfigMgr Exclusions (Client and Server Operating Systems)

Description	Process Exclusion
Client Exclusions	%windir%\CCM\CCMExec.exe %windir%\CCM\CMRCSservice.exe

Accounts and Permissions

The Adaptiva Server installation requires the installation account to have local administrator permissions on the chosen server. The installation will create a local service named **AdaptivaServer** and by default, that service will run under the Local System account.

The installation account must also have sysadmin permissions on the SQL Server where the database is to be hosted. This permission can be changed after the installation.

Depending on which Adaptiva product is enabled, additional accounts and permissions may be required. Refer to the **Accounts and Permissions** topic in the specific section.

After installation, optionally, the service account can be changed from local system to a specified service account.

The following table summarizes the permissions that must be granted to the service account running the Adaptiva Server service.

Server	Account	Permissions
Adaptiva Server	Installation account Optional Service account or System Account Reporting account	Local Administrators group The account must be granted the Log On As A Service User right Server Setup will automatically grant db_datareader permissions
SQL Server hosting Adaptiva database	Installation account Optional Service account or System Account	SQL Server Role Sysadmin (Installation account for initial installation) Minimum permissions Adaptiva Database Security User Mapping (account running Adaptiva Server Service) db_datareader db_datawriter db_ddladmin db_executor
Content Library	<domain>\<AdaptivaServer>\$ or Optional Service account	If the Adaptiva Content Library is to be relocated to a remote drive/share, the Adaptiva Server service account will need Modify permission to this location.

Certificates for the Adaptiva OneSite Admin Portal

Starting in Build 8.2 the Adaptiva Server will default to enabling TLS for the Admin Portal via a self-signed certificate. Alternatively, a certificate authority can be used. The certificate authority can be a 3rd party, like GoDaddy, DigiCert or Let's Encrypt, or you can use Active Directory Certificate Services.

Consider the following when deciding which certificate or certificate service to use:

- Does your Security department have any requirements that must be met when using Certificates?
Self-signed certificates vs a provided Certificate
Wildcard certificates vs Certificate specific to a server
Key size and Hash algorithm and expiry length requirements
NOTE: The self-signed certificate created by default as part of the Adaptiva Server Setup is 4096 bits, using SHA-512 hash and will expire in 12 years
- How many Administrators on remote devices will be using the Admin Portal?

Every remote device will need the certificate installed into their certificate store in order to securely access the Admin Portal. This can be done manually or via GPO or Intune Profile.

Deployment Planning – OneSite Anywhere

Consider the following when implementing OneSite Anywhere.

This design planning is also required when using Adaptiva OneSite Anywhere with Microsoft Endpoint Manager – Intune.

Design Considerations – OneSite Anywhere

The Adaptiva Server component will run on a server in the central office. SQL Server would also be installed on this server.

Single Server

Installing Adaptiva and SQL Server on a single server is the simplest configuration and provides the benefit of eliminating any network communications between the components. Often, this is used when SQL Express will be installed on the same server with Adaptiva.



Adaptiva OneSite Server with SQL

Two Servers

In this configuration, SQL Server is on its own server. For many customers, this is ideal when the database administration team requires that all databases be installed and maintained on managed servers. One of the advantages here is that often these SQL servers will be clustered or use Always On Availability Groups.



Adaptiva OneSite Server



SQL Server

Accounts and Permissions

No additional permissions are required

Internet Access

The Adaptiva server must be able to access the internet. Specifically, the server will need to get to URLs formatted as: https://*.adaptiva.cloud. This is an outbound connection only and will use TCP ports 80 or 443. The following Request Methods are required and may need to be explicitly allowed when using a proxy:

HEAD, GET, POST, and DELETE

The Adaptiva Server and internet-based clients need to be able to connect to the following internet destinations:

Source	Description	Destination	Port
Adaptiva Server	Adaptiva Services	*.adaptiva.cloud	http/https (TCP port 80, 443), ICMP, UDP 3478
Internet-based Clients		*.opendns.com	

Adaptiva Server	Approval Messaging, email and sms messages	Api.sendgrid.com Api.twilio.com ¹	https (TCP port 443)
-----------------	--------------------------------------------	-------------------------------------------------	----------------------

When using the Adaptiva CDN for storage:

Adaptiva Server Internet-based Clients	Adaptiva CDN	*.adaptivacd.cloud	http/https (TCP port 80, 443)
Adaptiva Server	CDN Storage	*.bunnycdn.com OR *.amazonaws.com (to be deprecated by end of 2024)	http/https (TCP port 80, 443)

When using the Adaptiva OneSite Patch Solution, the Adaptiva server or CDN-enabled devices will, by default, download from the 3rd party vendor location. The server and internet-capable clients must be able to reach these 3rd-party locations. Also, if additional solutions have been added for Crowdstrike, Defender or Tenable:

Adaptiva Server	Crowdstrike vulnerability manager	<region>.crowdstrike.com <region> is where the tenant's instance is hosted. E.g. api.us-2.crowdstrike.com. For more information go here . (A login is required)	https (TCP port 443)
Adaptiva Server	Microsoft Defender	<region>.api.security.microsoft.com <region> is * or the server closest geographically. For more information go here .	https (TCP port 443)
Adaptiva Server	Tenable Vulnerability Management	Cloud.tenable.com	https (TCP port 443)

If Azure storage is to be used instead of the Adaptiva CDN:

Adaptiva Server Internet-based Clients	Azure storage	*.windows.net	https (TCP port 443)
-------------------------------------------	---------------	---------------	----------------------

If Microsoft Endpoint Management – Intune is being used:

Adaptiva Server All Clients	Azure (for Intune)	*.microsoft.com *.windows.net	https (TCP port 443)
--------------------------------	--------------------	----------------------------------	----------------------

Admin Portal Communications

The introduction of OneSite Anywhere (version 8.0) will also install the new Admin Portal. By default, the Admin Portal will use the standard http TCP port 80, https TCP port 443 is available when using a certificate. The Admin Portal does not require Microsoft Internet Information Server (IIS). If there are other services listening on port 80 a different port must be entered during installation. Run `NETSTAT -nabo` to get a current list of ports that are being used.

HTTP Communications

Determine if the managed clients cannot communicate to the Adaptiva Server using UDP. Clients cannot use UDP when their IP Address is NAT'd. For example, when using cloud-based VPN products like ZScaler or when using Microsoft's Direct Access. The Adaptiva Server can be configured to allow binding on HTTP. By default, this will use port 80.

¹ We use an external vendor Twilio (and SendGrid, owned by Twilio) to send notification texts and emails, respectively, for alerts such as patch approvals or password change requests. Per their documentation, they do retain message content for a brief period of time, but we do not send any personal identification information over these channels.



If the Adaptiva Server will be installed on a server with the Web Server role or with SQL Server Reporting Services installed, a different port will be required, or choose to install Adaptiva Server on a different server.

Additional Planning – OneSite ConfigMgr Edition

Adaptiva OneSite integrates with Microsoft Endpoint Manager - Configuration Manager (ConfigMgr). The placement of the Adaptiva Server services may vary based on the design and configuration of the ConfigMgr environment.

Design Considerations - ConfigMgr

ConfigMgr Single Primary Site

Single Server

Integrating OneSite and a single ConfigMgr Primary Site is the simplest configuration. In this scenario, the Adaptiva Server will be installed on the same server which hosts the ConfigMgr Primary Site Server and SQL database.



Primary Site Server with SQL and Adaptiva

Separate Servers

Another option is to install the Adaptiva Server on a separate server. This is usually done where there is a security requirement to isolate applications, for example, when ConfigMgr High Availability is used. However, consideration should be made about the database placement. See **Database Considerations** section.



Primary Site Server with SQL



Adaptiva OneSite Server

ConfigMgr with CAS and Primary Sites

When installing Adaptiva in an environment with a Central Administration Server (CAS) and one or more Primary Site Servers, there are two options for where to install the Adaptiva Server. There are pros and cons to both scenarios which are addressed below.

Adaptiva Server Installed on CAS and All Primary Site Servers

This is the most common approach as each Adaptiva Server is integrated with their respective ConfigMgr server. In this scenario, devices which are managed by a given Primary Site server will also be managed by the Adaptiva Server installed on that site server. Adaptiva is installed on the CAS for visibility of policies and publication of content which originate on the CAS. This configuration is required when content and/or deployments are sourced at any of the Primary Site servers. Depending



Central Administration Server with SQL and Adaptiva



Primary Site Server with SQL and Adaptiva



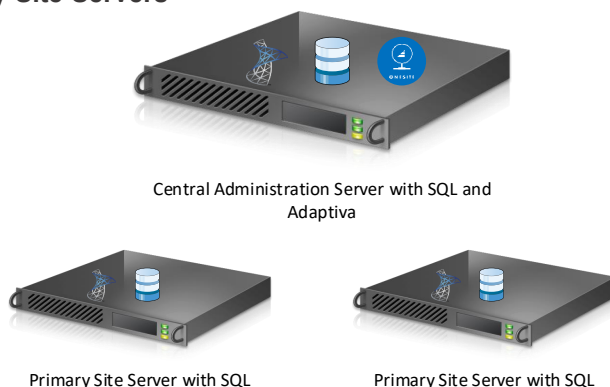
Primary Site Server with SQL and Adaptiva

on the use of Adaptiva, the administrative overhead of this configuration may be higher than other options, as there is no hierarchy in the Adaptiva platform.

Adaptiva Server Installed on CAS, but not Primary Site Servers

With this approach, the Adaptiva Server is only installed on the CAS Site Server and not the Primary Site servers. Even though ConfigMgr clients will report to their respective Primary sites, the Adaptiva clients on those devices will report into the Adaptiva Server on the CAS. Although this option may result in less administrative overhead, for this configuration to work all content and deployments must be sourced at the CAS. Any content or deployments sourced at the Primary Site servers will not be detected by Adaptiva.

NOTE: The Adaptiva OneSite feature Policy Bandwidth Management will not function in this configuration. Since policy changes are detected at the Primary Sites and not the CAS, the Policy Bandwidth Manager component will not be able to detect applicable policy changes.



Additional Server Considerations

- It is recommended that the Adaptiva Server be installed on the ConfigMgr site server itself. If installation on the site server is not possible (for technical or political reasons) install on a server within close proximity (network-wise) to the site server
- Disk space is required to store Adaptiva or ConfigMgr content

Content Library Storage	In addition to the general storage requirements, Adaptiva OneSite requires disk space to store its published content in the Content Library. The estimated size will be the same amount of storage estimated/being used for the content source files plus 20% for policy files and diff files. If using ConfigMgr, use the Content Source folder(s) to estimate the size as this is not compressed. Adaptiva will also compress the content that is stored in its Content Library.

Additional Database Considerations

Linked Servers

Because the Adaptiva server uses a separate database, it is necessary to create a link between the ConfigMgr database and the Adaptiva database to enable cross-database reporting. The Adaptiva server setup (discussed below in the Server Installation section) will create the necessary links in only one of the following two scenarios:

1. **Adaptiva and ConfigMgr databases share same SQL Server but use separate instances:** The Adaptiva server setup will create two links, one in each instance linking to the other instance. The links will be named using the fully qualified domain name (FQDN) of the SQL Server system hosting the default instance or the instance name for a named instance.

For example, if the FQDN of the server is SQL-123.MyOrg.MyDomain.com, and the default instance is used then the link in the other instance will be named SQL-123.MyOrg.MyDomain.com. Likewise, if the database is in an instance named Instance1 on the SQL-123 server described earlier, then the link in the other instance will be named SQL-123.MyOrg.MyDomain.com\Instance1.

2. **Adaptiva and ConfigMgr databases hosted by separate SQL Servers:** Links must be manually created in each instance of SQL Server prior to installing the Adaptiva server. The linked server name on Server A must be the FQDN (with instance name if needed) of the other SQL Server, and vice versa. Server setup will verify link existence and proper permissions before installation is successfully completed.

To create a linked server, see the instructions in Appendix B: SPNs and Delegation. Also, additional information can be found here: <https://docs.microsoft.com/en-us/sql/relational-databases/linked-servers/create-linked-servers-sql-server-database-engine?view=sql-server-ver15>

Accounts and Permissions

For integration with ConfigMgr, Adaptiva needs to have the relevant permissions to ConfigMgr. The default configuration during installation will specify: Use Adaptiva Server's Local System Account for the ConfigMgr Site Login. If this is used, no additional changes are required.

The following table summarizes the additional permissions that must be granted to any service account running the Adaptiva Server service. Instructions are also provided on how to make these changes in SQL Management Studio.

Server	Account	Permissions
Adaptiva Server	Optional Service account	The account must be granted the Log On As A Service User right
ConfigMgr Site Server	System Account of Adaptiva Server Optional Service account	Local Administrators group
SQL Server hosting ConfigMgr database	Installation account Optional Service account	During installation, the installation account must be either sysadmin or db_owner for the ConfigMgr database Minimum permissions (after installation) ConfigMgr Database Security User Mapping (optional service account) db_datareader db_datawriter db_ddladmin db_executor
SQL Server hosting Adaptiva database	ConfigMgr Reporting Services Point account	Adaptiva Database Security User Mapping db_datareader
In a CAS environment: SQL Server hosting child Primary database	System Account of Adaptiva Server Optional Service account	During PXE usage, the SQL account used by the CAS SQL database server must be able to access the child Primary database Minimum permissions (after installation) ConfigMgr Database Security User Mapping db_datareader db_datawriter db_executor
ConfigMgr Security	System Account of Adaptiva Server Optional Service account	It is not recommended to grant any accounts/groups the Full Administrator role. The minimum permissions are provided below: <input type="checkbox"/> Import the attached Security role or Create a custom Security Role named Adaptiva Administrator based on the default role, Read-Only Analyst , <input type="checkbox"/> ADD the below permissions OR https://Adaptiva.Cloud/Builds/Tools/Adaptiva%20Administrator.xml Application - Create, Delete, Modify, Modify Report Boot Image Package - Create, Delete, Modify Collection - Create, Delete, Delete Resource, Modify, Modify Collection Setting, Modify Resource Driver Package - Create, Delete, Modify Operating System Image - Create, Delete, Modify

		<p>Operating System Upgrade Package - Create, Delete, Modify Package - Create, Delete, Modify, Modify Report Query - Create, Delete, Modify Site - Modify, Modify Report Software Updates - Modify Report Status Messages - Create, Delete, Modify Report Task Sequence Package - Modify Report</p> <p><input type="checkbox"/> Add the custom role to the optional service account to be used when adding an Administrative User.</p> <p><input type="checkbox"/> If custom Security Scopes are used, select All instances of the objects that are related to the assigned security roles</p>
Inboxes (SMS_<sitecode> share location)	System Account of Adaptiva Server Optional Service account	If not in the local Administrators group, account must have Full Control to \\<ConfigMgrSiteServer>\SMS_<sitecode>\inboxes
Content Library	System Account of Adaptiva Server Optional Service account	If not in the local Administrators group, account must have at least Read-only permissions to Content Library as specified by the ConfigMgr Site Server (SCCMContentLib folder)

Additional Planning – OneSite for Workspace ONE

Design Considerations – Workspace ONE

The Adaptiva Server component will run on a server in the central office. For many customers, it is ideal to install the Adaptiva Server on the same server as the AirWatch Cloud Connector (ACC) since these are the only two components that need to communicate with each other. The ACC will contact the Adaptiva Server by calling the Adaptiva APIs that are installed. SQL Server would also be installed on this server. This also ensures the security of the platform as there is no access from outside the network to the Adaptiva Server.

Single Server

Integrating the ACC and Adaptiva components on the same server is the simplest configuration and provides the benefit of eliminating any network communications between the components.



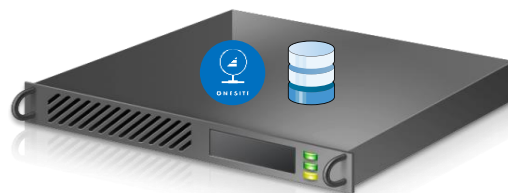
AirWatch Cloud Connector with SQL and
Adaptiva

Two Servers

In this configuration, the ACC is on its own server. Adaptiva is installed on its own server along with the SQL database. Often, this is used when SQL Express will be installed on the same server with Adaptiva.



AirWatch Cloud Connector



Adaptiva OneSite Server with SQL

Completely Isolated

If all components should be completely isolated, each can be installed on their own server. For many customers, this is ideal when the database administration team requires all databases be installed and maintained on managed

servers. One of the advantages here is often these SQL servers will be clustered or use Always On Availability Groups.



AirWatch Cloud Connector



Adaptiva OneSite Server



SQL Server

Accounts and Permissions

Server	Account	Permissions
Airwatch Cloud Connector	Airwatch Service Account	Registry Full Control access: HKLM\Software\Adaptiva HKLM\Software\Microsoft\SystemCertificates File System Read access: Location of Adaptiva DLLs (C:\Program Files\Adaptiva)

Installation Prerequisites

Certificates

Starting in Build 8.2 the Adaptiva Server will default to enabling TLS for the Admin Portal via a self-signed certificate. Alternatively, a certificate authority can be used.

If a certificate authority will be used, use the steps below to ensure the certificate and the key are in the correct PEM format. Certificates are usually provided as .pfx files. These need to be converted into .pem files with a separate file for the certificate and for the key. Also, the files must be in UTF-8 format.

When requesting the certificate from the certificate authority be sure to export the key as well.

To convert the .pfx file to a .pem file that can be used by the AdaptivaServerSetup.exe use the following powershell script (update the path as needed):

```
$pfxFilePath      = '<path>\certificate.pfx'
$outputpemFilePath = 'c:\admin\webportalcert\Output.pem'
$pemFilePath       = 'c:\admin\webportalcert\key.pem'
$cerFilePath       = 'c:\admin\webportalcert\cert.pem'

Install-Module -Name PSPKI
import-module PSPKI
Convert-PfxToPem -InputFile $pfxFilePath -Outputfile $OutputpemFilePath
(Get-Content $OutputpemFilePath -Raw) -match "(?ms)(\s*((?<privatekey>-----BEGIN PRIVATE
KEY-----.*?-----END PRIVATE KEY-----)|(?<certificate>-----BEGIN CERTIFICATE-----.*?-----
END CERTIFICATE-----))\s*){2}"
$Matches["privatekey"] | Set-Content $pemFilePath
$Matches["certificate"] | Set-Content $cerFilePath
```

You now have the necessary files to use during Adaptiva Server Setup.

Database Reporting Account

Starting in Build 8.3, you will need to create a database reporting account to ensure that the Adaptiva Server is operating at the highest level of security for your SQL Server environment. All data providers in the Adaptiva Server will use this account to query the Adaptiva database. The account will only be granted db_datareader permissions, ensuring that the account cannot change any data in the Adaptiva database or any other database hosted on the database server.

NOTE: A domain account is recommended for use as the database reporting account.

IMPORTANT: When SQL Server is remote from the Adaptiva Server, the installation will only be able to use a domain account. If a SQL account is required, open a support ticket.

When you install Adaptiva Server, the install will automatically grant permissions to the specified account.

SQL Express

If selecting SQL Express Edition during installation, see the following pre-requisites

Internet Access

If selecting SQL Express Edition during installation, the server must be able to connect to the internet to download Microsoft SQL Server Express Edition. This is only required if Express Edition will be installed during the Adaptiva Server installation.

If using the Cloud Edition, the Adaptiva Server must also be able to reach <http://services.adaptiva.cloud>.

Internet Explorer Settings

If selecting SQL Express Edition during installation, the following settings are required for the installation account to ensure the installation process can automatically download the installation media from Microsoft.


Install an alternative browser and set it as the default

OR

Turn off IE's Enhanced Security configuration

1. Open **Server Manager** (In **Administrative Tools**, if it is not already running)
2. Select **Local Server**
3. Look over to the right in the **Properties** box for: **IE Enhanced Security Configuration**
4. If **IE Enhanced Security Configuration** is set to **On**, then click **On**
5. Select **Off** for Administrators, click on **OK**

Configure Internet Explorer (If this is the default web browser)

1. Open Internet Explorer
2. If prompted, select **Use Recommended Settings** and click **OK**
3. Select the  and click **Internet Options**
4. Select the **Security** tab
5. Uncheck **Enable Protected Mode**
6. Select **Internet** and click **Custom Level...**
 - a. Downloads \ File Download: Enable
7. Close **Internet Explorer**

.NET Framework

If selecting SQL Express Edition during installation, Microsoft .NET Framework 3.5 SP1 must be enabled or download and install Microsoft .NET Framework 4.0. See the following links:

[Microsoft .NET Framework 3.5 SP1](#)

[Microsoft .NET Framework 4.0](#)

SQL Express pre-installed

If SQL Express has been installed beforehand, make sure the following configuration changes have been made.

Configuration	Steps to Implement
TCP/IP connections must be enabled	<ol style="list-style-type: none"> 1. Open SQL Server Configuration Manager 2. Expand SQL Server Network Configuration (not 32-bit), and select Protocols for MSSQLSERVER or the Instance name used 3. Enable TCP/IP if not already 4. Shared Memory should also be enabled, while Named Pipes can stay Disabled
Enable SQL Server Browser	<ol style="list-style-type: none"> 1. Select SQL Server Services 2. Right-click SQL Server Browser and select Properties 3. Confirm the Log on as setting is for Local Service 4. Click on Start
Grant Local System account Sysadmin role. Permissions can be reduced after installation	<ol style="list-style-type: none"> 1. Install SQL Server Management Studio 2. If the account does not exist under Security, Logins run the following T-SQL command:

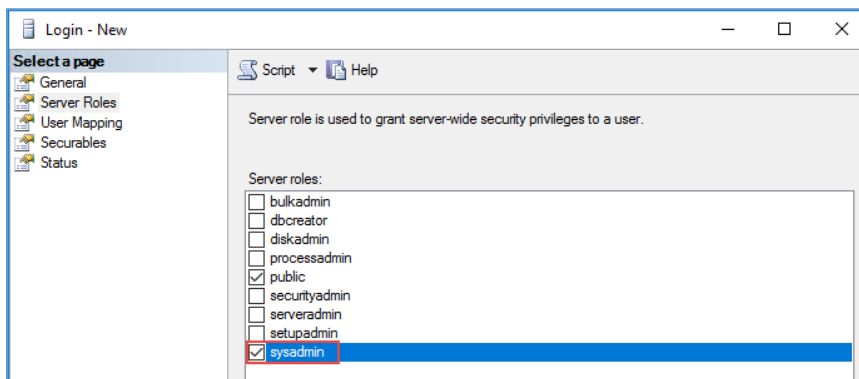
	<pre>CREATE LOGIN [NT AUTHORITY\SYSTEM] FROM WINDOWS WITH DEFAULT_DATABASE=[master], DEFAULT_LANGUAGE=[us_english];GO ALTER SERVER ROLE [sysadmin] ADD MEMBER [NT AUTHORITY\SYSTEM];GO</pre>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

SQL permissions

If SQL Express Edition will NOT be used, then prior to installing the Adaptiva Server, the installation account (and service account, if planned to use) and the Adaptiva Server SYSTEM account must be granted sysadmin permissions in SQL, to allow the creation of the Adaptiva database and the connections to the ConfigMgr database if that is being used. Once the installation is complete, these permissions can be reduced for day-to-day operations if required.

Pre-Install Instructions

1. In **SQL Management Studio** object explorer, expand the **Security** folder, right-click the **Logins** folder and select **New Login...**
2. Click on **Search...**, then ensure the Location is set to the domain and enter the username of the account performing the installation or will be the service account, click on **Check Names**, then **OK**
3. Select the **Server Roles** page and check the box for the **sysadmin** role.

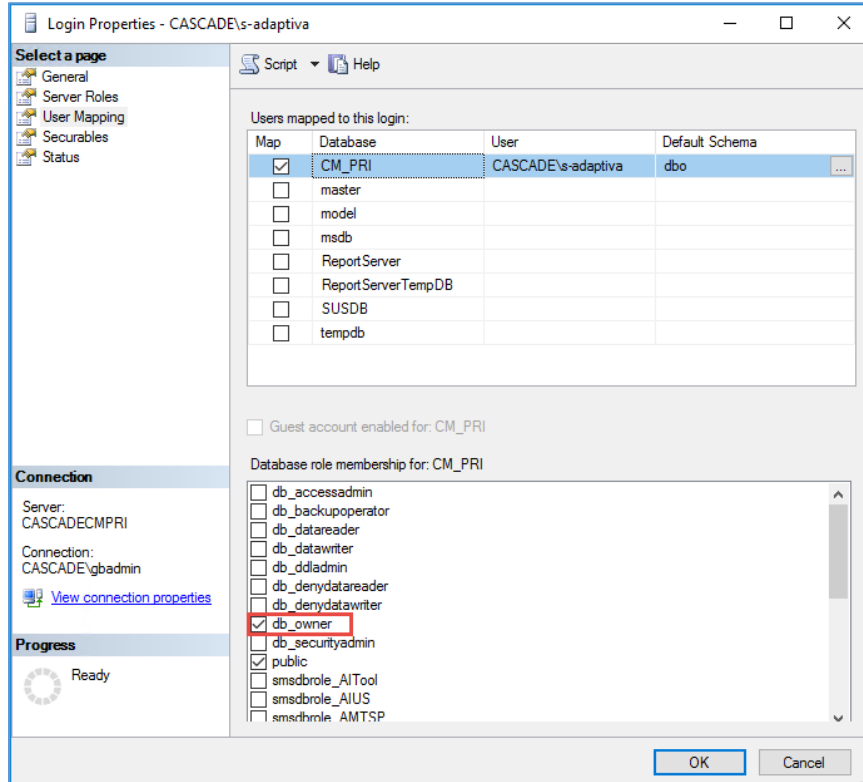


4. Click **OK** to add the login.

Additional prerequisites for ConfigMgr

1. Using **SQL Management Studio**, expand the **Security** folder and select **Properties** for the installation and/or service account

2. Select the **User Mapping** page, in the **Users mapped to this login** section, check the box next to the name of the ConfigMgr database and in the Database role membership section, check the box for the **db_owner** role



3. Click **OK**

Server Activation

If the Adaptiva Server will be activated to use the Adaptiva Cloud Relay Servers, then the following steps are required to request an activation code.

This is required for any Adaptiva solution where clients are on the internet or cannot communicate directly with the Adaptiva Server using UDP or HTTP.

This can be submitted via a request from the Support Portal.

1. Open a web browser and connect to <https://support.adaptiva.com> and log in
2. Click **Submit a request**
3. From the drop down, select **I would like to request Cloud and/or CDN activation for an Adaptiva Server**
4. Complete the form with the following information and click **Submit**
 - Server Name (or identifier - required):
 - Server Use: Production, Dev, Test, QA, etc (required):
 - Request type (required):
 - Cloud Activate & Provision Adaptiva CDN
 - Cloud Activate Only
 - Provision Adaptiva CDN Only
 - Support Email Address (required):
 - Billing Email Address (required):
 - Billing Telephone Number (required):
5. Within 24 hours an activation code will be sent.

App Registration

If the Adaptiva Server will be activated to use the Adaptiva Cloud Relay Servers AND the OneSite Intune Edition will be used with Microsoft Endpoint Manager - Intune, the following steps to create an App Registration are required. These steps need to be completed by the Azure Global Administrator. The Azure App Registration will be used to automate the creation of Apps in Intune by using the Admin Portal.

The following Microsoft documentation can be used for additional information:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

NOTE: Azure is updated regularly so screens may look different.

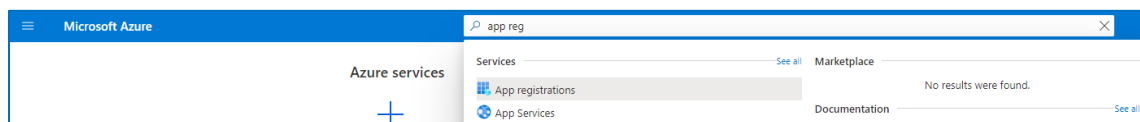
Create App Registration

There are now TWO types of App Registration possible.

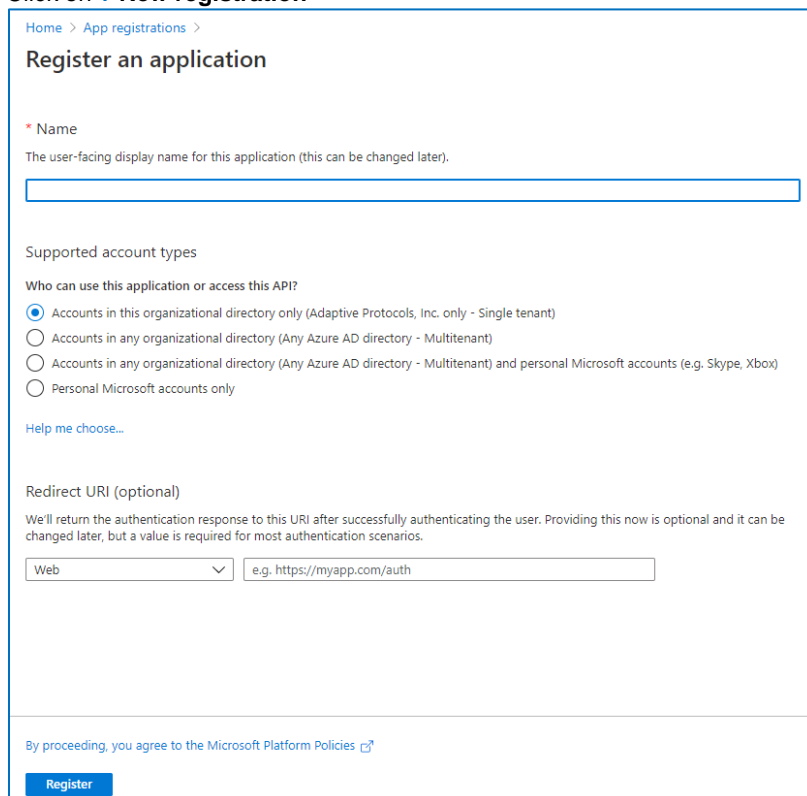
Option 1: Create an App Registration that every Admin Portal user will use. This option does not allow for automatic assignment of Scope Tags based on the User profile.

Option 2: Create an App Registration that uses Delegated Permissions. Permissions can be delegated to a specific account or can be assigned to the user account. This option is required if each user has the potential for different scope tags and those are to be associated with the app when the app is created.

1. Log into Azure (<https://portal.azure.com>) using an account with the appropriate role assignment
2. Using the search bar, search Azure services for **App Registration** and select it



3. Click on **+ New registration**



The screenshot shows the 'Register an application' form in the Azure portal. The form is titled 'Register an application' and includes the following fields and options:

- Name:** A text input field for the user-facing display name for this application (this can be changed later).
- Supported account types:** A section with radio buttons for selecting who can use this application or access this API:
 - ☒ Accounts in this organizational directory only (Adaptive Protocols, Inc. only - Single tenant)
 - ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 - ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 - ☐ Personal Microsoft accounts only
- Help me choose...** A link to help with account type selection.
- Redirect URI (optional):** A section with a dropdown menu set to 'Web' and a text input field containing 'e.g. https://myapp.com/auth'.
- By proceeding, you agree to the Microsoft Platform Policies** A checkbox.
- Register** A blue button to complete the registration.

Complete the following:

Name: Enter a name to identify this app registration for Adaptiva, e.g. AdaptivaOneSite

Supported account types: Accounts in this organizational directory only

Redirect URI (optional): Leave blank

Click on **Register**

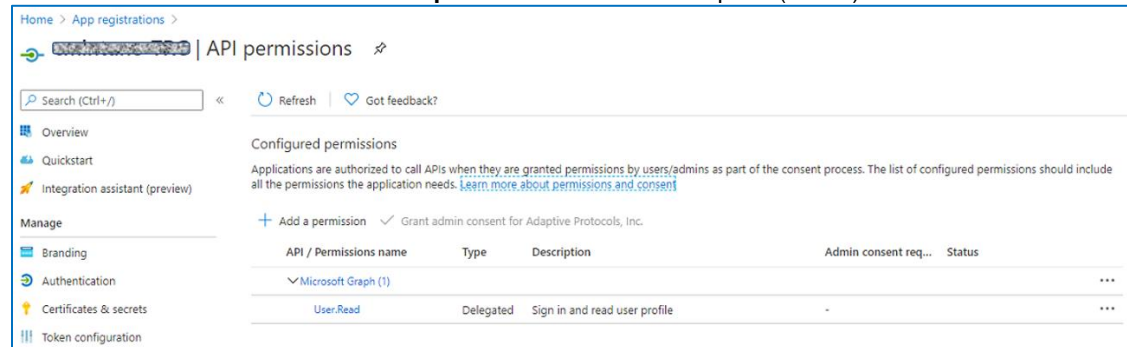
4. The properties of the App Registration will be displayed

Provide the following IDs to the Adaptiva administrator:

Application (client) ID: This will be used in the Intune App ID field

Directory (tenant) ID: This will be used in the Intune App Tenant ID field

5. Click on **View API Permissions** or **API permissions** in the action pane (far left).



Home > App registrations > [App Name] | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant (preview)

Manage Branding Authentication Certificates & secrets Token configuration

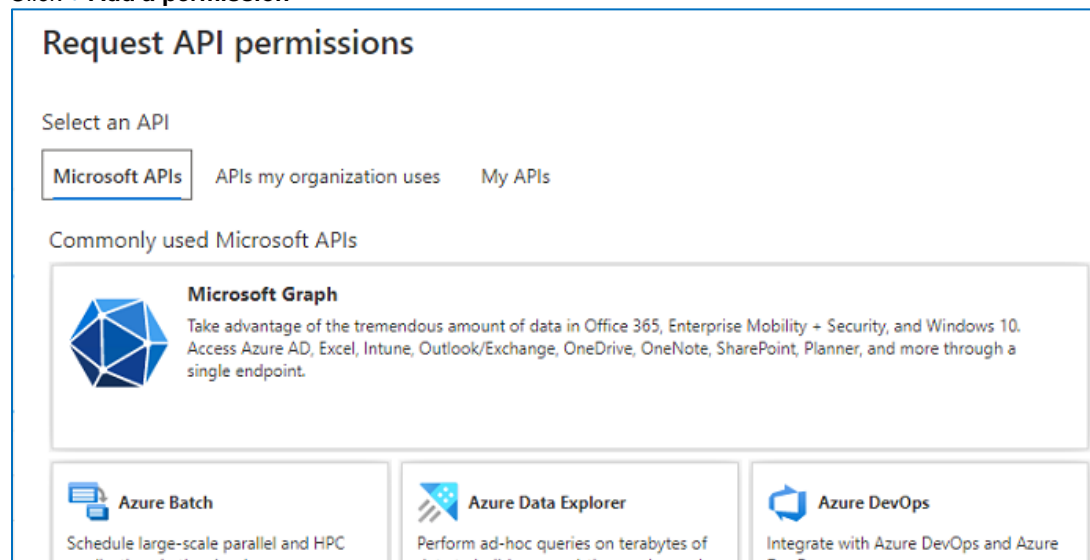
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Adaptive Protocols, Inc.

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	-	...

6. Click **+ Add a permission**




Request API permissions


Select an API

Microsoft APIs APIs my organization uses My APIs


Commonly used Microsoft APIs




Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch
Schedule large-scale parallel and HPC applications in the cloud.

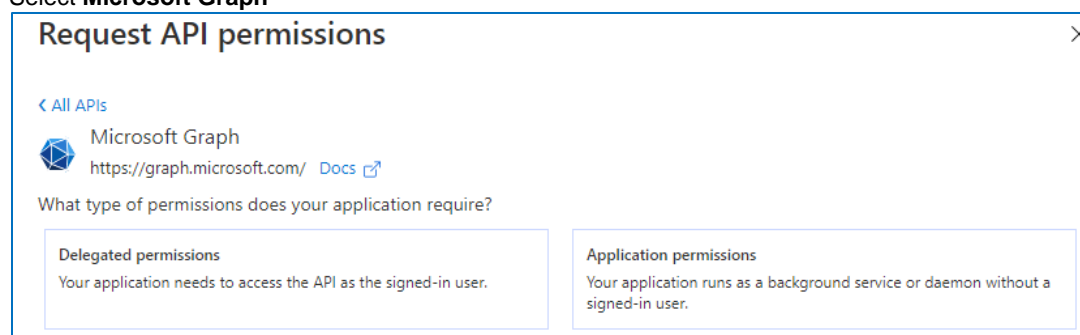


Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics.



Azure DevOps
Integrate with Azure DevOps and Azure DevOps services.

7. Select **Microsoft Graph**



Request API permissions

< All APIs

Microsoft Graph
<https://graph.microsoft.com/> Docs

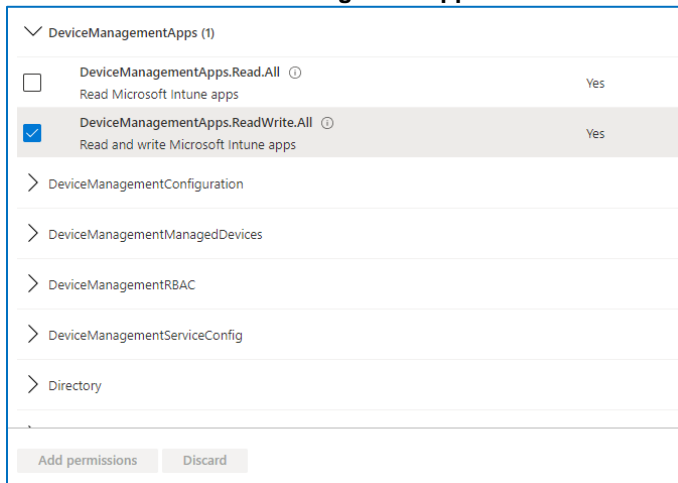
What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

8. **For Option 1: Select Application permissions**
For Option 2: Select Delegated permissions

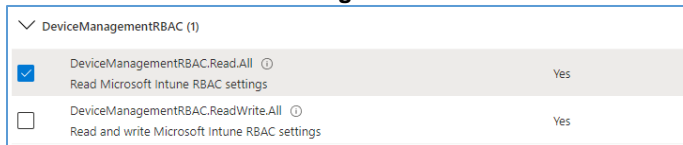
9. Enter **DeviceManagement** to filter the list
10. Expand **DeviceManagementApps**
11. Check the box for **DeviceManagementApps.ReadWrite.All**



DeviceManagementApps (1)		
<input type="checkbox"/>	DeviceManagementApps.Read.All ⓘ Read Microsoft Intune apps	Yes
<input checked="" type="checkbox"/>	DeviceManagementApps.ReadWrite.All ⓘ Read and write Microsoft Intune apps	Yes
> DeviceManagementConfiguration		
> DeviceManagementManagedDevices		
> DeviceManagementRBAC		
> DeviceManagementServiceConfig		
> Directory		

Add permissions Discard

12. Expand **DeviceManagementRBAC**
13. Check the box for **DeviceManagementRBAC.Read.All**




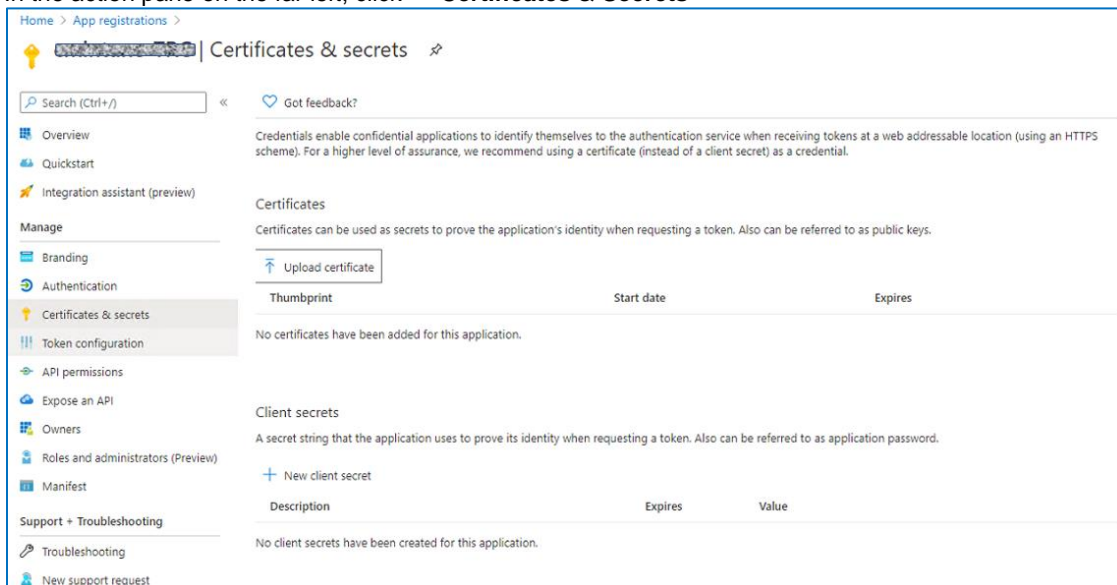
DeviceManagementRBAC (1)		
<input checked="" type="checkbox"/>	DeviceManagementRBAC.Read.All ⓘ Read Microsoft Intune RBAC settings	Yes
<input type="checkbox"/>	DeviceManagementRBAC.ReadWrite.All ⓘ Read and write Microsoft Intune RBAC settings	Yes

14. Click on **Add permissions**
15. Under **Configured** permissions, click on ☒ **Grant admin consent for <tenant>** and select **Yes**

Option 1

Complete these steps to create an App Registration for Option 1 where an App Secret will be used

16. In the action pane on the far left, click  **Certificates & Secrets**



Home > App registrations > Certificates & secrets

Search (Ctrl+/) Got feedback?

Overview
Quickstart
Integration assistant (preview)

Manage

- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators (Preview)
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Certificates

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires
No certificates have been added for this application.		

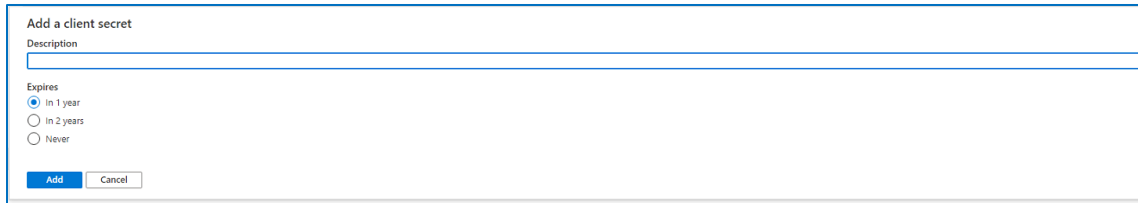
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value
No client secrets have been created for this application.		


17. Under **Client secrets**, click on **+ New client secret**



18. Enter a description, e.g. Adaptiva OneSite and select the appropriate expiration timeframe based on the company's security guidelines.
Click **Add**

IMPORTANT: There can only be TWO client secrets. Secrets can be deleted and recreated.

19. The client secret will be displayed. The secret can only be retrieved when it is created, it cannot be retrieved later.

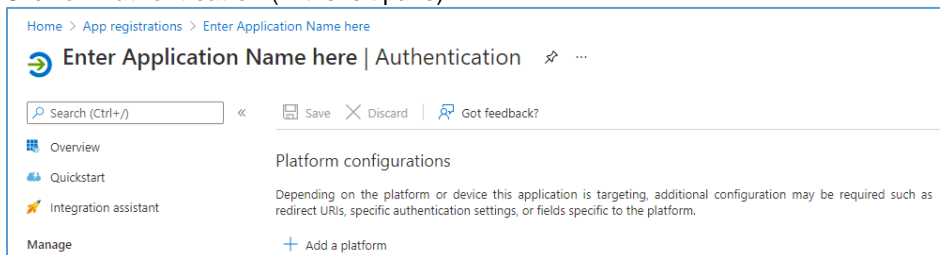
Under the **Value** column, click on the copy icon  to copy the secret to the clipboard

20. Provide the secret value to the Adaptiva Administrator along with the Directory (Tenant) and Client (App) IDs.
Create a reminder on your calendar for the end date to create a new App secret.

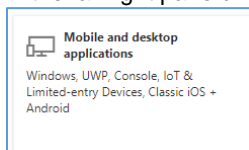
Option 2

Complete these steps to create an App Registration for Option 2 where a deferred account will be used

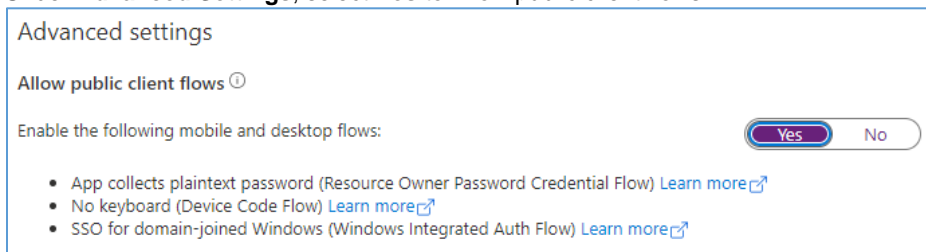
16. Click on **Authentication** (in the left pane)



17. Click on **+ Add a platform**
18. In the far-right pane under Configure platforms, select Mobile and desktop applications



19. Check the box for <https://login.microsoftonline.com/common/oauth2/nativeclient> and click **Configure**
20. Under **Advanced Settings**, select **Yes** to Allow public client flows



21. Click **Save**

Workspace ONE

The following steps must be completed before starting the Adaptiva Server installation. There are also post-installation steps that will need to be completed.

Install/Update the Cloud Connector

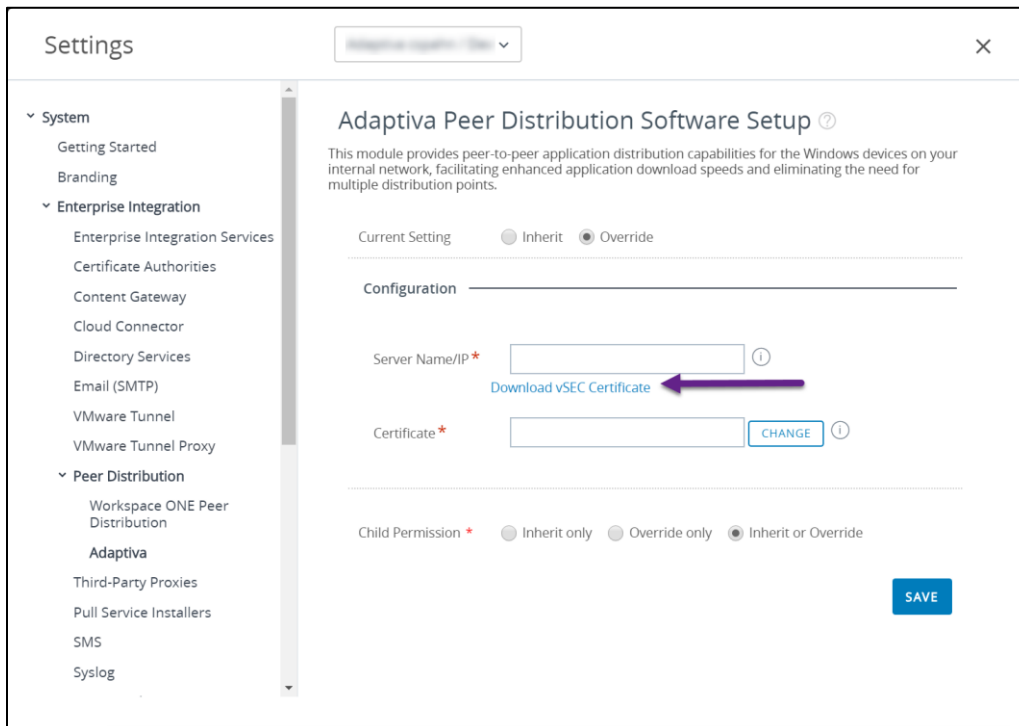
The AirWatch Cloud Connector (ACC) component must be installed before installing the Adaptiva Server. Make sure it is the proper version. For instructions on this, see the [omnissa Workspace ONE documentation library](#).

1. If the ACC is already installed, open the log file **CloudConnect.log** in <InstallPath>\Airwatch\Logs\CloudConnector
2. Search for *Starting CloudConnector*. The version should be **19.7.0.0** or later
3. If it is not 19.7.0.0 or later, open the Workspace ONE UEM console and navigate to: **Groups & Settings > All Settings > System > Enterprise Integration > Cloud Connector**. Select **Download AirWatch Cloud Connector Installer** and install
4. Click on **Test Connection** and validate the **AirWatch Cloud Connector is active**

Download the Certificate

Download the vSEC certificate for the current instance of Workspace ONE.

1. Open the Workspace ONE UEM console and navigate to: **Groups & Settings > All Settings > System > Enterprise Integration > Peer Distribution > Adaptiva**



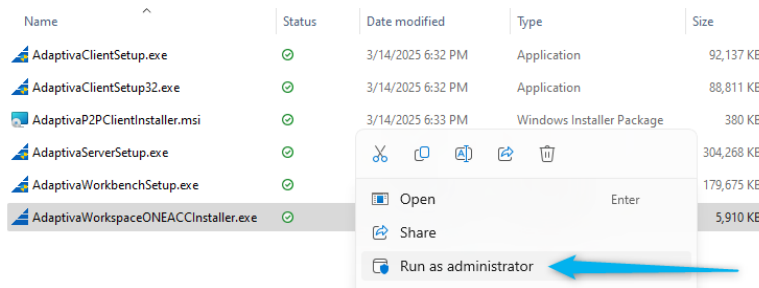
2. Click the link to **Download vSEC Certificate** and store it in a convenient location as it will be needed later. Return to this page after the installation of Adaptiva to upload the Adaptiva certificate and provide the name or IP address of the Adaptiva server.

Installing the Adaptiva APIs

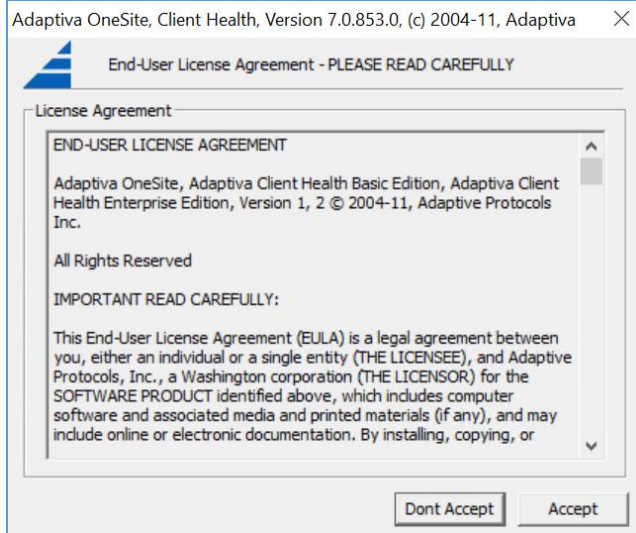
The ACC will require access to Adaptiva DLLs in order to call the APIs provided by Adaptiva. To install these on the server hosting the ACC follow these steps:

1. Navigate to the Adaptiva Installation source folder

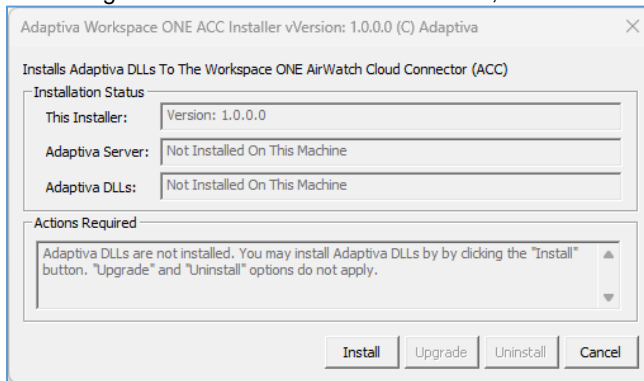
- Run the **AdaptivaWorkspaceONEACCInstaller.exe** as an administrator and click Yes if prompted



- On the **End-User License Agreement** screen click **Accept**



- The dialog will show current installation status, click **Install**



- When prompted: **Are You Sure you Wish To Install Adaptiva DLLs?**, click **Yes**
- When prompted that the **Installation Was Successful**, click **OK**

(Deprecated) Azure Storage

Adaptiva CDN storage is now recommended (build 8.0.925 or greater is required).

If the Adaptiva Cloud License will be activated but the Adaptiva CDN is not provisioned, the following steps to create an Azure Storage container are required to be followed by the Azure Global Administrator when cloud storage is

required. The Azure Storage Account Container will be used to store the package content. It is effectively the Adaptiva Content Library in the cloud.

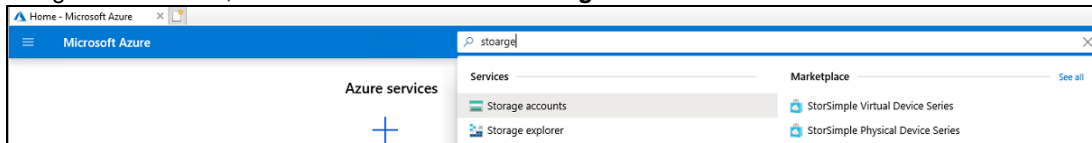
The following Microsoft documentation can be used for additional information:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview>

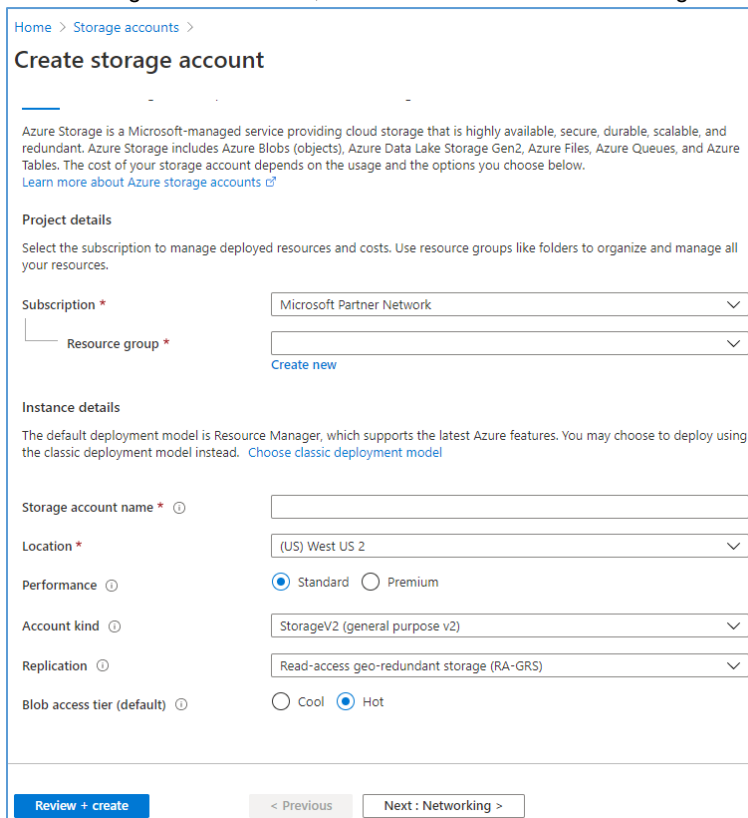
NOTE: Azure is updated regularly so screens may look different

Create Storage Account and Container

1. Log into Azure (<https://portal.azure.com>) using an account with the appropriate role assignment
2. Using the search bar, search Azure services for **Storage accounts** and select it



3. In the Storage Account blade, click on **+ Add** to create a Storage account. The following pane will be displayed:



Enter the following information on the **Basics** tab:

Subscription: Select the subscription to use for this storage account

Resource Group: Select an existing resource group OR create a new one. Resource groups are containers that hold related resources for an Azure solution. For example, the Adaptiva administrators could be assigned to this resource group to allow them to access the Storage account being created.

Storage account name: Enter a unique name (across all of Azure) for the storage account (**must** be 3 to 24 characters in length and all lowercase letters)

Location: Select the geo-location where the resource should exist

Performance: Standard

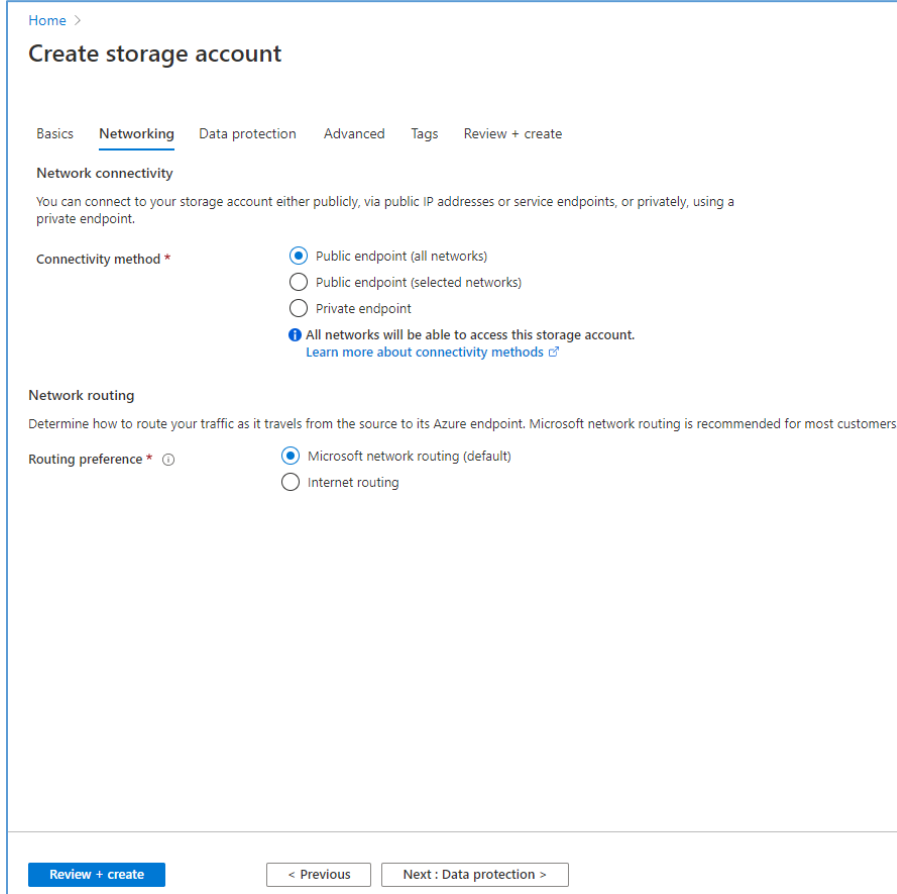
Account kind: StorageV2 (general purpose v2)

Replication: Locally-redundant storage (LRS) – this is the least expensive Storage option

Blob access tier (default): Hot

Click **Next : Networking >**

4. On the **Networking** tab



Home >

Create storage account

Basics **Networking** Data protection Advanced Tags Review + create

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Connectivity method *

- ☒ Public endpoint (all networks)
- ☐ Public endpoint (selected networks)
- ☐ Private endpoint

! All networks will be able to access this storage account.
[Learn more about connectivity methods](#)

Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference * ⓘ

- ☒ Microsoft network routing (default)
- ☐ Internet routing

[Review + create](#) < Previous Next : Data protection >

Connectivity method: Public endpoint (all networks)

Routing preference: Microsoft network routing (default)

Click **Next : Data protection >**

5. On the **Data protection** tab

[Home](#) >

Create storage account

[Basics](#)
[Networking](#)
[Data protection](#)
[Advanced](#)
[Tags](#)
[Review + create](#)

Recovery

☐ Turn on point-in-time restore
 Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)

The current subscription needs to have the following features enabled - Versioning, Change feed, RestoreBlobRanges

☐ Turn on soft delete for blobs
 Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)

☐ Turn on soft delete for containers
 Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)

Sign up is currently required to utilize the Container soft delete feature on a per-subscription basis. [Learn more about container soft delete](#)

☐ Turn on soft delete for file shares
 Soft delete enables you to recover file shares that were previously marked for deletion. [Learn more](#)

Tracking

☐ Turn on versioning
 Use versioning to automatically maintain previous versions of your blobs for recovery and restoration. [Learn more](#)

☐ Turn on blob change feed
 Keep track of create, modification, and delete changes to blobs in your account. [Learn more](#)

[Review + create](#)
[< Previous](#)
[Next : Advanced >](#)

All of these can be left **Unchecked**

Turn on point-in-time restore

Turn on soft delete for blobs

Turn on soft delete for containers

Turn on soft delete for file shares

Turn on versioning

Turn on blob change feed

Click **Next : Advanced >**

6. On the **Advanced** tab

Home >

Create storage account

Basics Networking Data protection **Advanced** Tags Review + create

Security

Secure transfer required ☐ Disabled ☒ Enabled

Allow Blob public access ☐ Disabled ☒ Enabled

Minimum TLS version

Infrastructure encryption ☒ Disabled ☐ Enabled

Azure Files

Large file shares ☒ Disabled ☐ Enabled

Data Lake Storage Gen2

Hierarchical namespace ☒ Disabled ☐ Enabled

NFS v3 ☒ Disabled ☐ Enabled

Review + create < Previous Next : Tags >

All of these can be left at their default

Secure transfer required: Enabled

Allow Blob public access: Enabled

Minimum TLS version: Version 1.2

Infrastructure encryption: Disabled

Large file shares: Disabled

Hierarchical namespace: Disabled

NFS v3: Disabled

Click **Next : Tags >**

7. On the **Tags** tab

Home > Storage accounts > Create storage account

Create storage account

Basics Networking Advanced **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
		Storage account

Click **Next : Review + create >**

8. Review the entries

Home > Storage accounts > Create storage account

Create storage account

✓ Validation passed

Basics Networking Advanced Tags [Review + create](#)

Basics

Subscription	[Redacted]
Resource group	[Redacted]
Location	West US 2
Storage account name	onesiteforintune
Deployment model	Resource manager
Account kind	StorageV2 (general purpose v2)
Replication	Locally-redundant storage (LRS)
Performance	Standard
Access tier (default)	Hot

Networking

Connectivity method	Public endpoint (all networks)
---------------------	--------------------------------

Advanced

Secure transfer required	Enabled
Large file shares	Disabled
Blob soft delete	Disabled
Blob change feed	Disabled
Hierarchical namespace	Disabled
NFS v3	Disabled

[Create](#) [< Previous](#) [Next >](#) [Download a template for automation](#)

Click **Create**

It will take a few minutes for the resource to be created

9. When **Your deployment is complete** is displayed, click on **Go to resource**

Home > Microsoft.StorageAccount-20200406124924 | Overview

Microsoft.StorageAccount-20200406124924 | Overview

Deployment

Overview Inputs Outputs Template

Delete Cancel Redeploy Refresh

✓ Your deployment is complete

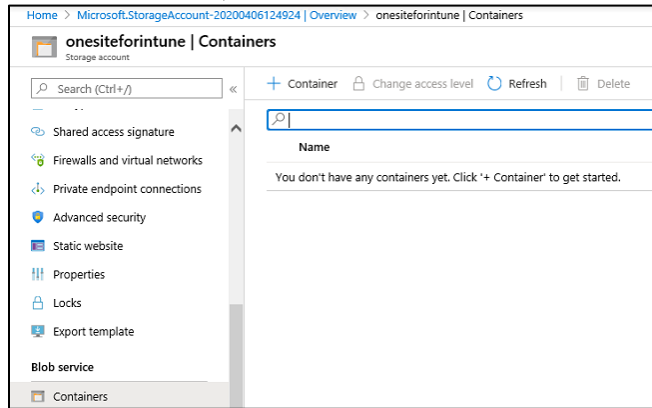
Deployment name: Microsoft.StorageAccount-20200406124924 Start time: 4/6/2020 1:15:19 PM
 Subscription: [Redacted] Correlation ID: 413373bb-20bb-49eb-a1f6-e765fcaa11c0
 Resource group: [Redacted]

▼ Deployment details (Download)

^ Next steps

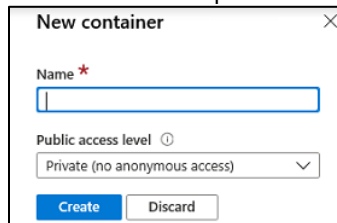
[Go to resource](#)

10. Under **Blob service**, select **Containers**



Click **+ Container**

11. The New container pane will be displayed on the far right



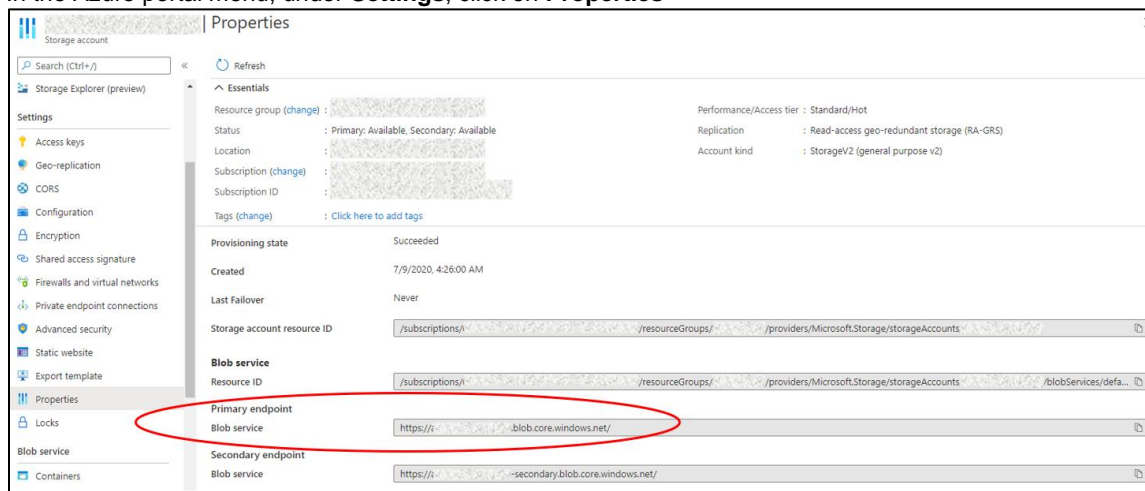
Enter a container name (**must** be all lowercase)

This will be the Root Container Name used by Adaptiva and will need to be provided to the Adaptiva Administrator

The **Public access level** will remain at: Private (no anonymous access)

Click **Create**

12. In the Azure portal menu, under **Settings**, click on **Properties**



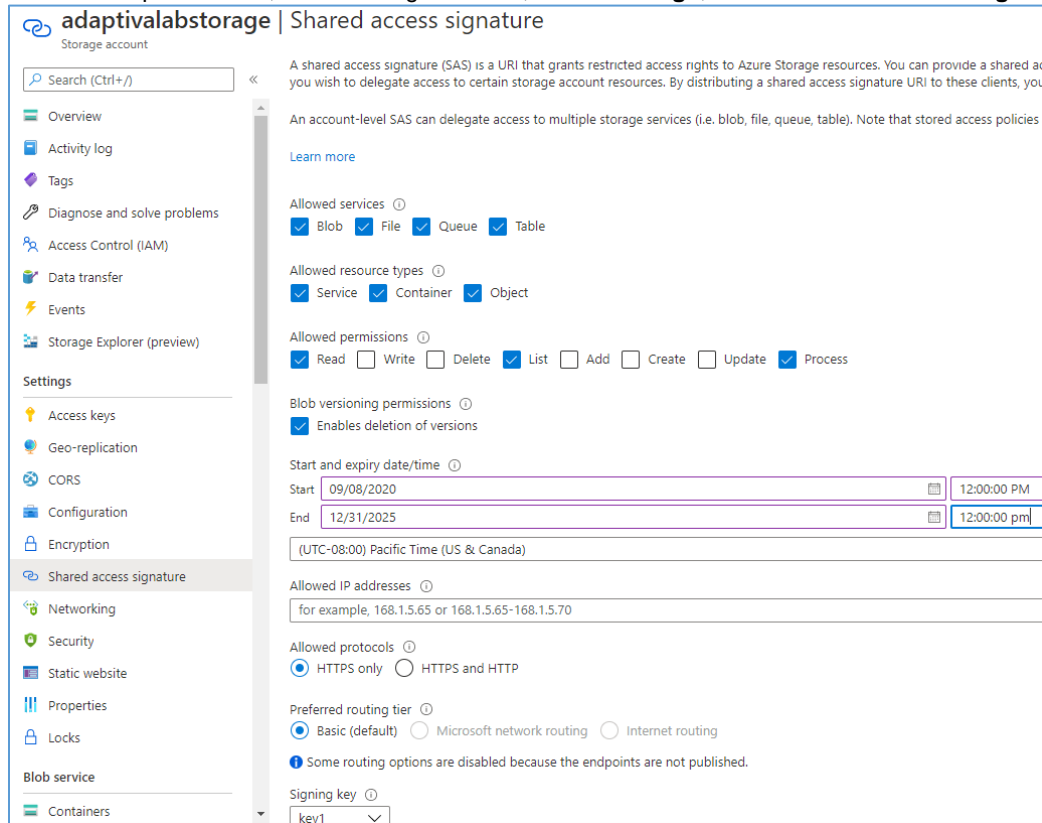
Provide the following information to the Adaptiva Administrator:

Blob Service: `https://<StorageAccountName>.blob.core.windows.net/`

Create the Container Read Token

To get the Container Read and Write Tokens we need to create Shared Access Signatures in the Azure Storage Account. These tokens can only be retrieved when they are created, they cannot be retrieved later.

1. In the Azure portal menu, in the Storage account, select **Settings**, click on **Shared access signature**



The screenshot shows the 'Shared access signature' configuration page in the Azure portal. The left sidebar contains a navigation menu with options like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data transfer, Events, Storage Explorer (preview), Settings, Access keys, Geo-replication, CORS, Configuration, Encryption, Shared access signature (selected), Networking, Security, Static website, Properties, Locks, Blob service, and Containers. The main content area is titled 'Shared access signature' and includes a search bar. Below the title, there is a description of SAS and a 'Learn more' link. The configuration section includes:

- Allowed services:** Blob, File, Queue, Table (all checked).
- Allowed resource types:** Service, Container, Object (all checked).
- Allowed permissions:** Read, Write, Delete, List, Add, Create, Update, Process (Read, List, and Process are checked).
- Blob versioning permissions:** Enables deletion of versions (checked).
- Start and expiry date/time:** Start date is 09/08/2020 at 12:00:00 PM, and End date is 12/31/2025 at 12:00:00 pm. The time zone is (UTC-08:00) Pacific Time (US & Canada).
- Allowed IP addresses:** A text field for IP addresses, with an example: 168.1.5.65 or 168.1.5.65-168.1.5.70.
- Allowed protocols:** HTTPS only (selected), HTTPS and HTTP.
- Preferred routing tier:** Basic (default) (selected), Microsoft network routing, Internet routing. A note states: 'Some routing options are disabled because the endpoints are not published.'
- Signing key:** A dropdown menu showing 'key1'.

5. **Allowed services:**
Check **ALL** boxes: **Blob, File, Queue, Table**
6. **Allowed resource types:**
Check **ALL** boxes: **Service, Container, Object**
7. **Allowed permissions:**
Check **ONLY** the boxes: **Read, List, Process**
8. **Blob versioning permissions:** Check the box: **Enables deletion of versions**
9. Enter an **End** date. Follow the company's security guidelines for the allowable length of time.
Create a reminder on the calendar for that end date that the SAS token needs to be renewed.
10. **Allowed IP addresses:** Leave blank.
11. **Allowed protocols:** HTTPS only

Click on **Generate SAS and connection string**

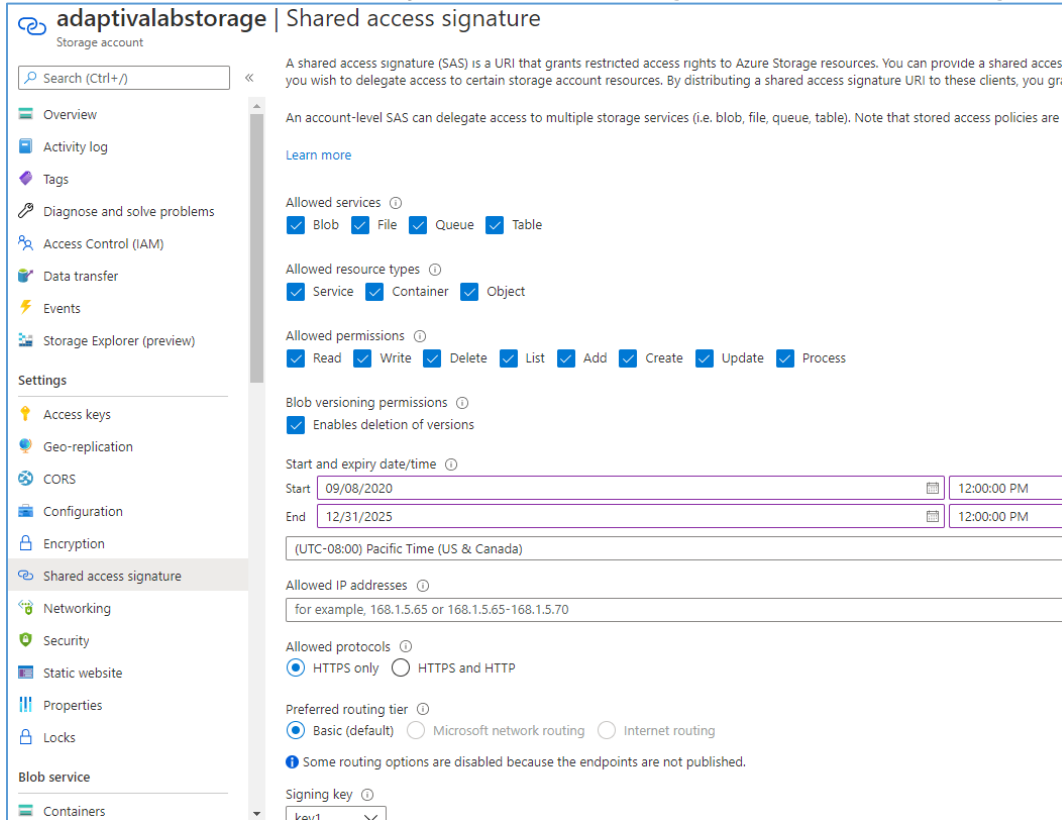
2. Scroll down and copy the **SAS token** and provide it to the Adaptiva Administrator. Also provide the expiration date.

NOTE: This token cannot be retrieved later. Clicking on **Generate SAS and connection string** in the future will create a **NEW** token. The original token created is still valid until the end timestamp. The token can be changed at any time in the workbench or Admin Portal.

Create the Container Write Token

To get the Container Read and Write Tokens we need to create Shared Access Signatures in the Azure Storage Account. These tokens can only be retrieved when they are created, they cannot be retrieved later.

1. In the Azure portal menu, in the Storage account, select **Settings**, click on **Shared access signature**



The screenshot shows the 'Shared access signature' configuration page in the Azure portal. The left sidebar lists various settings, with 'Shared access signature' selected. The main content area includes a description of SAS, a 'Learn more' link, and several configuration sections:

- Allowed services:** Checkboxes for Blob, File, Queue, and Table, all of which are checked.
- Allowed resource types:** Checkboxes for Service, Container, and Object, all of which are checked.
- Allowed permissions:** Checkboxes for Read, Write, Delete, List, Add, Create, Update, and Process, all of which are checked.
- Blob versioning permissions:** A checkbox for 'Enables deletion of versions' is checked.
- Start and expiry date/time:** The 'Start' date is 09/08/2020 at 12:00:00 PM. The 'End' date is 12/31/2025 at 12:00:00 PM. The time zone is set to (UTC-08:00) Pacific Time (US & Canada).
- Allowed IP addresses:** A text field with the placeholder 'for example, 168.1.5.65 or 168.1.5.65-168.1.5.70'.
- Allowed protocols:** Radio buttons for 'HTTPS only' (selected) and 'HTTPS and HTTP'.
- Preferred routing tier:** Radio buttons for 'Basic (default)' (selected), 'Microsoft network routing', and 'Internet routing'. A note below states: 'Some routing options are disabled because the endpoints are not published.'
- Signing key:** A dropdown menu showing 'key1'.

Allowed services: Check **ALL** boxes: **Blob, File, Queue, Table**

Allowed resource types: Check **ALL** boxes: **Service, Container, Object**

Allowed permissions: Check **ALL** boxes: **Read, Write, Delete, List, Add, Create, Update, Process**

Blob versioning permissions: Check the box: **Enables deletion of versions**

Enter an **End** date. Follow the company's security guidelines for the allowable length of time. **Create a reminder on the calendar** for that end date that the SAS token needs to be renewed.

Allowed IP addresses: Leave blank.

Allowed protocols: HTTPS only

2. Click on Generate SAS and connection string
3. Scroll down and copy the **SAS token** and provide it to the Adaptiva Administrator. Also provide the expiration date.

The other information is not required

NOTE: This token cannot be retrieved later. Clicking on **Generate SAS and connection string** in the future will create a **NEW** token. The original token created is still valid until the end timestamp. The token can be changed at any time in the workbench or Admin Portal.

OneSite Platform Installation

Adaptiva provides the OneSite Platform files in a compressed (.zip) file. The compressed file includes three folders: Documentation, Installers and Tools folder. OneSite Platform installation requires two files from the Installer folder:

1. AdaptivaServerSetup.exe
2. AdaptivaClientSetup.exe

All components require local administrator privileges to install.

Prerequisites

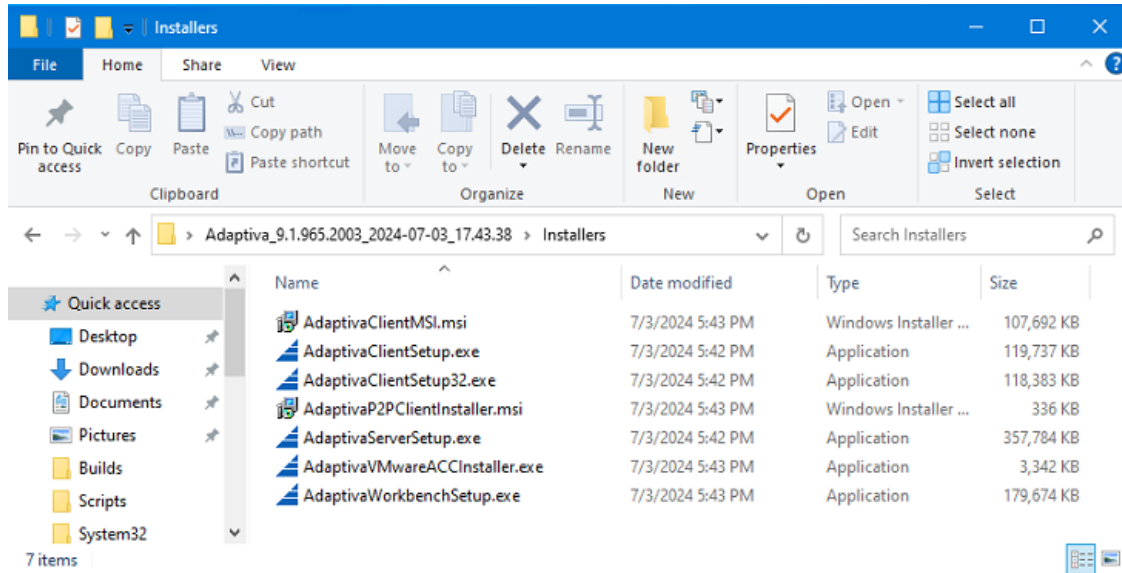
Review the Deployment Planning sections above prior to installing the OneSite Platform.

For information about additional, optional installation procedures, see Appendix C: Optional Configuration Activities.

Prepare the Installation Files

Upon purchase, Adaptiva provides the OneSite Platform installation files in a compressed (.zip) folder. To extract the files for installation, complete the following steps:

1. Download or move the file to the server acting as the Adaptiva Server instance.
2. Right click the file, and then select **Extract All...**
3. Click **Browse** and navigate to the location on the Adaptiva Server where you want to save the files.
4. Select **Show Extracted Files When Complete**, and then click **Extract**. This extracts the files and displays them in a folder structure.



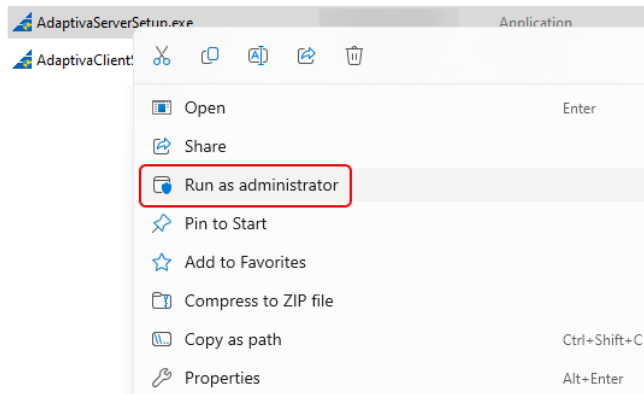
Server Installation

Launch the Adaptiva Server Installer

To install the Adaptiva Server, use the `AdaptivaServerSetup.exe` executable.

IMPORTANT: If integrating with ConfigMgr, the logged in user must have appropriate permission to the Configuration Manager Site and file server – review the Accounts and Permissions section of the Deployment Planning guide. This user must also be an SA on the SQL Server that will host the Adaptiva database as well as the SQL Server that is hosting the ConfigMgr database. Permissions can be reduced after a successful installation.

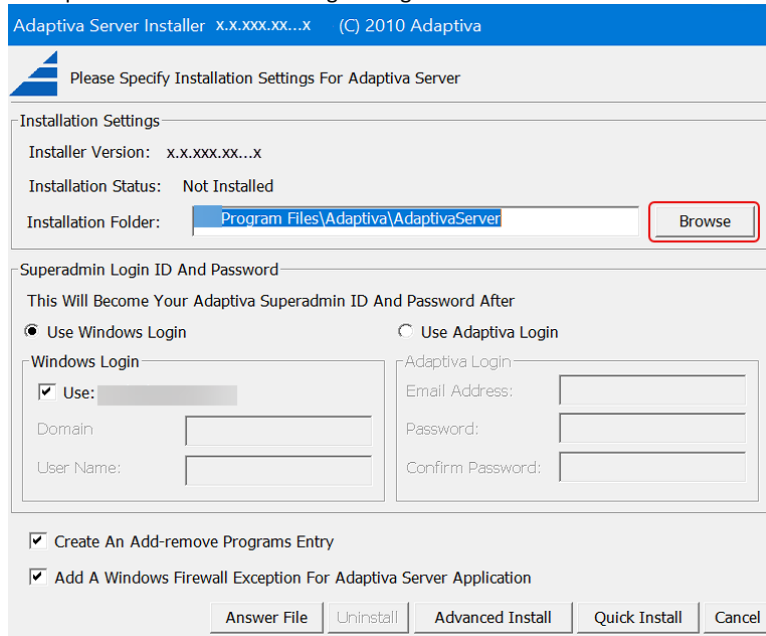
1. Right click the **AdaptivaServerSetup.exe**, and then select **Run as administrator**.



2. Read through the **End User License Agreement (EULA)**, and then click **Accept** to continue with the installation.



This opens the Installation Settings dialog box:



3. Configure the Installation Settings.

Configure Installation Settings

After launching the Adaptiva Server Installer configure the installation settings for your Adaptiva Server.

1. Click Browse under Installation Settings and navigate to the location where you want the Adaptiva Server instance installed. Adaptiva recommends using the default file structure (Program Files\Adaptiva\AdaptivaServer\) on a primary drive designation other than Operating System (OS) C:

IMPORTANT: Do not install Adaptiva Server on the Operating System (OS) C: drive. The OneSite product log files and the Adaptiva Content Library installed with the Adaptiva Server grow over time, which impacts storage and performance on the OS C: drive. If you need to move the Content Library after installation, see the Post-Install Instructions section for information about moving the Content Library.

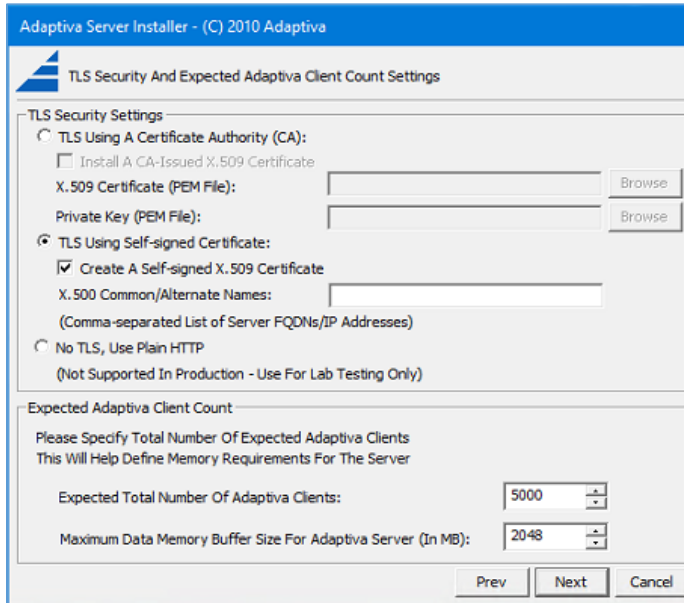
2. Set the **Superadmin Login ID and Password** using one of the following options:
 - Select **Use Windows Login** to use the same account details you used to log in to the Windows server. The installation adds the domain name and username specified here to the superadmin role. (Recommended)
 - Select **Use Adaptiva Login** and supply an email address and password to create an internal Adaptiva login. Adaptiva recommends this for lab/test environments only.
NOTE: The email address entered does not have to be a valid email address.
3. The following items are checked by default:
 - **Create an Add/Remove Programs Entry:** When enabled (default), the Adaptiva Installer creates an entry for Adaptiva Server in the Windows Control Panel > Programs > Programs and Features and Apps & Features workspace.
 - **Add a Windows Firewall Exception for Adaptiva Server Application:** When enabled, automatically adds local exceptions in the Windows firewall for the default server ports (See Appendix B: Communication Ports).

IMPORTANT: Review any existing domain-based group policies (GPO) that configure or restrict Windows firewall rules or rule creation as they can prevent or override these Adaptiva-created firewall exceptions.

4. Click **Advanced Install** to continue with a new installation:
 - To create an Answer File to automate a later new installation, see Create Silent Installation Answer
 - To perform a Quick Install (Not Recommended for Production environments), click on Quick Install. This will Install SQL Server 2022 Express Edition, with SQL Authentication, with Instance Name: AdaptivaSQL. There will be no third-party integrations. The Admin Portal will be configured with a self-signed certificate using port 443.
5. See Configure TLS Security Settings

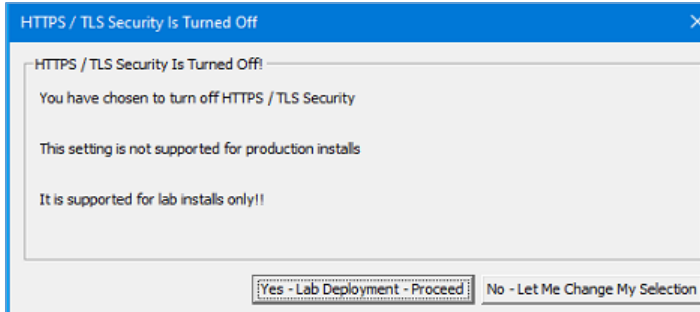
Configure TLS Security Settings and Client Count

Use the TLS Security Settings to define the security settings for the Adaptiva Admin Portal. The Deployment Planning Installation Prerequisites provides details about Certificates, including how to convert them to the required format.



The screenshot shows the 'Adaptiva Server Installer - (C) 2010 Adaptiva' window. The title bar is blue with the Adaptiva logo. The main window has a light gray background. The title of the window is 'TLS Security And Expected Adaptiva Client Count Settings'. There are two main sections: 'TLS Security Settings' and 'Expected Adaptiva Client Count'. In the 'TLS Security Settings' section, there are three radio buttons: 'TLS Using A Certificate Authority (CA):', 'TLS Using Self-signed Certificate:', and 'No TLS, Use Plain HTTP'. The 'TLS Using Self-signed Certificate:' option is selected. Under this option, there is a checked checkbox 'Create A Self-signed X.509 Certificate' and a text box for 'X.500 Common/Alternate Names:'. There is also a note '(Not Supported In Production - Use For Lab Testing Only)'. In the 'Expected Adaptiva Client Count' section, there is a text box for 'Expected Total Number Of Adaptiva Clients:' with the value '5000' and a spin box for 'Maximum Data Memory Buffer Size For Adaptiva Server (In MB):' with the value '2048'. At the bottom, there are 'Prev', 'Next', and 'Cancel' buttons.

1. Select one of the following TLS security settings, based on the preferences of your organization. These settings allow secure access to the Adaptiva Admin Portal for devices with the certificate:
 - Select **TLS Using A Certificate Authority (CA)** to use a certificate you exported from a Certificate Authority. If you choose this option, the CA-based certificate must be installed on the devices requiring access to the Adaptiva Admin portal. An auto-enrollment GPO can be configured and targeted to specific devices or a wild-card certificate can be used.
 - i. Click **Install A CA-Issued X.509 Certificate**.
 - ii. Click **Browse**, and then navigate to the location of the Certificate PEM File.
 - iii. Click **Browse**, and then navigate to the location of the Private Key PEM File.
 - Select **TLS Using Self-signed Certificate** to use a self-signed certificate. If you choose this option, you must provide the certificate to every Adaptiva Administrator who must add it to the Certificate store on the device from which they access the Adaptiva Admin Portal. See Post-Install Instructions, Add Certificate to the Root Store
 - i. Click **Create A Self-signed X.509 Certificate**.
 - ii. Enter the **names or IP addresses** associated with the servers that host the Adaptiva Admin Portal. For example, include server details for NETBIOS, FQDN, DNS Alias or IP Address. Separate each entry by comma.
 - Select **No TLS, Use Plain HTTP** if your organization does not require TLS to access the Adaptiva Admin Portal.
3. Set the expected Adaptiva Client Count. Use the number identified in the Memory Allocation table of the Hardware Requirements gathered during Design Planning.
The **Expected Total Number Of Adaptiva Clients** defaults to 5000, which automatically sets the **Maximum Data Memory Buffer Size** to 2048 MB.
2. Click **Next** to proceed to **Integrating Third Party Products**.
3. If No TLS, Use Plain HTTP was selected, the installer prompts you to confirm that this is a lab server.

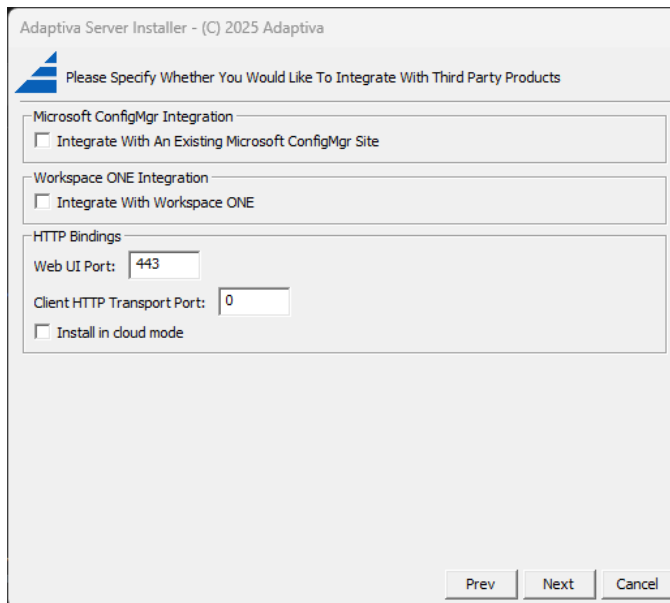


- Click Yes - Lab Deployment - Proceed and skip to **Integrating Third Party Products**.
 - Click No - Let Me Change My Selection to return to the TLS Security Settings and try again.
4. Continue with Integrate Third Party Products.

Integrate Third Party Products

This installation dialog box provides third-party integration options such as Microsoft ConfigMgr and omnisia Workspace One. You must also set HTTP Bindings and may configure Cloud Installation settings from this screen.

You are not required to integrate a third party product.



Set HTTP Bindings for Adaptiva Server

As part of the Integrate with Third Party Products configuration screen, first configure the HTTP Bindings.

- i. In the **Web UI HTTP** port enter 443. If, on the server where you are installing Adaptiva, there are other services using port 443, change the port to use for the Web UI HTTP Port, e.g.: 9678
Port 80 can be used if No TLS, Use Plain HTTP was selected on the previous screen and no other services are using port 80.

IMPORTANT: Be sure to share this port with all Adaptiva Administrators. It is required to access the Admin Portal via a web browser.

- ii. **Enable Client HTTP Communications** should only be selected if the managed clients cannot communicate with the Adaptiva Server via the UDP ports in Appendix B. If managed clients can connect using TCP ports, check the box and

enter a port to allow the clients to communicate with the AdaptivaServer, e.g.: 9679. Make sure this port is not listening on the server.

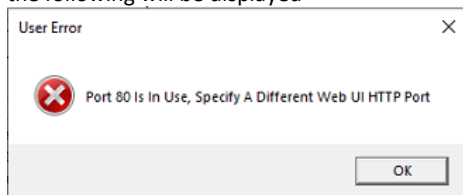
Skip the **Cloud Installation** configuration unless directed by Adaptiva Customer Support.

- i. If the Adaptiva Server is being installed in Azure or Amazon Web Services (AWS) then the assumption is there will be no other devices with the Adaptiva Client on the same subnet. Check the box for **Install in the Cloud** and enter the range(s) of IP Addresses in a Corporate office that should be used as the Central Office. This can be done after installation.

This should only be done with the help of Adaptiva Customer Support

Select Third Party Products

1. Decide whether to integrate with third party products. You may choose to integrate with one product only:
 - If integrating with ConfigMgr, select **Integrate an Existing Microsoft ConfigMgr Site**. Skip to section Installation Settings for OneSite with ConfigMgr
 - If integrating with ommissa Workspace ONE, select **Integrate With Workspace One**. Skip to section Installation Settings for OneSite for ommissa Edition
 - To continue without integrating any products, leave them unchecked. Skip to section Database Settings
2. Click **Next** to continue to the next screen
3. If the port entered for either the Web UI HTTP Port or the Client HTTP Communications HTTP Port is currently in use the following will be displayed



Click OK to return to the Integrate Third Party Products screen and enter a port that is not currently in use.

Integrate an Existing Microsoft ConfigMgr Site

The Site Server information screen provides information about the ConfMgr Site Server that the Adaptiva Server will be integrated with. This integration requires access to the SMS Provider, ConfigMgr database, Site Server inboxes and the Content Library file system hosted by the Site Server. If Integrate with an Existing ConfigMgr Site was selected, the following screen is displayed.

1. Enter the Site Server details using the information gathered during Deployment Planning:

Adaptiva Server Installer - (C) 2010 Adaptiva

Please Provide Information For The Site Server To Which This Adaptiva Server Will Connect

Site Server Information

Site Server

Machine Name: FQDN

Site Code: xxx

ConfigMgr Site Login

☒ Use Adaptiva Server's Local System Account

Domain

User Name:

Password:

Confirm Password:

Prev Next Cancel

- Enter the Machine Name (FQDN) of the ConfigMgr Site Server that hosts the SMS Provider.
- Enter the three-character site code of the ConfigMgr site.

2. Enter the **ConfigMgr Site Login** details gathered during Deployment Planning:

Adaptiva Server Installer - (C) 2010 Adaptiva

Please Provide Information For The Site Server To Which This Adaptiva Server Will Connect

Site Server Information

Site Server

Machine Name: FQDN

Site Code: xxx

ConfigMgr Site Login

☒ Use Adaptiva Server's Local System Account

Domain

User Name:

Password:

Confirm Password:

Prev Next Cancel

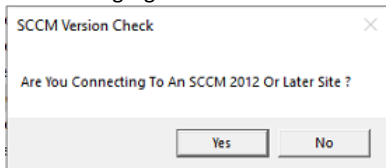
- Adaptiva recommends selecting **Use Adaptiva Server's Local System Account** (default). This is the simplest method of authentication of an Adaptiva Server connection with ConfigMgr.

NOTE: If the Adaptiva Server is not co-located with the ConfigMgr Site Server you must grant the Adaptiva Server's computer object the necessary permissions in Configuration Manager.

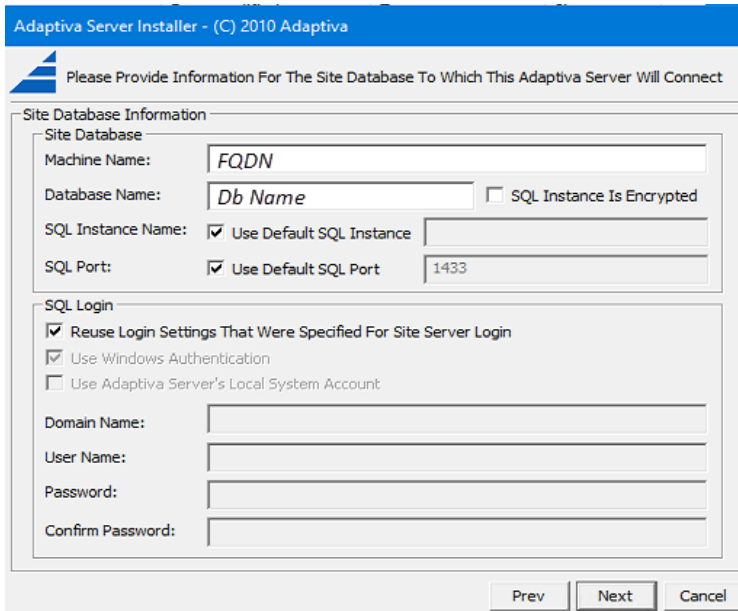
- If you choose not to use the Local System Account, enter the Netbios Domain name, User Name and Password for the domain account that has been granted the necessary permissions in Configuration Manager.

3. Click **Next**

4. If the ConfigMgr site server is a different server, the following will be displayed



Select Yes to continue to the Site Database Information screen.



Adaptiva Server Installer - (C) 2010 Adaptiva

Please Provide Information For The Site Database To Which This Adaptiva Server Will Connect

Site Database Information

Site Database

Machine Name: FQDN

Database Name: Db Name ☐ SQL Instance Is Encrypted

SQL Instance Name: ☒ Use Default SQL Instance

SQL Port: ☒ Use Default SQL Port 1433

SQL Login

☒ Reuse Login Settings That Were Specified For Site Server Login

☒ Use Windows Authentication

☐ Use Adaptiva Server's Local System Account

Domain Name:

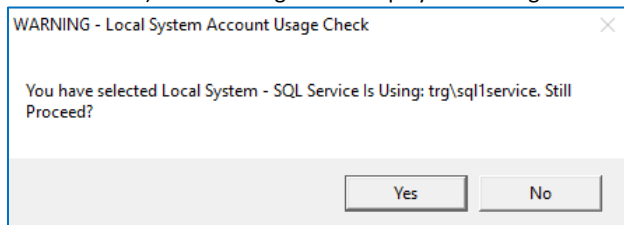
User Name:

Password:

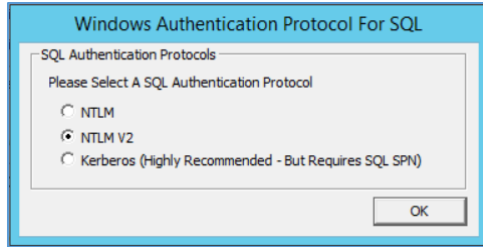
Confirm Password:

Prev Next Cancel

- **Machine Name** contains the FQDN of the ConfigMgr SQL Server.
- **Database Name** contains the ConfigMgr database name.
- The other settings: **SQL Instance Name** and **SQL Port** will all be updated automatically from settings obtained using the logged in user's permissions to the ConfigMgr Site Server.
- If the SQL Server Instance is using encryption select **SQL Instance Is Encrypted**
- **Reuse Login Settings That Were Specified For Site Server Login** is selected by default. Uncheck this box to specify the account information that will connect to the ConfigMgr database SQL Server.
- If you choose not to use the Local System Account, enter the NETBIOS Domain name, User Name and Password for the domain account that has been granted the necessary permissions in Configuration Manager. Uncheck Use Windows Authentication to specify an account created in SQL Server.
- Click **Next** to continue to the Adaptiva Database Options
- If the account specified is different from the login account used for the service SQL Server (MSSQLSERVER | InstanceName) the following will be displayed showing the account used by the SQL Service



- If the settings are correct, click **Yes**, otherwise, click **No** and update the settings.
- At the SQL Authentication Protocols dialog, select the authentication method that will be used to connect to the ConfigMgr Site database.

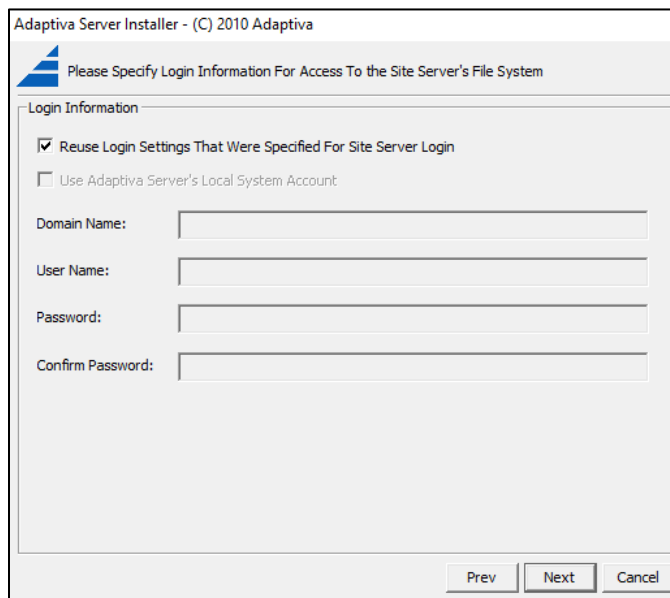


- i. Select NTLM v2 (Default) when the ConfigMgr and Adaptiva databases are hosted on the same SQL server.
- ii. Select Kerberos when the ConfigMgr and Adaptiva databases are hosted on different SQL servers or additional security is required. To support Kerberos authentication, Service Principal Names (SPNs) must be created and delegated properly in Active Directory. See Appendix B in this document.
- iii. Click **OK** to continue to the Login Information To Access the Site Server's File System screen

Specify Login Information for Accessing Site Server Files

The Login Information For Access To the Site Server's File System screen allows you to specify an account that has the necessary permissions to access the Site Server's file system. Specifically, this account must be able to access the inboxes and the Content Library. Review the table of permissions required in the Deployment Planning for ConfigMgr Edition for potential actions required for this account.

1. At the **Login Information** screen, enter information to access the ConfigMgr file system.

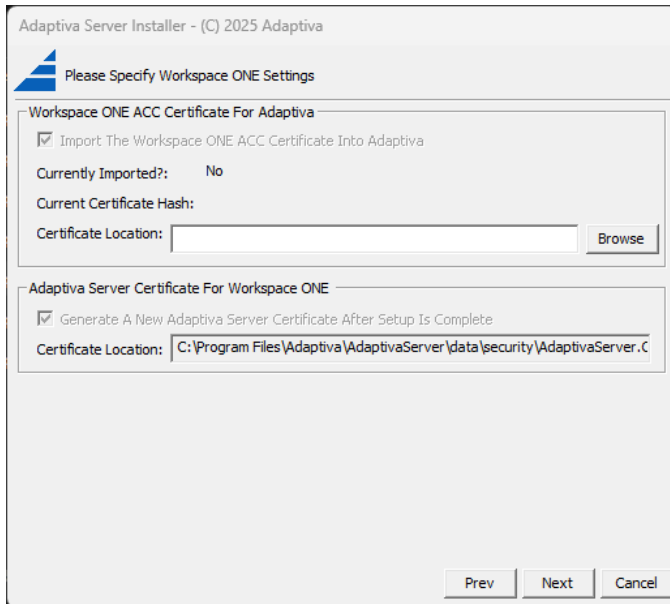


- Reuse Login Settings That Were Specified For Site Server Login is the default. Uncheck to specify an account
 - If the Site Server Login screen used a named account but the File System requires using the Adaptiva server's System account, check Use Adaptiva Server's Local System Account
 - If you choose not to use the Local System Account, enter the Netbios Domain name, User Name and Password for the domain account that has been granted the necessary permissions in Configuration Manager.
2. Click Next to continue to Options for Creating the Adaptiva SQL Database

Integrate with Workspace ONE

If **Integrate with WorkSpace ONE** was selected, the following screen is displayed.

1. At the **Please Specify Workspace ONE Settings** screen, enter the path or browse to the location of the downloaded ACC certificate.



The screenshot shows the 'Please Specify Workspace ONE Settings' dialog box. It has two main sections. The first section, 'Workspace ONE ACC Certificate For Adaptiva', contains a checked checkbox 'Import The Workspace ONE ACC Certificate Into Adaptiva', a label 'Currently Imported?: No', a label 'Current Certificate Hash:', and a 'Certificate Location:' field with a 'Browse' button. The second section, 'Adaptiva Server Certificate For Workspace ONE', contains a checked checkbox 'Generate A New Adaptiva Server Certificate After Setup Is Complete' and a 'Certificate Location:' field with the path 'C:\Program Files\Adaptiva\AdaptivaServer\data\security\AdaptivaServer.c'. At the bottom are 'Prev', 'Next', and 'Cancel' buttons.

2. Record the location where the **Adaptiva Server Certificate For Workspace ONE** will be located after a successful installation: By default, this is: `<Path>\Adaptiva\AdaptivaServer\data\security`
3. Skip to the section: **Options for Creating the Adaptiva SQL Database**

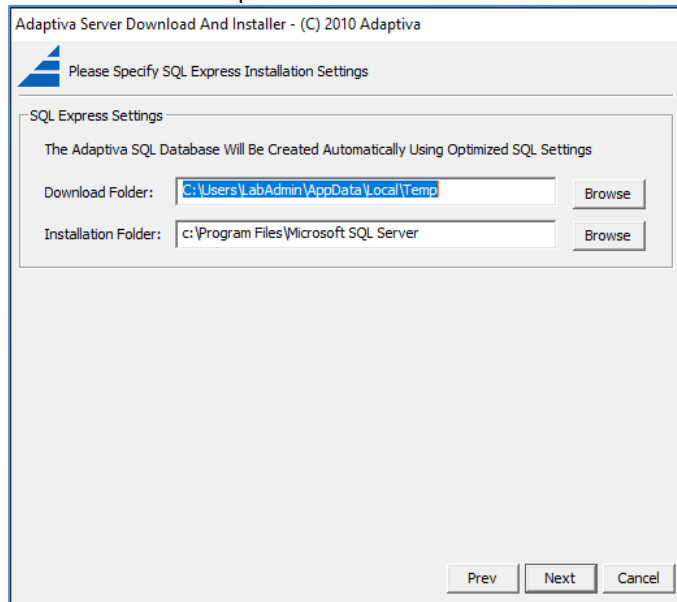
Options For Creating the Adaptiva SQL Database

The Options for Creating the Adaptiva SQL Database screen allows you to choose where the Adaptiva database will be located. Refer to the Deployment Planning for OneSite Anywhere.

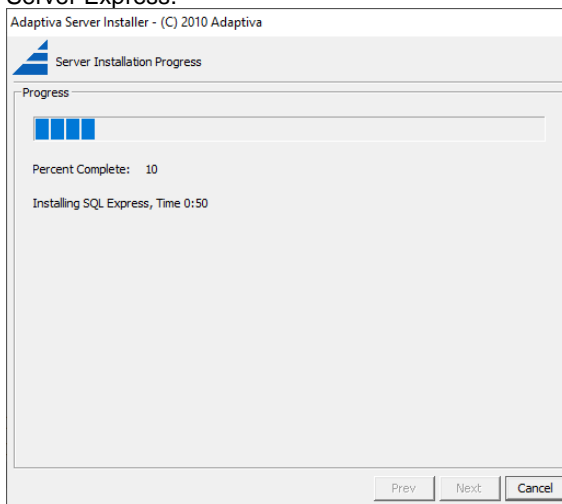
1. Select the option where the Adaptiva database should be created.
 - If using SQL Express Edition, choose the option Download And Install Free Microsoft SQL Express And Auto-create Adaptiva Database.
Follow the instructions in the section **Error! Reference source not found.**
 - If using an existing SQL Server Instance, choose the option Create The Adaptiva Database In An Existing SQL Server Instance.
Follow the instructions in the section **Error! Reference source not found.**
 - If using the same SQL Instance as the ConfigMgr database, choose the option Create the Adaptiva Database In The Same SQL Instance As ConfigMgr.
Follow the instructions in the section **Error! Reference source not found.**

Download and Install Free Microsoft SQL Express And Auto-create Adaptiva Database

1. At the SQL Express Settings screen enter where the SQL Server Express installer should be downloaded to and where SQL Server Express will be installed



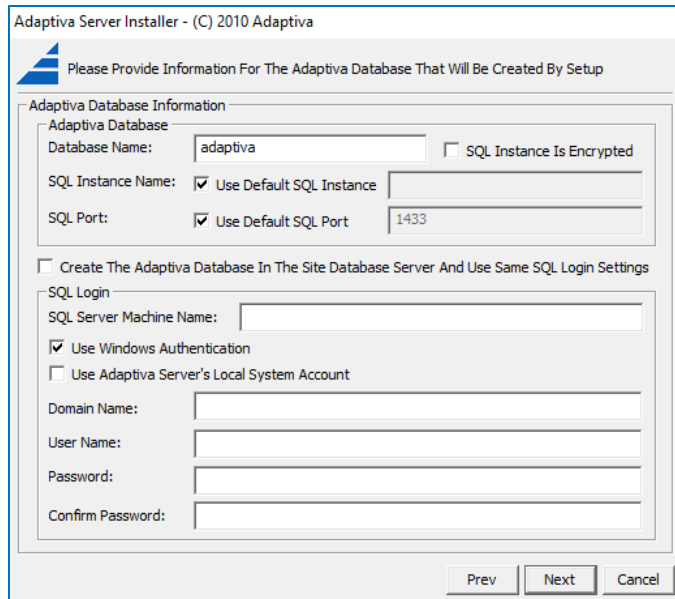
2. Click **Next**
3. The wizard will begin the download of SQL Server Express. Once downloaded, it will install and configure SQL Server Express.



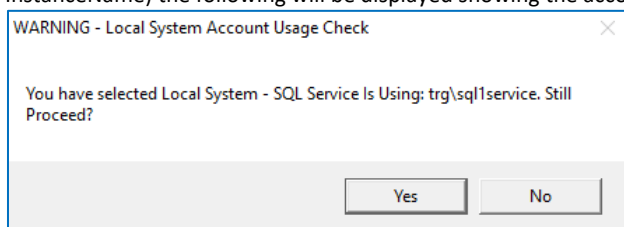
4. Skip to the section: **Read-Only SQL Login For Adaptiva Reporting**

Create The Adaptiva Database In An Existing SQL Server Instance

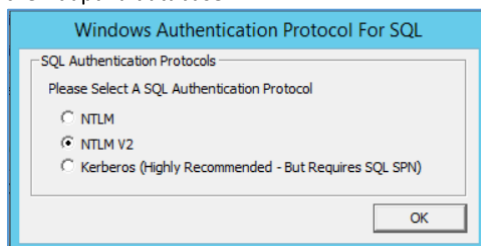
1. At the **Adaptiva Database Information** screen enter the SQL Server information. See the descriptions below, then click **Next**



- **Database Name** contains the Adaptiva database name.
- If the SQL Server Instance is using encryption select **SQL Instance Is Encrypted**
- If the Default SQL Instance is not used, uncheck the box and enter the SQL Instance name
- If the Default SQL Port is not used, uncheck the box and enter the SQL Port
- Because you selected Create the Adaptiva Database in an existing SQL Server instance the box for Create the Adaptiva Database in the Site Database Server and use Same SQL Login Settings will not be checked
- Enter the SQL Server Machine Name FQDN
- If you choose not to use the Local System Account, enter the NETBIOS Domain name, User Name and Password for the domain account that has been granted the necessary permissions in Configuration Manager. Uncheck Use Windows Authentication to specify an account created in SQL Server.
- Click **Next** to continue to the Read-Only SQL Login For Adaptiva Reporting screen.
- If the account specified is different from the login account used for the service SQL Server (MSSQLSERVER | InstanceName) the following will be displayed showing the account used by the SQL Service.



- If the settings are correct, click **Yes**, otherwise, click No and update the settings.
- At the SQL Authentication Protocols dialog, select the authentication method that will be used to connect to the Adaptiva database.

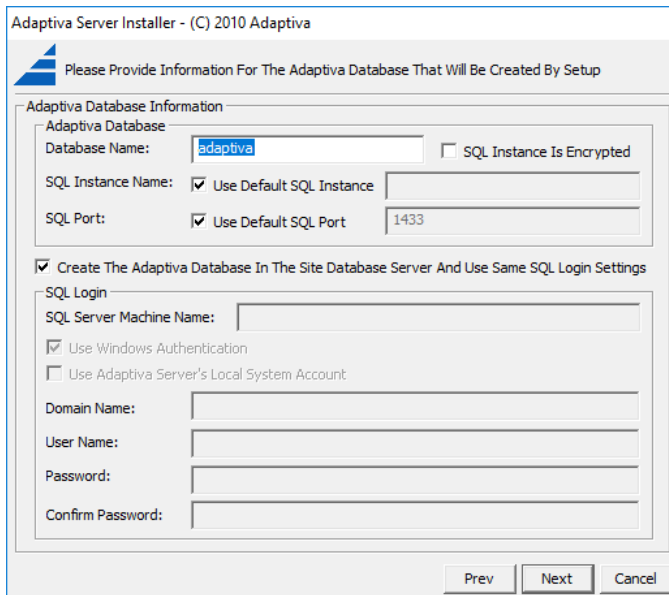


- i. Select NTLM v2 (Default) when the ConfigMgr and Adaptiva databases are hosted on the same SQL server

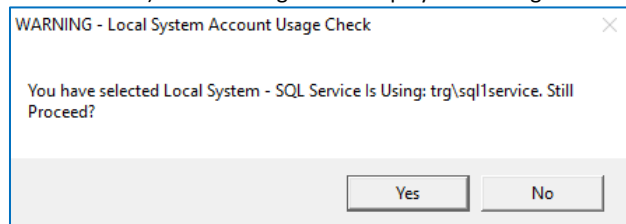
- ii. Select Kerberos when the ConfigMgr and Adaptiva databases are hosted on different SQL servers or additional security is required. To support Kerberos authentication, Service Principal Names (SPNs) must be created and delegated properly in Active Directory. See Appendix B in this document.
 - iii. Click **OK** to continue to the Login Information To Access the Site Server's File System screen
- 4. Skip to the section: Read-Only SQL Login For Adaptiva Reporting

Create the Adaptiva Database In The Same SQL Instance As ConfigMgr

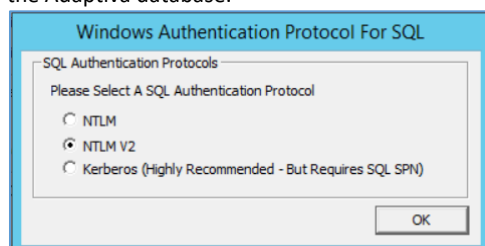
1. At the Adaptiva Database Information screen the settings should not need changing as they were reused from the ConfigMgr database information. The SQL Instance Name and Port could be changed if required, then click **Next**



- **Database Name** contains the Adaptiva database name.
- If the SQL Server Instance is using encryption select **SQL Instance Is Encrypted**
- If the Default SQL Instance is not used, uncheck the box and enter the SQL Instance name.
- If the Default SQL Port is not used, uncheck the box and enter the SQL Port
- Because you selected Create the Adaptiva Database in the same SQL Server instance as ConfigMgr the box for Create the Adaptiva Database in the Site Database Server and use Same SQL Login Settings will be checked.
- SQL Server Machine Name will contain the SQL Server server FQDN.
- If you choose not to use the same settings, enter the NETBIOS Domain name, User Name and Password for the domain account that has been granted the necessary permissions in Configuration Manager.
- Uncheck Use Windows Authentication to specify an account created in SQL Server.
- Click **Next** to continue to the Read-Only SQL Login For Adaptiva Reporting screen.
- If the account specified is different from the login account used for the service SQL Server (MSSQLSERVER | InstanceName) the following will be displayed showing the account used by the SQL Service



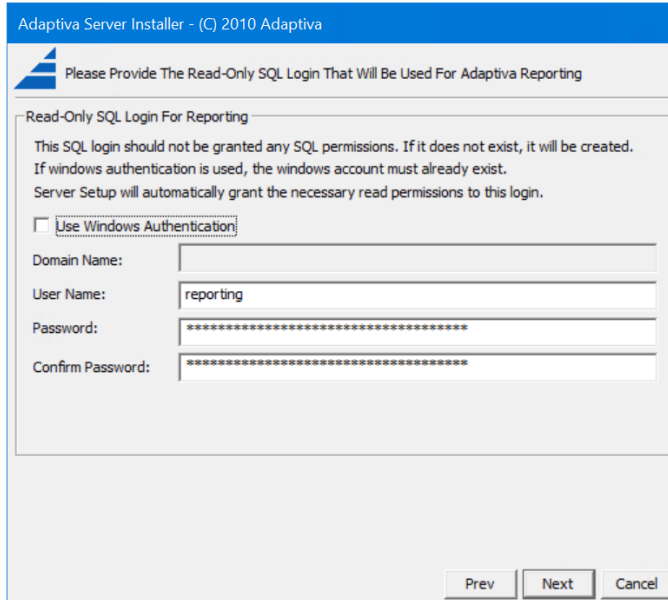
- If the settings are correct, click **Yes**, otherwise, click No and update the settings.
- At the SQL Authentication Protocols dialog, select the authentication method that will be used to connect to the Adaptiva database.



- i. Select NTLM v2 (Default) when the ConfigMgr and Adaptiva databases are hosted on the same SQL server
- ii. Select Kerberos when the ConfigMgr and Adaptiva databases are hosted on different SQL servers or additional security is required. To support Kerberos authentication, Service Principal Names (SPNs) must be created and delegated properly in Active Directory. See Appendix B in this document.
- iii. Click **OK** to continue to the Read-Only SQL Login For Adaptiva Reporting screen

Read-Only SQL Login For Adaptiva Reporting

1. At the **Read-Only SQL Login For Reporting** screen, complete the fields as follows:



Use Windows Authentication – Check this if the reporting account has been created in the domain. This box will be checked and greyed out when Windows Authentication mode has been specified in SQL Server.

IMPORTANT: When SQL Server is remote from the Adaptiva Server, the installation will only be able to use Windows authentication.

Domain Name – Enter the NETBIOS domain name used for the reporting account. Leave blank if **Use Windows Authentication** is unchecked and a SQL Login account is to be used.

User Name – Enter the account name to use for the reporting account.

Password – Enter the password for the reporting account.

Confirm Password – Confirm the password that you entered above.

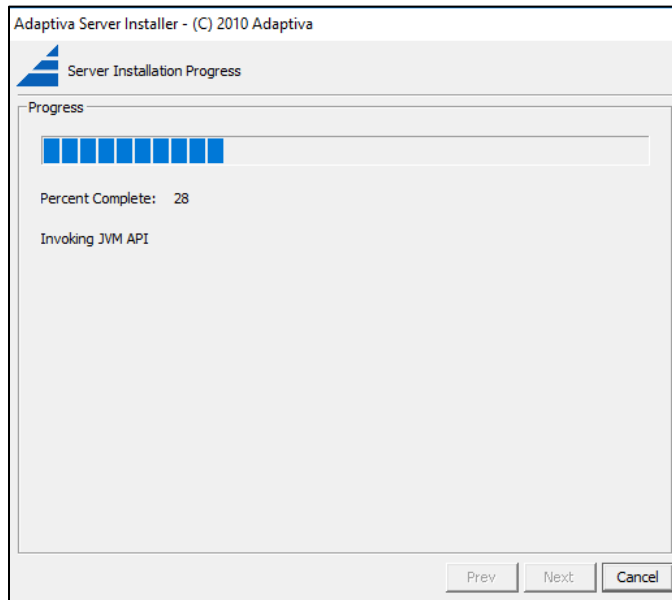
2. Click **Next** when complete, and then go to the [Completing the Installation](#) section.

Completing the Installation

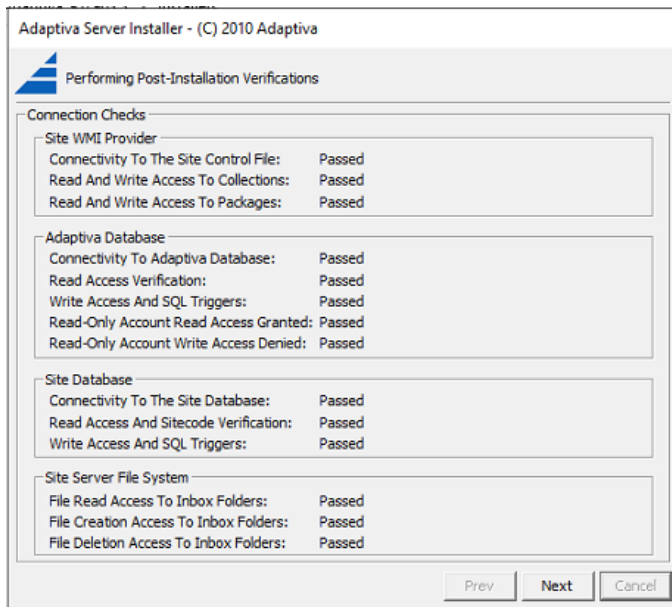
1. The installation will progress.

Be Patient. Sometimes it will seem to hang at around 80%. It will finish.

- When it reaches 100%, click **Next**

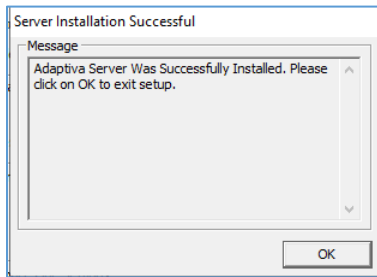


- Once the installation is complete, a post-installation verification will run, verifying all of the chosen accounts and settings. Click **Next**



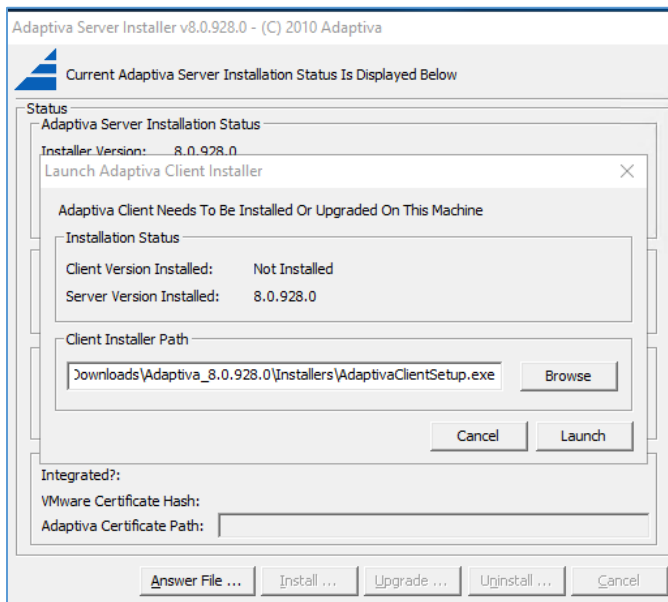
NOTE: Some of these will be skipped based on the integrations selected. Also, there is a known issue when the Kerberos authentication protocol is selected for the Adaptiva database: The Read-Only Account Write Access Denied will report Failed. This can be ignored.

- Click **OK** to complete the Adaptiva server installation.

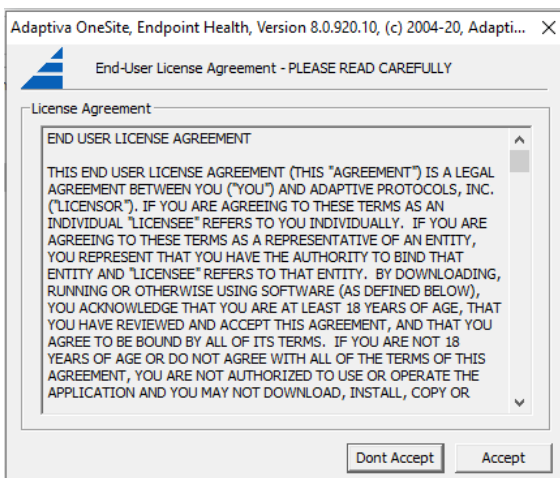


Adaptiva Client Installation on the Server

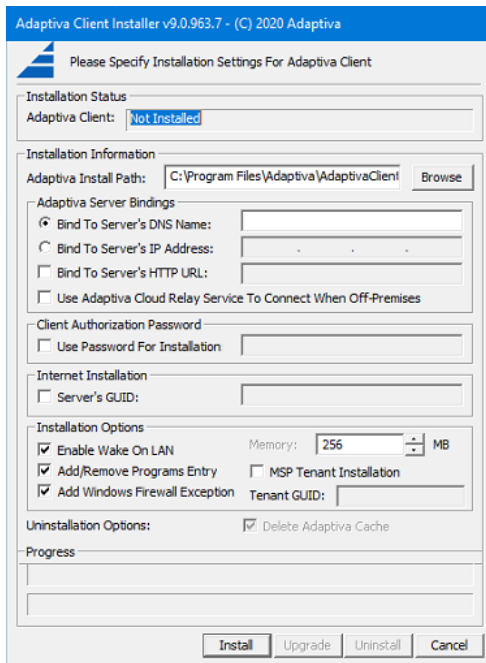
- After the Adaptiva Server is installed, the Adaptiva Client must be installed on the server. At the **Launch Adaptiva Client Installer** dialog, the Client Installer Path will be displayed based on the relative path the server component was installed from.
- Click **Launch** to begin the Client installation.



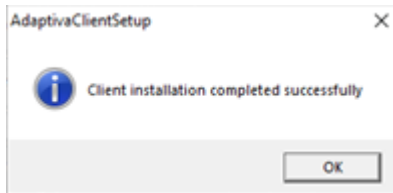
- At the **License Agreement** screen, click **Accept** to continue.



- At the **Adaptiva Client Installer** dialog, verify desired **Adaptiva Install Path**, then click **Install**.



- Click **OK** at the **Success** dialog.



Server Installation Log

In the case where an administrator needs to troubleshoot an Adaptiva Server installation, the following table contains the installation log locations. Other logs exist in the installation folder.

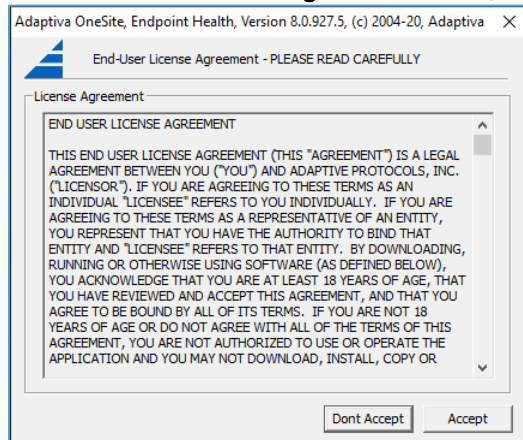
Function	Log Location and Name
Server Installation Logs	%windir%\AdaptivaSetupLogs\Server\AdaptivaServerSetup.log <path>\Adaptiva\AdaptivaServer\logs\Adaptiva.#.log
Client Installation Log	%windir%\AdaptivaSetupLogs\Client\AdaptivaClientSetup.log

Create Silent Installation Answer file

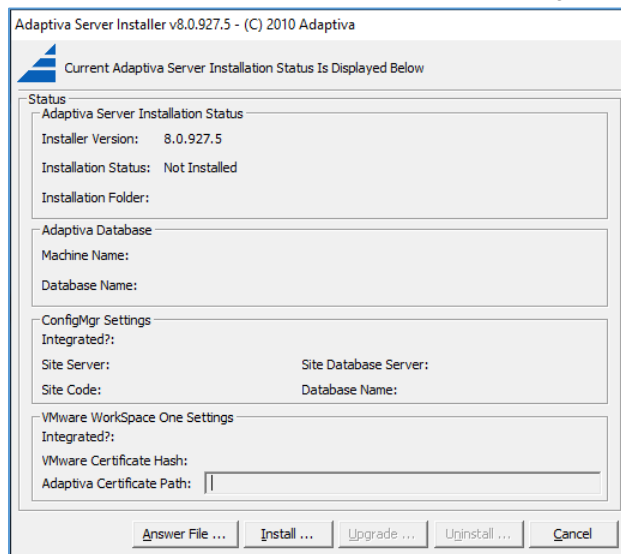
An answer file can be created to automate the installation of the Adaptiva server. The executable must be run with Administrative privileges. The answer file can only be created when the Adaptiva Server has not been previously installed.

- Execute **AdaptivaServerSetup.exe** as the Administrator

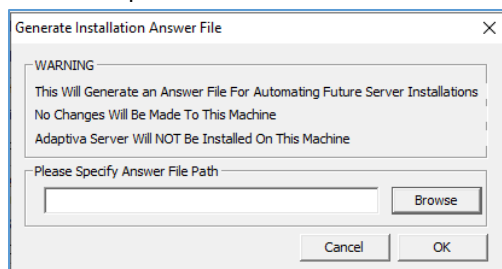
2. At the **End-User License Agreement** screen, click **Accept**



3. At the **Status** screen, click the **Answer File...** to begin the process

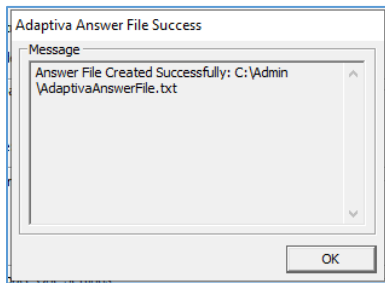


4. At the Generate Installation Answer File, click on **Browse** to select the folder where the file will be created. Open the appropriate folder, creating a new folder if necessary, and click **Save**. Click **OK**. The answer file will be named AdaptivaAnswerFile.txt in the folder selected.



The installation screens will proceed as described in the Server Installation section. Each answer will be saved in the Answer file. The installation will NOT install the product. Use the Server Installation section below to learn about each screen during the installation process.

- When all the prompting screens are complete the answer file is created. Click **OK**.



The installation process will end.

NOTE: If passwords were entered for the SuperAdmin ID or Service accounts, these passwords will be stored in clear text in the Answer File. Delete or secure the answer file after the installation has been completed.

Installation using the Answer File

If you have created an answer file, follow these steps to use the answer file to install the Adaptiva OneSite Server.

NOTE: Answer files should be created for each version as some parameters might change.

NOTE: If passwords were entered for the SuperAdmin ID or Service accounts, these passwords will be stored in clear text in the Answer File. Delete or secure the answer file after the installation has been completed.

- Open a Command Prompt as Administrator
- Change to the installation source folder
- Enter the following command:

```
AdaptivaServerSetup.exe -InstallOrUpgrade <path>:\<AnswerFileName>
```

For example: AdaptivaServerSetup.exe -InstallOrUpgrade c:\admin\AdaptivaAnswerFile.txt

- There is no progress bar during the installation. The installation can be monitored using the Task Manager, monitoring the AdaptivaServerSetup.exe process and by monitoring the log file c:\windows\AdaptivaSetupLogs\Server\AdaptivaServerSetup.log using CMTrace or equivalent.
- Upon a successful installation the AdaptivaServerSetup.exe process will be replaced with AdaptivaServerService and the AdaptivaServerSetup.log will show:

```
~performSilentServerInstall(): 2C58: Line: 160: Server installation was successful
```

NOTE: The server installation normally launches the AdaptivaClientSetup.exe to install the Adaptiva Client. The silent installation does not do this. Be sure to install the Adaptiva Client using AdaptivaClientSetup.exe

Post-Install Instructions

Add Certificate to the Root Store

Starting in Build 8.2 the Adaptiva Server will default to enabling TLS for the Admin Portal via a self-signed certificate. Alternatively, a certificate authority can be used.

If a self-signed certificate was selected, you should import the certificate into the Trusted Root Certification Authorities container on the device. Each Adaptiva Administrator who will use the Admin Portal from a remote device will need to import the certificate. Alternatively, the certificate can be deployed using a GPO or Intune policy.

If the certificate will be automatically imported, this step can be skipped.

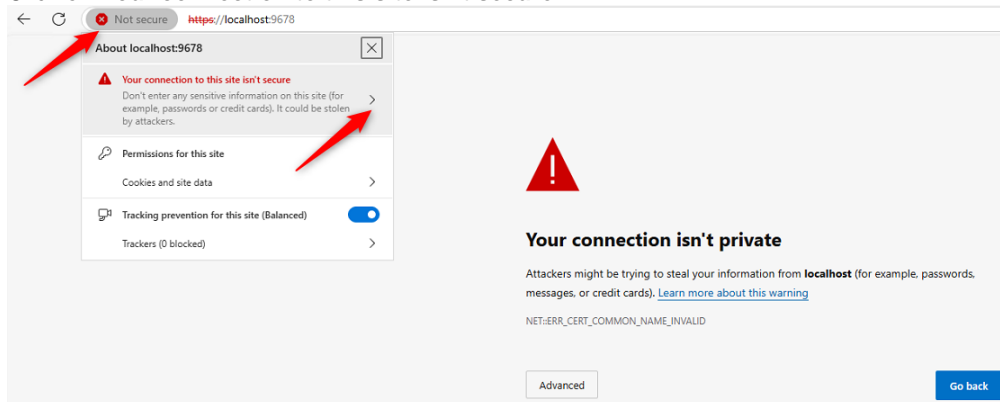
Complete the following process:

- The certificate is stored in the registry at hklm\SOFTWARE\Adaptiva\server\certificates.cloudui_public_cert
- The data can be saved into a UTF-8 formatted text file with a .crt extension
- See the steps below to Install the certificate

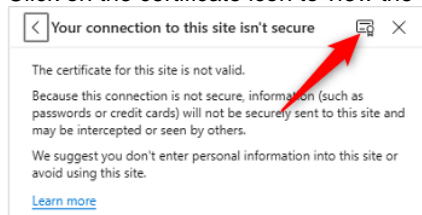
OR

- In your Browser, enter the Adaptiva server name with optional :port [https://adaptivaservername\[:port\]](https://adaptivaservername[:port])

2. You will see the message Your connection isn't private
3. Click on the text **Not secure** next to the Address URL
4. Click on **Your connection to this site isn't secure**



5. Click on the certificate icon to view the certificate



6. Select the **Details** tab
7. Click on **Export**
8. Select a destination (your Downloads folder) - leave the default filename of adaptiva.crt
9. Close the browser

Complete the next steps to install the certificate

1. Open File Explorer and browse to where you saved the above file
2. Find the file and double-click on it
3. Select **Install Certificate...**
4. Select Local Machine (recommended) and click Next
5. Select Place all certificates in the following store
6. select Browse and select Trusted Root Certification Authorities and click OK then click Next
7. Click Finish

OR

1. Run the command
Certutil.exe -addstore root "<path>\adaptiva.crt"

Test the certificate

1. In your Browser, enter the Adaptiva server name with optional :port [https://adaptivaservername\[:port\]](https://adaptivaservername[:port])
2. You will now see the Adaptiva Login Page
3. There will now be a lock icon next to the URL

Content Library Location

The Content Library will default to Adaptiva Server installation folder

<Path>\Adaptiva\AdaptivaServer\Data\ContentLibrary. Consider moving the Content Library to a dedicated drive.

IMPORTANT: Ensure this drive is backed up or replicated.

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

SQL Database Configuration

By default, the installation account is assigned as the owner of the Adaptiva database. SQL best practice is to set the SA account to the owner.

1. In **SQL Management Studio**, right-click on the **adaptiva** database and select **Properties**
2. Select the **Files** page. Change the Owner to **SA**
3. Select the **Options** page. Verify the Recovery model is set to **Simple**

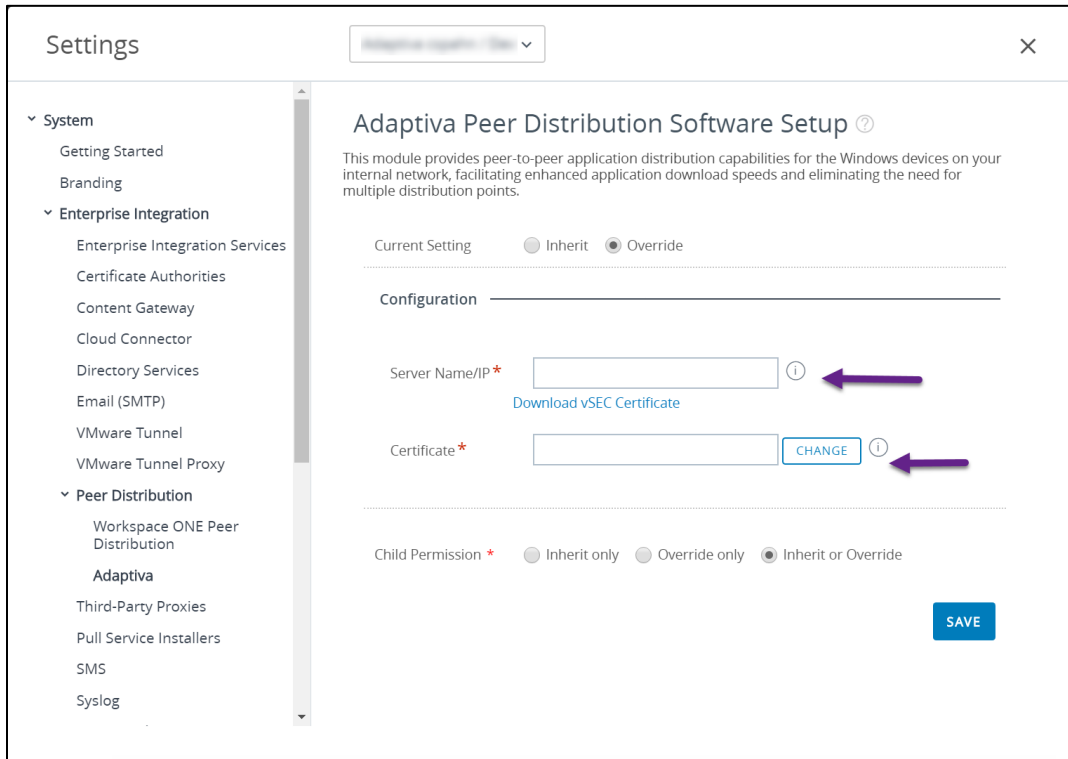
NOTE: If the Adaptiva database will be part of a SQL Always On Availability Group, the Recovery model should be set to Full

Finalizing the Workspace ONE Integration

This is only applicable if the Workspace ONE integration was selected.

After a successful installation, return to the Workspace ONE UEM console to complete the integration of the two platforms.

1. Navigate to the Adaptiva settings page (**Groups & Settings > All Settings > System > Enterprise Integration > Peer Distribution > Adaptiva**) and enter either the name or the internal IP address of the Adaptiva server. This will allow the ACC to communicate with the Adaptiva server on the internal network.
2. Upload the Adaptiva Server certificate so the authentication between the ACC and Adaptiva services is secure. Recall the certificate was saved here: `<InstallPath>\Program Files\Adaptiva\AdaptivaServer\data\security\AdaptivaServer.cer`




Settings

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/IP* ⓘ 

[Download vSEC Certificate](#)

Certificate* [CHANGE](#) ⓘ 

Child Permission* ☐ Inherit only ☐ Override only ☒ Inherit or Override

[SAVE](#)

- Click **Save** and the system will save the settings and immediately perform a health check to validate communications and then initiate publication of application metadata to the Adaptiva Server.

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/IP * ?

[Download vSEC Certificate](#)

Certificate * CHANGE ?

Troubleshooting

HEALTH CHECK ? ✓

Last Checked Wednesday, October 2, 2019 7:53:05 AM (UTC-08:00) Pacific Time (US & Canada)

Installed Version 7.0.853.0

PUBLISH CONTENT ?

Publish Queued

Publish Initiated Wednesday, October 2, 2019 7:53:12 AM (UTC-08:00) Pacific Time (US & Canada)

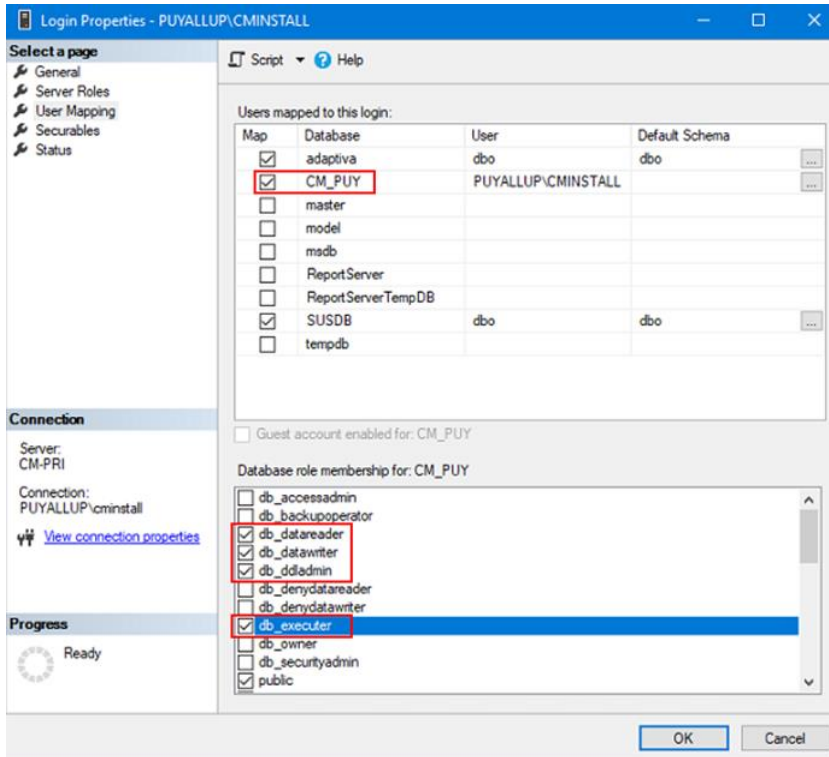
(Optional) Reducing SQL permissions

To remove SQL sysadmin access from the account

- Stop the **AdaptivaServer** service
- In **SQL Management Studio**, open a **New Query** window for the ConfigMgr database and **Execute** the following:

```
CREATE ROLE db_executer
GRANT EXECUTE TO db_executer
```
- Repeat the above step against the Adaptiva database
- Expand **Security**, **Logins** folder, right-click the Installation account / service account and select **Properties**
- Select the **Server Roles** page and uncheck the server role: **sysadmin**
- In the **Users mapped to this login** section, select the **adaptiva** database, and under the database role membership, select the following roles:
db_datareader
db_datawriter
db_ddladmin
db_executer
- In the **Users mapped to this login** section, select the **ConfigMgr** database, and under the database role membership, de-select the db_owner role, and select the following fixed roles:
db_datareader
db_datawriter

db_ddladmin
db_executer



8. Click **OK** when complete
9. Start the **AdaptivaServer** service

Workbench Installation

The Adaptiva Workbench is the interface for communicating with the Adaptiva Server and performing configuration of OneSite and Endpoint Health. The workbench can be installed on any machine with network connectivity to the Adaptiva Server. It can also be installed on as many machines as required.

NOTE: While many of the Workbench features are now available in the Admin Portal, there are a few features that can only be completed using the Workbench. It is recommended to install the Workbench on the Adaptiva Server.

The Adaptiva Workbench is not installed on the Adaptiva server as part of the server installation, so the installation must be invoked manually.

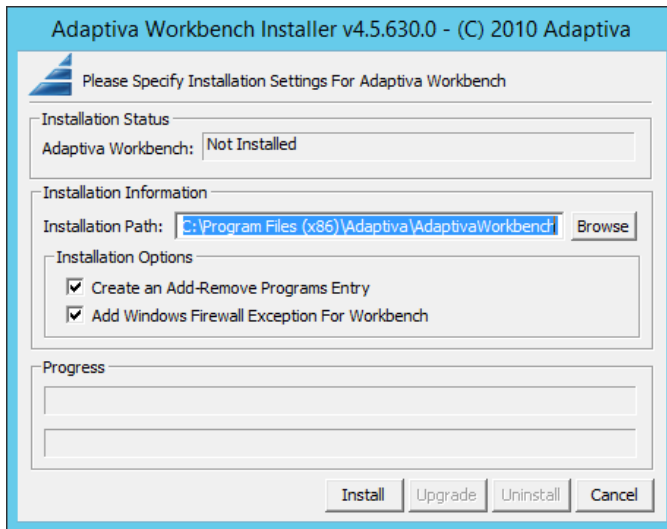
The Adaptiva Workbench supports a manual attended installation as well as a silent unattended installation. See the below sections for details on each option.

To install the Adaptiva workbench component, use the **AdaptivaWorkbenchSetup.exe** executable which can be found in the Installation source folder and must be run with elevated privileges.

Manual Attended Installation

1. Run the **AdaptivaWorkbenchSetup.exe** executable as Administrator to start the installation
2. At the **License Agreement** screen, click **Accept** to continue

3. In the **Installation Information** screen, make any desired modifications then click **Install**



4. Once complete, click **OK** to close the installer. A shortcut to the Adaptiva Workbench can be found in the Start Menu

Silent Unattended Installation

The Adaptiva Workbench can be installed silently by calling AdaptivaWorkbenchSetup.exe with the following command line options:

Parameter	Usage
Required	
-cleaninstall	Installs a fresh workbench, removing previous installation if any.
-installorupgrade	Installs or upgrades the workbench, as appropriate.
-uninstall	Uninstalls the existing workbench.
Optional	
-folder	The desired installation path.
-noarp	The installer will NOT create an entry in Add/Remove Programs.
-nofirewall	The installer will NOT create Windows Firewall rules for the Adaptiva Workbench.

These installation parameters can be viewed at any time by using the -? or -help switches when calling AdaptivaWorkbenchSetup.exe.

Workbench Installation Log

In the case where an administrator needs to troubleshoot an Adaptiva Workbench installation, the following table contains the installation log location. Other logs exist in the installation folder.

Function	Log Location and Name
Workbench Installation Log	%windir%\AdaptivaSetupLogs\Workbench\AdaptivaWorkbenchSetup.log

Installing the License Key

After the Adaptiva Server setup is complete, enable one of the evaluation licenses or install your Adaptiva-provided license key to enable the product. This will activate the product and prepare to license clients.

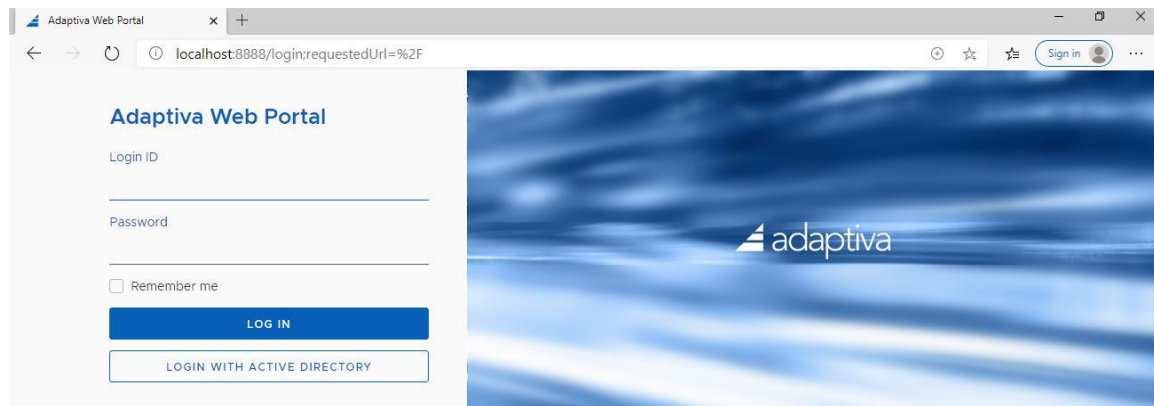
IMPORTANT: License keys can only be added via the Adaptiva Admin Portal

1. In a web browser (except Internet Explorer), enter one of the following addresses:

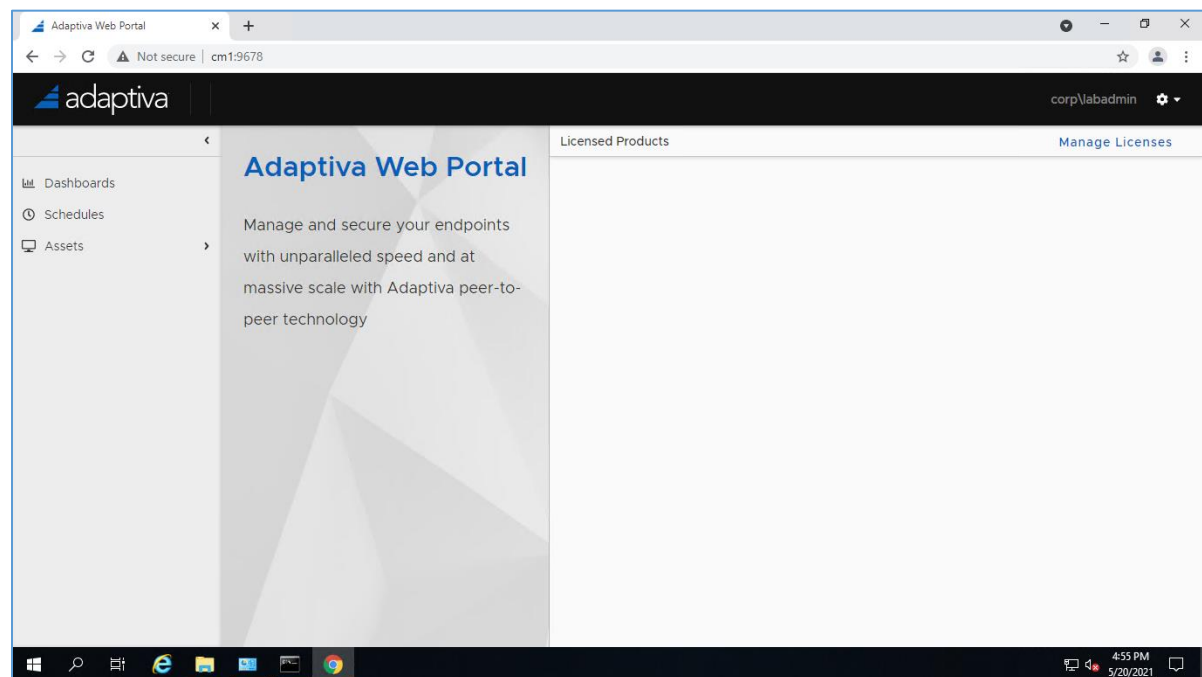
- If https is enabled – Enter the following:
<https://AdaptivaServerFQDN>
- If a custom port was configured – Enter the following:
<http://AdaptivaServerFQDN:customport>


2. At the Adaptiva Web Portal, click **Login with Active Directory**.

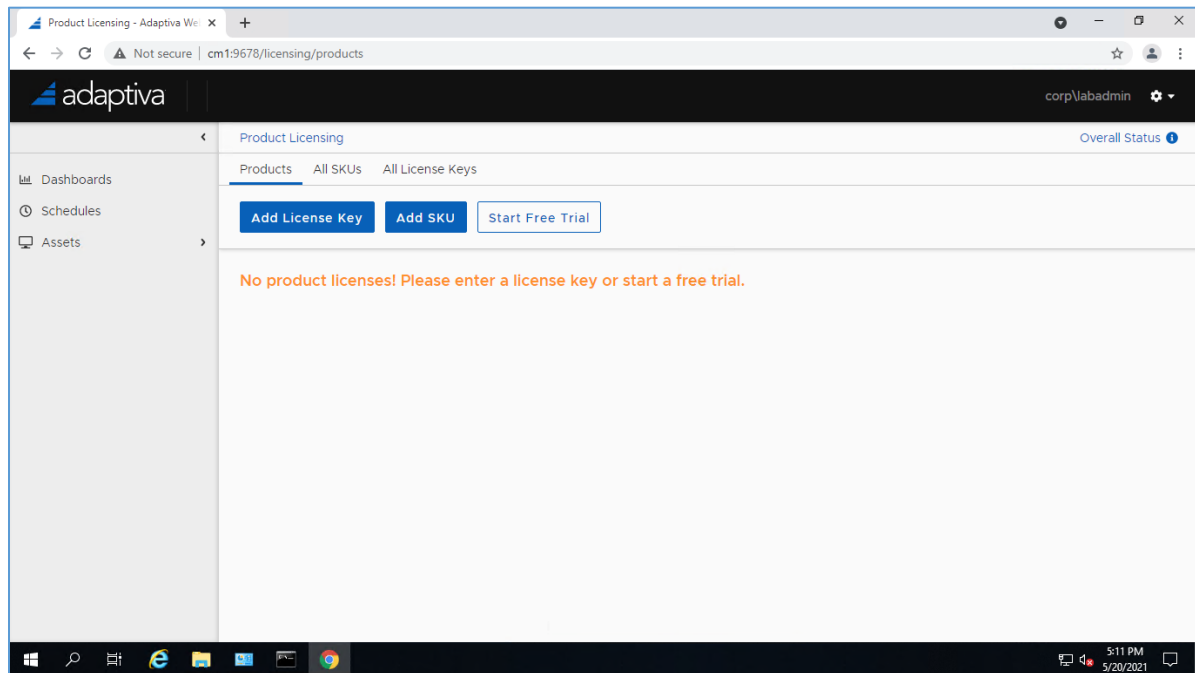
If an Adaptiva login account was created, enter the email address and password created during installation and click **LOG IN**.



3. After logging in, the Adaptiva Web Portal will be displayed. A license must be added to activate the features of that product in the Adaptiva Web Portal.



4. Click **Manage Licenses**, or from the , select **Product Licensing**.



5. Click **Add License Key**, **Add SKU** or **Start Free Trial**.
- If a License Key was provided, click **Add License Key**, enter the provided License Key and then click **OK**
 - If a SKU was provided, click **Add SKU**, enter the provided SKU and then click **OK**.
 - When **Start Free Trial** is selected, check the box(es) to select the product(s), or check **Select All**, and then click **OK**.

×
Enable Free Trial

Select Products

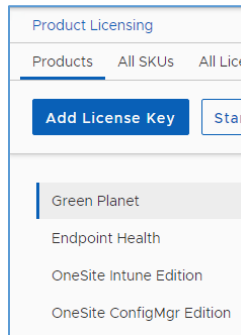
☐ Select All

☐ Endpoint Health

☐ OneSite Intune Edition

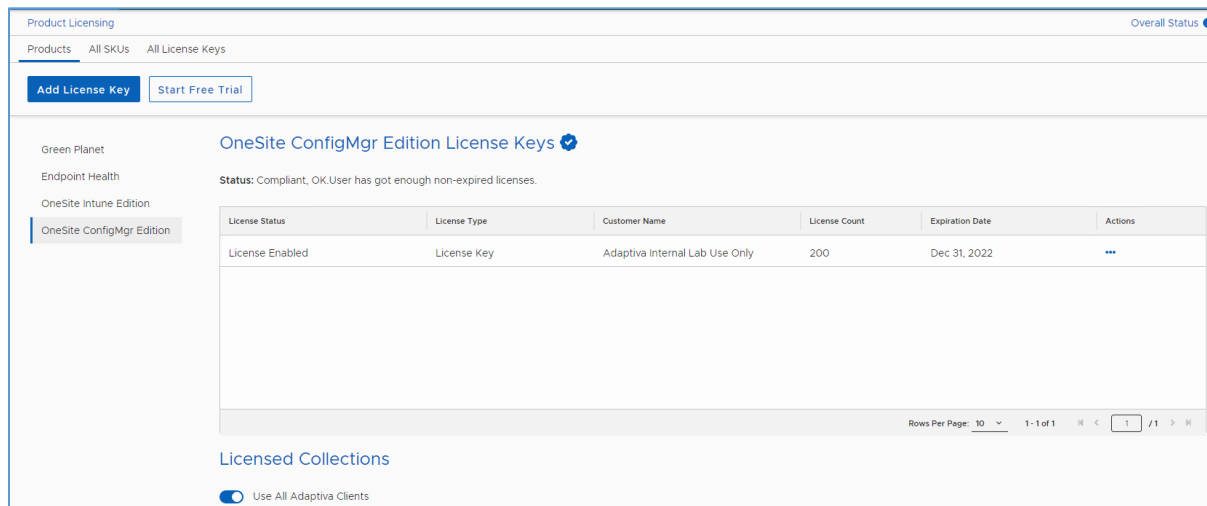
☐ OneSite ConfigMgr Edition

- Notice the enabled products will be listed on the left.

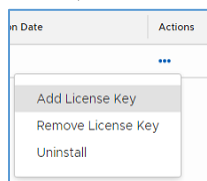


- Select each enabled product to review the current license status.

Notice the **License Count**, **Expiration Date** and specific **Licensed Collections** of devices targeted to receive the license.



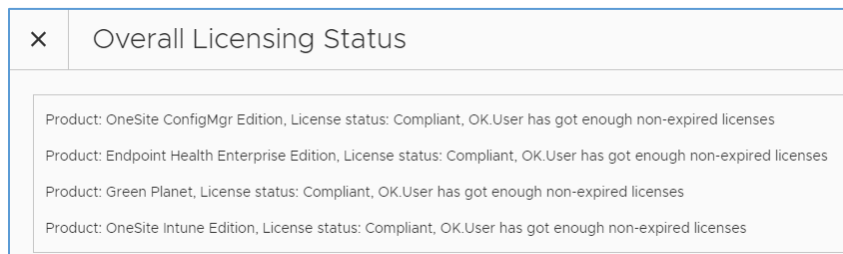
Clicking on the ellipses (...) under the **Actions** column will display this menu. These menu options can be used to Add, Remove or Uninstall a given license key or product.



- For each enabled product, target which Adaptiva clients will receive this license.

Toggle **Use All Adaptiva Clients** (slide to the right) or, click on **Browse** and select a collection or group and click **OK**.

- Click **Overall Status** to see the current license status of all enabled products.



Click **OK** to close the **Overall Licensing Status** window.

(Optional) Post Installation Tasks


These can only be completed after OneSite ConfigMgr Edition or Endpoint Health has been licensed.

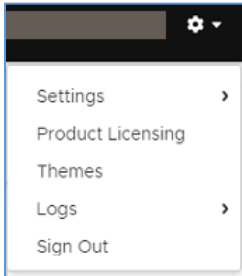
Server Activation

Once the activation code is received continue with the next step.

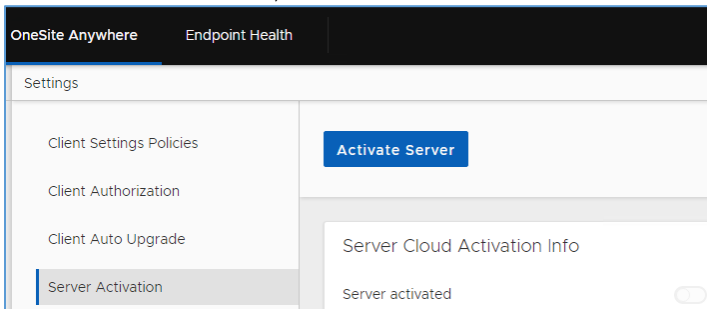
If you have not requested the Activation Code, see the section [Server Activation](#) in the [Installation Prerequisites](#) section

Using the Admin Portal

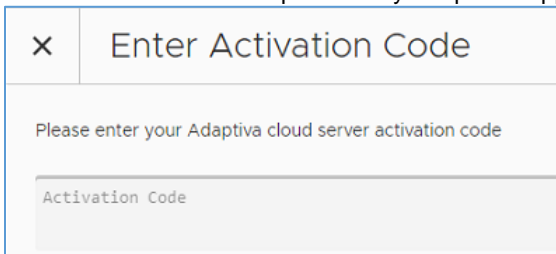
1. In a web browser connect to the Admin Portal (except Internet Explorer) – [http://AdaptivaServerFQDN\[:port\]](http://AdaptivaServerFQDN[:port])
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on the  with the drop-down on the far right and select **Settings**



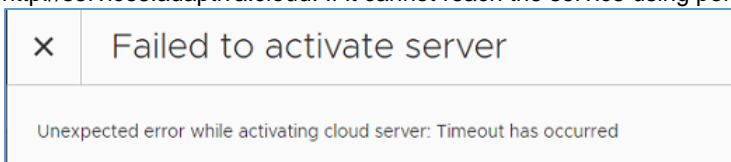
4. Select **Server Activation**, then click on **Activate Server**



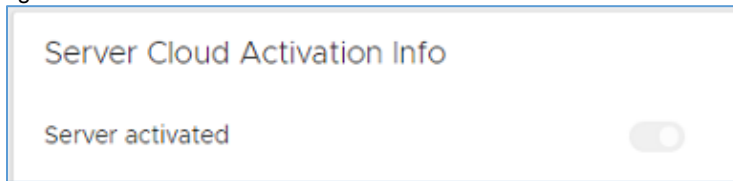
5. Enter the Activation Code provided by Adaptiva Support and click **OK**



6. The Adaptiva Server Service will attempt to contact the Adaptiva Cloud Relay Server at <http://services.adaptiva.cloud>. If it cannot reach the service using port 80 you will see the following error:



If it successfully registers with the Adaptiva Cloud Relay Service, the Server activated slider will be slid to the right



Note the other information available in the Cloud Connect Adaptiva Server settings screen:

Customer name: This is initially the FQDN of the Adaptiva server. After activation, it will display the name that was entered at the Cloud Relay Server.

Global ID: Unique ID of the Adaptiva Server assigned at registration time

Tenant ID: Unique ID of the Adaptiva Server. Also, part of the certificate issued to the server and make up the server's identity

Server GUID: This uniquely identifies your Adaptiva Server and can be used for client installations. It is required if the client is being installed without connectivity to the Adaptiva Server, requiring the client to validate through the Adaptiva Cloud Relay Service.


Connecting to Cloud Storage

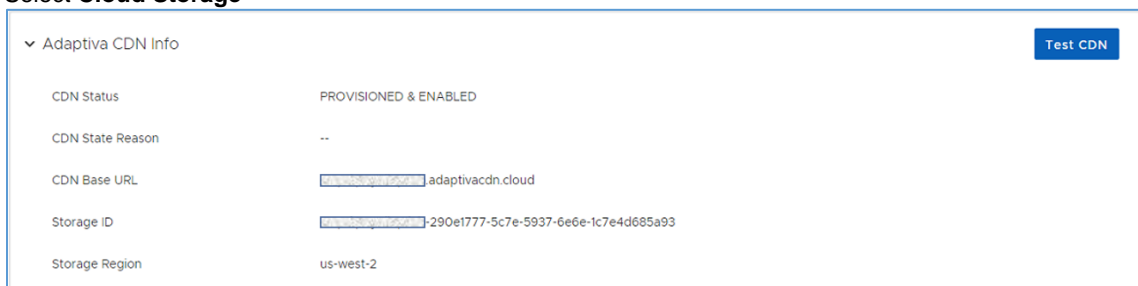
Adaptiva OneSite Anywhere now provides Adaptiva Cloud storage instead of Azure Storage. This storage allows customer content to be available globally. The Adaptiva CDN must be enabled when the Adaptiva Server is registered for activation. If the Adaptiva CDN is not enabled, then an Azure Storage Account may be configured to store customer content in the cloud. Azure provides the CDN capabilities based on the settings chosen when setting up the Storage Account.

Adaptiva CDN

Using the Admin Portal

If the server was recently activated, restart the Adaptiva Server service to ensure the Adaptiva CDN Info is displayed

1. Connect to the Admin Portal using a web browser (except Internet Explorer) – [http://AdaptivaServerFQDN\[:customport\]](http://AdaptivaServerFQDN[:customport])
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Select the , **Settings**
4. Select **Cloud Storage**



This will show the following information:

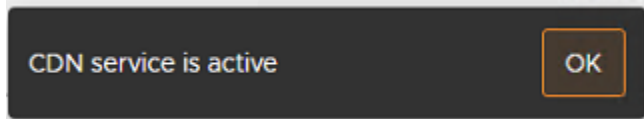
CDN Status: This will report PROVISIONED & ENABLED when everything is configured

CDN State Reason: This will show -- when things are working correctly

CDN Base URL: This will be the URL to the content. The URL will be <your registered servername>.adaptivacd.com

Storage Region: This is the region selected when the activation record was created and the Adaptiva CDN storage was enabled.

- Click on **Test CDN**. After a few seconds, the following will pop-up:



If the CDN service is not yet active, it will pop-up:



If the Adaptiva CDN registration was recently completed, this can take some time. Try again in 15 minutes.


(Deprecated) Azure Storage

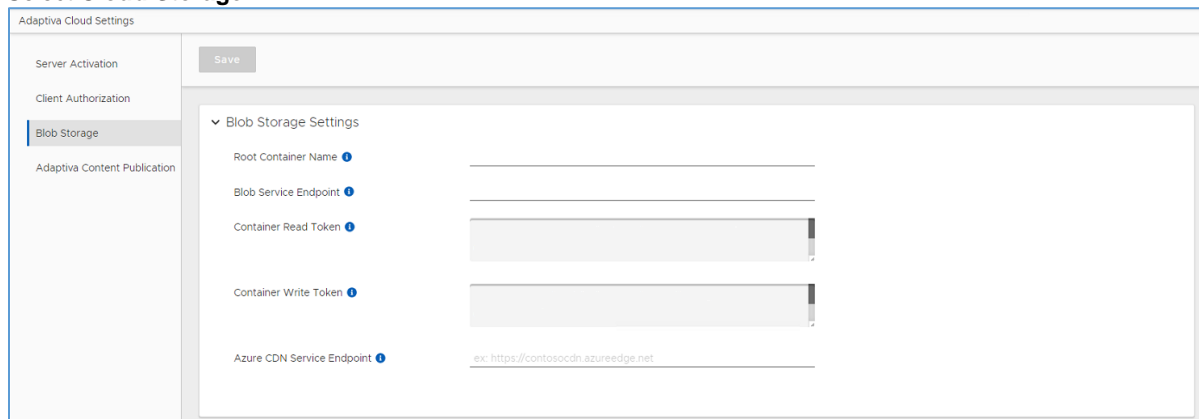
Adaptiva CDN storage is now recommended (build 8.0.925 or greater is required).

This needs to be completed to configure Adaptiva to communicate with the Azure Storage Container. To complete these settings, gather information from the Azure Global Administrator. The following information should have been provided – see Azure Storage in the Installation Prerequisites section:

Storage Account Name
Container Name
Read and Write SAS Tokens

Using the Admin Portal

- Connect to the Admin Portal using a web browser (except Internet Explorer) – [http://AdaptivaServerFQDN\[:customport\]](http://AdaptivaServerFQDN[:customport])
- Enter the appropriate credentials or click on **Login with Active Directory**
- Select the  **Settings**
- Select **Cloud Storage**



Enter the following information

Root Container Name: This is the name of the container that was created for Adaptiva Content. This must be entered as all lower-case.

Blob Service Endpoint: This will be <https://<StorageAccountName>.blob.core.windows.net>

Container Read Token: Enter the Read token provided. Make a note of the expiration date to ensure the token is renewed before it expires.

This should start with a ?. For example: ?sv=2021-06-08&ss=bfqt&srt=sco&sp=rlptfx&se=2027-09-02T03:03:40Z&st=2022-09-09T19:03:40Z&spr=https&sig=hjnLEK2Jsup9OU2afg01sT0fjPRAZDDqf08d%2F40XILs%3D

Container Write Token: Enter the Write token provided. Make a note of the expiration date to ensure the token is renewed before it expires.

This should start with a ?. For example: ?sv=2021-06-08&ss=bfqt&srt=sco&sp=rlptfx&se=2027-09-02T03:03:40Z&st=2022-09-09T19:03:40Z&spr=https&sig=H9YbNKbc3O34Rc9IXKdAY0b3oHl1IWCSQxIAhlrWqd4Pg%3D
The Azure CDN Endpoint URL can be left blank

IMPORTANT: If the Security Access Token expires, Adaptiva clients will NOT be able to download content from Azure. New Content CANNOT be created. Do not let these expire.

5. Click on **Save**
A read and write test will be conducted to the storage container.

OneSite Anywhere: Intune Configuration

This only needs to be configured if Onsite for Intune Edition has been licensed.

This need to be completed to allow Adaptiva to automate the creation of Intune apps. To complete these settings, gather information from the Azure Global Administrator. The following information should have been provided – see **App Registration** in the **Installation Prerequisites** section:

Tenant ID
App ID
(optional) Client Secret

Download Win32 Content Prep tool

1. Open a web browser and go to the following URL: <https://github.com/Microsoft/Microsoft-Win32-Content-Prep-tool>
2. Select the Code dropdown and click **Download ZIP**

NOTE: If doing this on the server using Internet Explorer and there is no response when clicking **Clone or Download**, click  **Internet Options**, select the **Security** tab, be sure Internet is selected and click **Custom Level**. Scroll down to **Downloads**, under **File Downloads** select **Enable**. Click **OK**, **Yes**, **OK**. Click **Clone or Download** again to retry

Also, when downloading files from another computer they can be initially blocked. Right-click on the file and select **Properties**, if there, check the box to Unblock the file and click **OK**

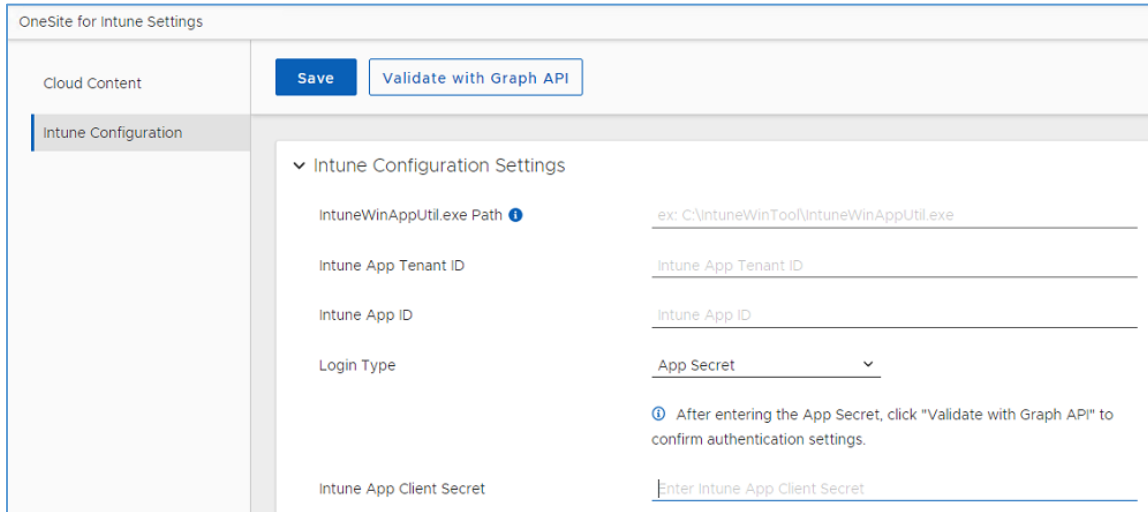
Security: This file came from another computer and might be blocked to help protect this computer. ☐ Unblock

3. Extract the files to a folder
For example: C:\IntuneWinTool or C:\Program Files (x86)\IntuneWinTool

Using the Admin Portal

1. Connect to the Admin Portal using a web browser (except Internet Explorer) – [http://AdaptivaServerFQDN\[:customport\]](http://AdaptivaServerFQDN[:customport])
2. Enter the appropriate credentials or click on **Login with Active Directory**
3. Click on **Go to OneSite Intune Edition** or click **OneSite**, **OneSite Intune Edition**, then click **Go to Settings** or select **Intune Settings** in the action pane on the far left

4. Select Intune Configuration



Complete the following:

IntuneWinAppUtil.exe Path: Enter the local path including the executable name to the downloaded IntuneWinAppUtil.exe

The following should be provided by the Azure Global Admin. They can be found in App Registrations. Select the App registration created for Adaptiva.

Intune App Tenant ID: Enter the Directory (Tenant) ID

Intune App ID: Enter the Client (App) ID

Login Type: Select the following based on how the App Registration was created above

Login Type	App Registration
App Secret	<p>Option 1 was followed to create the App Registration. All apps will be created using the App Secret</p> <p>Login Type App Secret</p> <p>After entering the App Secret, click "Validate with Graph API" to confirm authentication settings.</p> <p>Intune App Client Secret Enter Intune App Client Secret</p>
Global Deferred Account Per Admin Deferred Account	<p>Option 2 was followed to create the App Registration.</p> <p>Use Global Deferred Account when all Intune apps should be created using the same Azure AD account</p> <p>Use Per Admin Deferred Account when each Intune app should be created using the account associated with the Adaptiva Login ID</p> <p>When these options are used the login type will display:</p> <p>Login Type Global Deferred Account Authenticate</p> <p>Click on "Authenticate" above to create authentication token with Microsoft. Once authenticated, click "Validate with Graph API" to confirm authentication settings.</p>

5. Click on **Save**

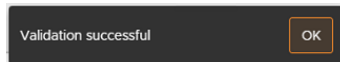
Complete one of the Options below depending on which App Registration was created

Option 1

Complete these steps to enter the Intune Settings for Option 1 where an App Secret will be used

6. Enter the Intune App Client Secret that was provided by the Intune Global Admin
7. Click on **Save**
8. Click **Validate with Graph API** to confirm the settings will allow the creation of apps in Intune

The server will validate the connection and will display the following when successful (for 3 seconds)



If the App Secret entered is not correct a message will be displayed in the Error View panel

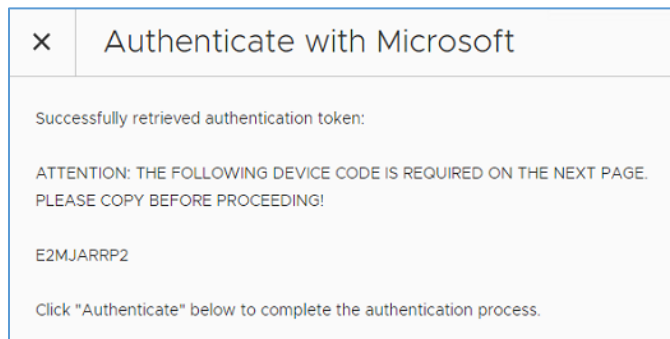
Error View 1	
Component	Title
Failed validation	Unknown error [Error Message = Unable to get token from confidential application., Error Code = 1, Source Object = null]. See server error log for details...

Correct the App Secret, click Save and retry the Validate

Option 2

Complete these steps to enter the Intune Settings for Option 2 where a deferred account will be used

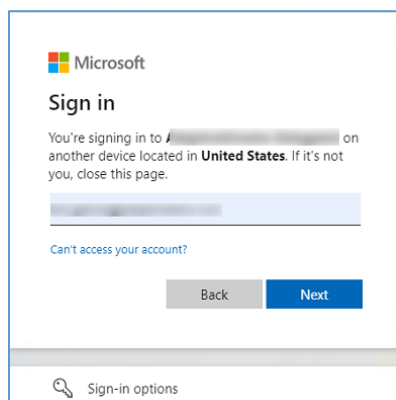
6. Click **Authenticate**.



7. 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

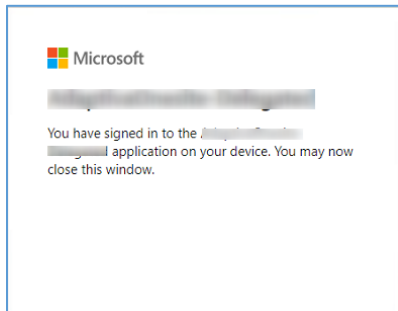
8. A login for Microsoft will be displayed, enter the code from the previous screen. Click **Next**
9. Confirm the Tenant and the username is correct. Click **Next**



10. Enter the password for that account in that Tenant. Click **Sign in**

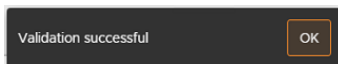
Complete any authentication that is required.

11. Close the tab



9. Click **Validate with Graph API** to confirm the settings will allow the creation of apps in Intune

The server will validate the connection and will display the following when successful (for 3 seconds)



When Per Admin Deferred Account has been selected every Adaptiva user will be prompted to enter their Azure AD account credentials. This will occur when the P2P App is published to Intune.

Client Installation

The Adaptiva Client needs to be installed on every device that will be managed. The Adaptiva Client supports a manual installation as well as a silent unattended installation.

The Adaptiva Client can be installed manually or deployed via the existing Software Distribution mechanism (ConfigMgr, Intune, Workspace ONE), or to ensure complete coverage, the client agent setup can also be added to a GPO-enforced startup script, the OS deployment process and/or deployed using the peer-to-peer MSI (described below).

NOTE: The Adaptiva Client should always be installed on the Adaptiva server as referenced in the Adaptiva Client Installation on the Server section. There should also be additional clients installed on the same subnet or Office as the Adaptiva Server to support content load sharing.

Client Installation Files

Adaptiva provides the following client installation files in the Installers folder of the compressed build files.

File	Purpose
AdaptivaClientSetup.exe	Primary client installer
AdaptivaClientSetup32.exe	Primary client installer for 32-bit operating systems
AdaptivaP2PClientInstaller.msi	Small footprint, client installer. Will try the local subnet first, then download the AdaptivaClientSetup.exe from the specified location.
adaptiva-client-#.###.#_amd64.deb	Full client installer for Debian 11 and 12 and for Ubuntu 22 and 24
adaptiva-client-#.###.#-el9.x86_64.rpm	Full client installer for CentOS Stream 9 and 10
adaptiva-client-#.###.#-macOS.pkg	Full client installer for MacOS
client_install.sh	Shell script that performs the installation
ClientSetupConfig.xml	Installation configuration settings

¹ The #.###.# represents the version number, which changes with each build release.

NOTE: If the Adaptiva Client has already been deployed using AdaptivaClientSetup.exe then the MSI Product key will not be registered, and clients will reinstall. Also, it is NOT recommended to mix the installation of the MSI and the EXE. Different values are registered in Add/Remove Programs and one product cannot uninstall the other completely. If an MSI must be used to deploy the Adaptiva client, deploy the AdaptivaP2PClientInstaller.msi

Client Installation Logs

In the case where an administrator needs to troubleshoot an Adaptiva Client installation, the following table contains the installation log locations. Other logs exist in the installation folder.

Function	Log Location and Name
Standard client installation	%windir%\AdaptivaSetupLogs\Client\AdaptivaClientSetup.log
P2P MSI client installation	%windir%\AdaptivaSetupLogs\ClientAdaptivaP2PClientSetup.log
Cross Platform Client installation	Mac: /opt/adaptivaclient/logs/adaptiva.log Linux use the following command: sudo journalctl -u adaptivaclientd.service

Full Client Installation

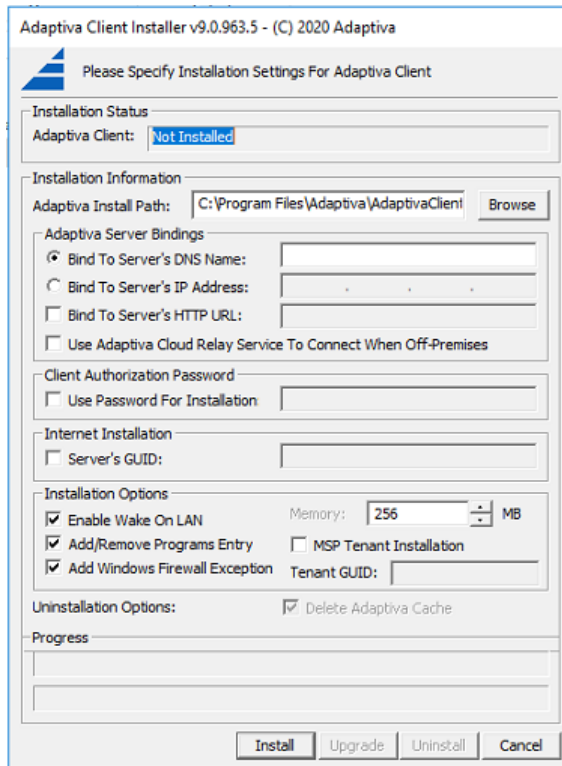
Manual Attended Installation

Using the **AdaptivaClientSetup.exe** full client installation.

Use this method on a one-off basis during testing, initial rollout or to supplement automatic deployment.

1. Execute the **AdaptivaClientSetup.exe** as Administrator found in the installation source folder.

- At the **License Agreement** screen, click **Accept** to continue.
- At the **Adaptiva Client Installer** dialog, verify or change the following installation options then click **Install**. The installation will begin immediately.



Adaptiva Install Path – Directory where the Adaptiva client will be installed.

Adaptiva Server Bindings – Specify one of the following

- Adaptiva Server's DNS Name
- Adaptiva Server's IP Address

Adaptiva Server Bindings – Check the options as required

If clients need to bind using HTTP, check the box: **Bind to Server's HTTP URL**

- Adaptiva Server's HTTP URL – Be sure to add the port that was used during server installation. E.g. <http://servername.adaptiva.com:9679>

If clients will be on the Internet, check the box: **Use Adaptiva Cloud Relay To Connect When Off-Premises**

For additional security check the following boxes:

- Use Password for Installation** – Enter the password created in the Workbench
- Server's GUID** – Enter the Adaptiva Server GUID.

This option must be used when the client is on the internet and is a new client

NOTE: How to find the [Server GUID](#):

In the Admin Portal in , **Settings, Server Activation**

OR on the Adaptiva Server in `HKLM\Software\Adaptiva\server | client_data_manager.server_guid`

Enable Wake On LAN – Allows the client to be woken up using peer-to-peer WOL.

Add/Remove Programs Entry – Adds an entry allowing for uninstallation of the client agent from the Control Panel.

Add Windows Firewall Exception – Adds exceptions to the local Windows Firewall for the default client ports, see Appendix A: Communication Ports for a list of these ports.

Memory – Should be a minimum of 256MB. Set in increments of 128MB only.

MSP Tenant Installation – Should only be checked if using the Managed Service Provider license and requires the entry of **Tenant GUID**.

Unattended Installation EXE Command Line Parameters

Using the **AdaptivaClientSetup.exe** full client installation.

In some cases, an administrator may want to use an alternative unattended method to install the Adaptiva client. The table below describes the command line parameters available for the **AdaptivaClientSetup.EXE** installation.

Parameter		Usage
Required		
Install Type	-cleaninstall	Uninstalls the existing client installation and cleanly installs a new copy of the client.
	-installorupgrade	Installs the Adaptiva client or upgrades the existing client.
	-uninstall	Uninstalls the Adaptiva client.
Server Info	-servername <servername>	FQDN of the Adaptiva server.
	-serverIP <server IP>	IP address of the Adaptiva server.
Optional		
-cloudrelay		Enables the client to use the Adaptiva Cloud Relay Service to connect when off-premises
-custompacurl <URL of PAC file>		The installer will access the PAC file to gather the proxy information
-customproxy <server>:<port>:<scheme>		The installer will use the information to access the proxy when trying to contact Adaptiva Cloud Services e.g. -customproxy 10.10.10.1:9000:http
-customproxybypass <server1>;<server2>;<server3>		When -customproxy is used the servers included in the custom proxy bypass list will be excluded from using the proxy.
-delay <seconds>		Delays the starting of the installation executable. This is useful during a client self-upgrade using Adaptiva content push allowing workflows to complete before the AdaptivaClient service is stopped.
-folder <folder path>		The desired installation path. By default, the Adaptiva client is installed under: %ProgramFiles%\Adaptiva\AdaptivaClient
-mem <memorysize>		Maximum Java heap size, in MB (default: 256).
-noarp		The installer will NOT create an entry in Add/Remove Programs.
-nocachedel		This parameter can be used with the options: -uninstall or -cleaninstall. If this parameter is used the Adaptiva cache will not be deleted.
-nofirewall		The installer will NOT create Windows Firewall rules for the Adaptiva client.
-nomif		The installer will not send ConfigMgr MIF status in the case of any errors found during installation.
-nowol		Specify this option to disable Wake on LAN. By default, the Adaptiva Client enables Windows Wake on LAN settings on all the network cards installed in the machine.
-password <provided password>		Provides additional security. Enter the password that was created on the Adaptiva Server
-preferuserproxy true false		When preferuserproxy is true the proxy settings will be obtained from the internet explorer settings Default: false
-serverguid <GUID>		The GUID of the Adaptiva Server can be provided by the Adaptiva Admin. Required with the client is on the internet. This property can only be used if -CLOUDRELAY is included.

-serverurl <server-url:port>	Tells the client to communicate to the Adaptiva Server via HTTP instead of using UDP
-tenantguid	Use this to access the Managed Services Provider (MSP) functionality and create and maintain multi-tenant environments

Peer-to-Peer (P2P) MSI

The Adaptiva Client P2P MSI installer helps administrators in achieving 100% distribution of the Adaptiva agent. In most common scenarios, ConfigMgr / Workspace ONE will be able to install the Adaptiva client onto most systems within an enterprise, but it is often difficult to ensure complete coverage in the case of unhealthy ConfigMgr / Workspace ONE clients. Using the AdaptivaClient P2P MSI installer, the Adaptiva Client can be pushed using a group policy, a startup script, psexec (from SysInternals) or any other remote execution method available.

Once executed, the Adaptiva P2P Client MSI installs the full Adaptiva Client agent. The MSI does not actually contain the full client installation though. Instead, the MSI – which is specific to a particular version of the Adaptiva client agent – first looks for the Adaptiva Client on a peer system in the same subnet with the correct version. If it finds one, it retrieves the AdaptivaClientSetup.exe from that local client and installs the Adaptiva Client from that executable. If it cannot find a peer with the correct version, the MSI retrieves the setup from a UNC path specified on the command line. If multiple systems run the MSI simultaneously and none of them find the correct version of the client locally, an election takes place among these clients. Only the *winner* of the election downloads the setup from UNC path and it then makes the setup available to the other client systems.

NOTE: Ensure that the security context the MSI is executed under has read access to the UNC Path.

The Adaptiva P2P Client MSI is not an interactive installer; it is a completely silent installer with no user-interaction.

The P2P installer is named **AdaptivaP2PClientInstaller.msi** and is in the compressed (.zip) product download source.

Unattended Installation MSI Command Line Parameters

The following table contains the MSI properties are valid for the P2P client installer:

NOTE: Be sure to enter these on the command line as **PROPERTY=Value**

Property	Value	Description
Required		
SERVERIP SERVERNAME	IP address of server or server name.	The Adaptiva server that this client will report to. SERVERIP takes precedence over SERVERNAME if both are specified.
SOURCEUNCPATH SOURCEURLS	<UNC path of source>\AdaptivaClientSetup.exe OR URL address of AdaptivaClientSetup.exe	SOURCEUNCPATH: The location to download the client installer from if it cannot be found in the local office. The account executing the installation must have at least read access to the UNC path. SOURCEURLS: The list of Source CDN URLs (where each SOURCE URLS is separated by '<' character) from where the P2P installer will download the AdaptivaClientSetup.EXE by HTTP protocol in case it is not available in the local office
Optional		
ARPSYSTEMCOMPONENT	1: suppresses creation 0: does not suppress creation (default)	Suppresses the creation of an Add/Remove Program entry for the actual Adaptiva client. The P2P MSI creates a hidden Add/Remove Program entry for

Property	Value	Description
		itself named Adaptiva Peer to Peer Client Installer.
CLEANINSTALL	1: performs a clean installation 0: perform an InstallOrUpgrade installation (default)	Uninstalls the existing client installation and cleanly installs a new copy of the client. If not specified, the InstallOrUpgrade option is used by default.
MEM	<memory in MB>	The amount of memory in MB to be used by the Adaptiva client. Default: 256 MB.
CLOUDRELAY	1: Use the cloud relay feature 0: Do not use the cloud relay feature (default)	When enabled, allows the client to communicate with the Adaptiva Cloud Relay server. Include the SERVERGUID property.
CUSTOMPACURL	<URL of PAC file>	The installer will access the PAC file to gather the proxy information
CUSTOMPROXY	<server>:<port>:<scheme>	The installer will use the information to access the proxy when trying to contact Adaptiva Cloud Services e.g. -customproxy 10.10.10.1:9000:http
CUSTOMPROXYBYPASS	<server1>;<server2>;<server3>	When -customproxy is used the servers included in the custom proxy bypass list will be excluded from using the proxy.
NOCACHEDEL	1: cache is preserved 0: cache is deleted during uninstallation (default)	Preserves the Adaptiva client cache after uninstallation. This property is only valid when used in conjunction with the UNINSTALL property.
NOFIREWALL	1: does not create any firewall exceptions 0: creates firewall exception (default)	Disables creating exceptions in the Windows Firewall for the Adaptiva client.
NOLOGGING	1: only FATAL errors are logged, but no other logging is done 0: normal INFO logging (default)	Controls the logging level during the client install. Only logging fatal errors is helpful if the client system uses shared storage and to minimize logging.
NOWOL	1: disables WoL 0: enables WoL (default)	Disabled Wake-on-LAN
PASSWORD	Password provided by Adaptiva Admin	The password is entered by Adaptiva Admin in the workbench to ensure only authorized connections. This property can only be used if CLOUDRELAY=1.
PREFERUSERPROXY	true false	When preferuserproxy is true the proxy settings will be obtained from the internet explorer settings Default: false
SERVERGUID	GUID of the Adaptiva Server	The GUID of the Adaptiva Server can be provided by the Adaptiva Admin. Required when the client is on the internet. This property can only be used if CLOUDRELAY=1

Property	Value	Description
SERVERURL	Server FQDN URL:port	Tells the client to communicate to the Adaptiva Server via HTTP instead of using UDP
TARGETDIR	<path of desired install folder>	The installation folder of the Adaptiva Client. By default, it is %SystemDrive\Program Files\Adaptiva or %SystemDrive%\Program Files (x86)\Adaptiva
TENANTGUID	Tenant GUID provided by the Adaptiva administrator	Use this to access the Managed Services Provider (MSP) functionality and create and maintain multi-tenant environments
UNINSTALL	1: performs an uninstallation 0: performs an installation (default)	Ignores all other properties and performs an uninstallation of the Adaptiva client.
WAITFORCOMPLETION	1: the MSI installer waits the client installation to finish 0: the MSI will not wait for Adaptiva Client installation to be completed (default)	Specifies whether the Adaptiva P2P Client Installer MSI will wait until installation will be completed.
WANBYTESPERSECOND	X: bytes per second 0: Unlimited (default)	The maximum download speed that will be used while downloading the Adaptiva client Installer exe over the WAN from the SOURCEUNCPATH.

Installation command lines

To deploy the Adaptiva P2P Client Installer, the only file needed for the package source is **AdaptivaP2PClientInstaller.msi** which can be found in the Adaptiva installation source. Two programs should be created for Install and Uninstall. The AdaptivaClientSetup.exe must be accessible via a Share or a URL. See some example commands below:

Install with Server Share Source:

```
Msiexec.exe /I AdaptivaP2PClientInstaller.msi /qn SERVERNAME=AdaptivaServer.domain.com
SOURCEUNCPATH=\\ServerFQDN\AdaptivaClient\AdaptivaClientSetup.exe WAITFORCOMPLETION=1
```

Install with Cloud and Internet Source:

```
Msiexec.exe /I AdaptivaP2PClientInstaller.msi /qn SERVERNAME=AdaptivaServer.domain.com
SOURCEURLS=https://tiny.url/abcdefg CLOUDRELAY=1 SERVERGUID=abcdefgh-abcd-1234-efgh-abcdefghijk1
WAITFORCOMPLETION=1
```

IMPORTANT: Include the following switches as required if the Cloud Relay service or if HTTP client communications will be used:

Cloud Relay service: CLOUDRELAY=1, SERVERGUID=<GUID>, PASSWORD=<auth. Secret>

HTTP communications: SERVERURL=<ServerURL:port>

NOTE: How to find the Server GUID:

In the Admin Portal in , Cloud Settings, Server Activation
On the Adaptiva Server in HKLM\Software\Adaptiva\server | client_data_manager.server_guid

Uninstall:

```
Msiexec.exe /I AdaptivaP2PClientInstaller.msi /q UNINSTALL=1 NOCACHEDEL=1
```

NOTE: The uninstall command line uninstalls any version of the Adaptiva client. Using the normal Windows Installer uninstall parameter (/x) only uninstalls a specific version of the Adaptiva client corresponding to the version of the MSI – the MSI packaged with each version of the product is specific to that client version of the product.

Client Installation using ConfigMgr

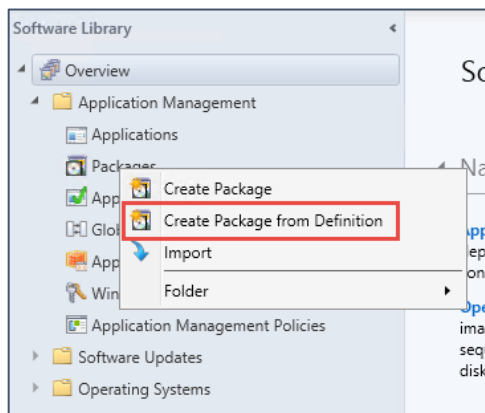
Using the power of ConfigMgr is a great way to go for large-scale, production deployment of the Adaptiva Client. As with all Software Distribution in ConfigMgr, the first step is to create the package and program(s). If using Operating System Deployment, a Package and Program will be needed in the Task Sequence, do not use an Application.

The Application model can also be used for Adaptiva client deployment outside of a task sequence.

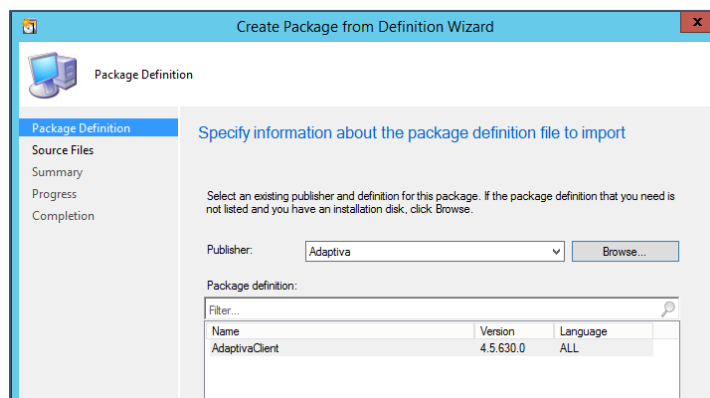
Creating a Package and Program from the Package Definition File

To create a pre-defined ConfigMgr package and program, a Package Definition File has been provided. The file can be found on the Adaptiva Server under: <InstallPath>\Program Files\Adaptiva\AdaptivaServer\config and is named **AdaptivaClientSetupSilent.sms**.

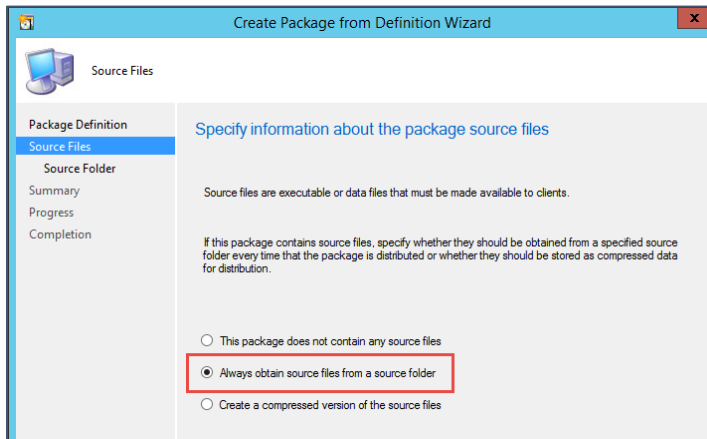
1. Create a new folder in the content source file repository per current company standards
2. Copy the **AdaptivaClientSetup.exe** file from the installation source to the newly created folder
3. In the ConfigMgr console, open the **Software Library** workspace and expand **Application Management** then right-click **Packages**. In the context menu, select **Create Package from Definition**.



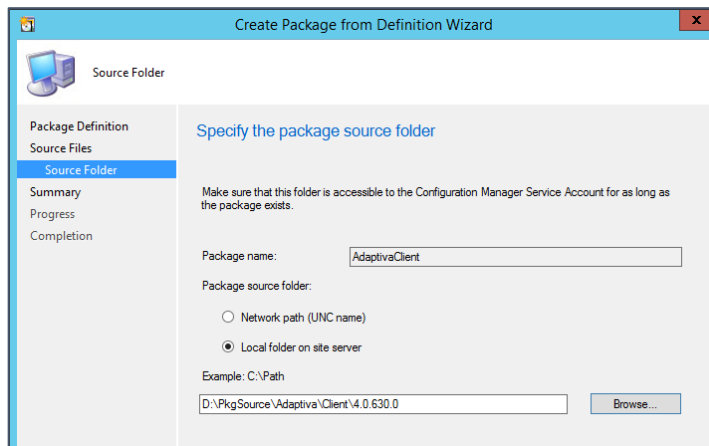
4. At the **Package Definition** page, click the **Browse** button then navigate to the <InstallPath>\Program Files\Adaptiva\AdaptivaServer\config folder on the Adaptiva server and select the **AdaptivaClientSetupSilent.SMS** file then click **Open**. The package name and version will be displayed. Select it, then click **Next**.



- At the **Source Files** page, select **Always obtain source files from a source folder** then click **Next**.



- At the **Source Folder** page, enter the UNC path of the folder created in the first step and then click **Next**.



- Complete the **Create Package from Definition Wizard**

The above procedure creates the following package:

Adaptiva AdaptivaClient <version> ALL

The package includes three programs:

- CleanInstall – Uninstalls the existing client installation and installs a new copy of the client
- InstallOrUpgrade – Installs the Adaptiva client or upgrades the existing one in place
- Uninstall – Uninstalls the Adaptiva client

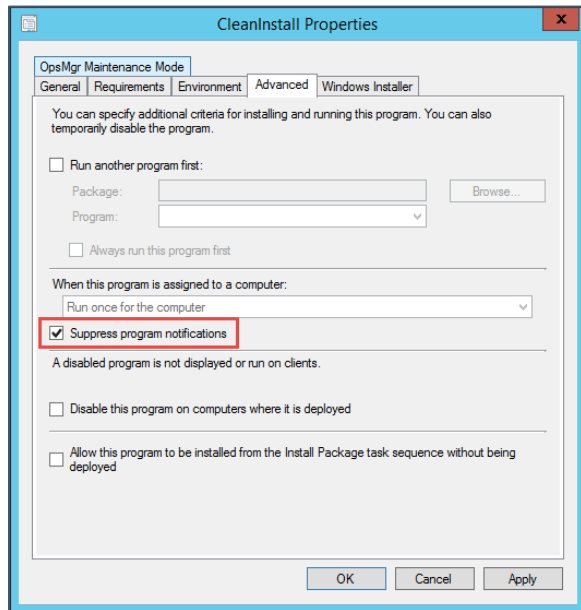
IMPORTANT: Include the following switches as required if the Cloud Relay service or if HTTP client communications will be used:

Cloud Relay service: -CloudRelay, -ServerGUID=<GUID>, -Password=<auth.Secret>

HTTP communications: -ServerURL=<ServerURL:port>

By default, the program will be set to display notifications to users when deployed unless notifications are suppressed via client policy. To disable notifications for a program, open the program properties, and select the **Advanced** tab.

Check the option: **Suppress program notifications** then click **OK** to save the setting.



The desired program is now available to be deployed to collections of devices in the environment according to the company's standards and practices.

Creating an Application using the EXE

To create a ConfigMgr application and deployment type using AdaptivaClientSetup.exe.

1. Create a new folder in the content source file repository per the company's standards
2. Copy the AdaptivaClientSetup.exe file from the installation source to the newly created folder
3. In the ConfigMgr console, open the Software Library workspace and expand Application Management then right-click on **Applications**. In the context menu, select **Create Application**
4. Select **Manually specify the application information** and click **Next**
5. Enter the information
 Name: Adaptiva Client Setup
 Publisher: Adaptiva
 Software version:
 Enter the other fields as required by the company's standards
 Click **Next**
6. On the Software Center page enter the information as required by the company's standards and click **Next**
7. On the Deployment Types page, click **Add...**
8. On the General page, be sure to change the Type, selecting **Script Installer**
 Then, select **Manually specify the deployment type information** and click **Next**
 On the General Information page, enter Name: Adaptiva Client Setup
 Click **Next**
9. On the Content page enter the following:
 Select **Browse...** and enter the UNC path where AdaptivaClientSetup.exe was stored.
 Installation program: AdaptivaClientSetup.exe -INSTALLORUPGRADE -SERVERNAME serverfqdn | -
 SERVERIP serveripaddress -CloudRelay

IMPORTANT: Include the following switches as required if the Cloud Relay service or if HTTP client communications will be used:

Cloud Relay service: `-CloudRelay, -ServerGUID <GUID>, -Password <auth.Secret>`

HTTP communications: `-ServerURL <ServerURL:port>`

Uninstall program: `AdaptivaClientSetup.exe -UNINSTALL`

Check the box: **Run installation and uninstall program as 32-bit process on 64-bit clients**

Click **Next**

See the section [Unattended Installation EXE Command Line Parameters](#) for other EXE Properties

10. On the Detection Method page, click **Add Clause...**

Setting Type: Registry

11. Next to Hive, click on **Browse...**

12. Enter the Adaptiva Server computer name and click **Connect**

13. On the Adaptiva Server, expand

HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AdaptivaClient

14. In the Registry Value pane, select **DisplayName** and click **OK**

15. Select This registry setting must satisfy the following rule to indicate the presence of this application
The current value will be automatically entered

16. Click **OK**

17. Click **Next**

18. On the **User Experience** page, select the following:

Installation behavior: Install for system

Logon requirement: Whether or not a user is logged on

Installation program visibility: Hidden

Click **Next**

19. On the **Requirements** page, click **Next**

20. On the **Dependencies** page, click **Next**

21. On the **Summary** page, click **Next** and click **Close** when the wizard has completed successfully

22. Click **Next** to leave the Deployment Types page

23. Click **Next** on the Summary page and click on Close when the wizard has completed successfully

24. Select the application, then from the Home tab on the ribbon, select **Distribute Content**

25. The Distribute Content Wizard will be displayed, click **Next** two times

26. On the Content Destination page, Add the necessary Distribution Point or Distribution Point Group, then click **Next** and then **Close**

Creating an Application using the P2P MSI

To create a ConfigMgr application and deployment type, an MSI file has been provided.

Share AdaptivaClientSetup.exe

Share this for the on-premises users

1. Create a content source folder as follows:

<ContentSource-Drive>:\<Path>\Adaptiva\FullClient

Copy the AdaptivaClientSetup.exe from the Installation source into the FullClient folder

2. Share this folder on the server as **AdaptivaClient**

Share permissions: Everyone: READ

NTFS permissions: Domain Computers: Read and Execute, List, Read

Create the Application using the AdaptivaP2PClientInstaller.msi

1. Create a new folder in the content source file repository per the company's standards
2. Copy the **AdaptivaP2PClientInstaller.msi** file from the installation source to the newly created folder
3. In the ConfigMgr console, open the **Software Library** workspace and expand **Application Management** then right-click on **Applications**. In the context menu, select **Create Application**
4. Select **Automatically detect information about this application from the installation files**
5. Click on **Browse...** and enter the UNC to the content source file repository path just created and press enter. Select the MSI file and click **OK**, then click **Next**
6. Click **Next** on the **View imported information page** if the Application information was successfully imported from the Windows Installer (*.msi file) file.
7. On the **General Information** page, update as required. It is recommended to enter the publisher and the Software version
8. Update the installation program command line:

```
Msiexec.exe /I AdaptivaP2PClientInstaller.msi /qn SERVERNAME=AdaptivaServer.domain.com  
SOURCEUNCPATH=\\ServerFQDN\AdaptivaClient\AdaptivaClientSetup.exe WAITFORCOMPLETION=1
```

See the section [Unattended Installation MSI Command Line Parameters](#) for other MSI Properties

IMPORTANT: Include the following switches as required if the Cloud Relay service or if HTTP client communications will be used:

Cloud Relay service: **CLOUDRELAY=1, SERVERGUID=<GUID>,**

PASSWORD=<auth. Secret>

HTTP communications: **SERVERURL=<ServerURL:port>**

9. Check the box to **Run installation and uninstall program as 32-bit process on 64-bit clients**
10. Click **Next**
11. Click **Next** on the **Summary** page and click on **Close** when the wizard has completed successfully
12. Select the application, select the Deployment Types tab (lower pane) and select the deployment type, then select **Properties**
13. Select the **Content** tab and check the box: **Allow clients to use distribution points from the default site boundary group** also, select **Download content from distribution point and run locally** under **Select the deployment option to use when a client uses a distribution point from a neighbor boundary group or the default site boundary group**
14. Select the **Detection Method** tab
15. Notice the detection method. The MSI product code is specific to this version of the Adaptiva Client P2P Installer.
16. Click **OK**
17. To make this visible in Software Center, select Properties on the Application and update the General Information and Software Center tabs as required per the company's standards. Click **OK** when finished
18. Select the application, then from the Home tab on the ribbon, select **Distribute Content**
19. The Distribute Content Wizard will be displayed, click **Next** two times
20. On the Content Destination page, Add the necessary Distribution Point or Distribution Point Group, then click **Next** and then **Close**

Client Installation using Intune

When integrating OneSite with Intune, the Adaptiva Client will need to be deployed to target devices.

A Windows app (Win32) can be created for either one or both of the client installation methods below

- (Recommended) Distribute the Peer-to-Peer client installer by publishing the AdaptivaP2PClientInstaller.msi
- Distribute the full client by publishing the AdaptivaClientSetup.exe

P2P Client Installer

Windows installer files can only be deployed via Intune as a Line of Business App and as such will be installed as the User. To work around this, an .intunewin file will be created so the app can be installed correctly.

Because these are Intune clients, there is also the possibility they will be on the internet and not able to get to an on-premises server-based share. We need to host the AdaptivaClientSetup.exe in Azure. Clients that are on-premises will be able to download from a peer.

This process will download the 1MB AdaptivaP2PClientInstaller.msi using Intune. If the full client is not available on the local subnet, then it will be downloaded either from a server share UNC or from a web-based URL.

This process will download the P2P Client installer (approx. 1MB) using Intune. The full client will be downloaded from a peer on the same subnet or will be copied from the provided server share name or internet-based URL.

Complete the following prerequisites to deploy the Adaptiva P2P Client Installer to Intune clients

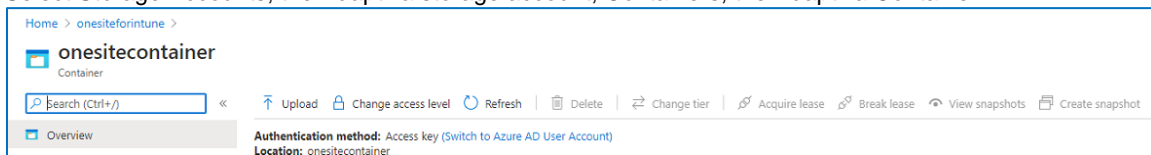
Share AdaptivaClientSetup.exe

Share this for the on-premises users

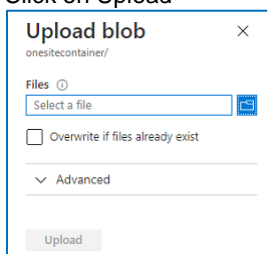
1. Create a content source folder as follows:
 <ContentSource-Drive>:\<Path>\Adaptiva\FullClient
 Copy the AdaptivaClientSetup.exe from the Installation source into the FullClient folder
2. Share this folder on the server as **AdaptivaClient**
 Share permissions: Everyone: READ
 NTFS permissions: Domain Computers: Read and Execute, List, Read

Also, make it available for those that might be out on the internet

1. Open a browser and connect to Azure (<https://portal.azure.com>) with an account with appropriate access to the Storage Account Container
2. Select Storage Accounts, the Adaptiva storage account, Containers, the Adaptiva Container

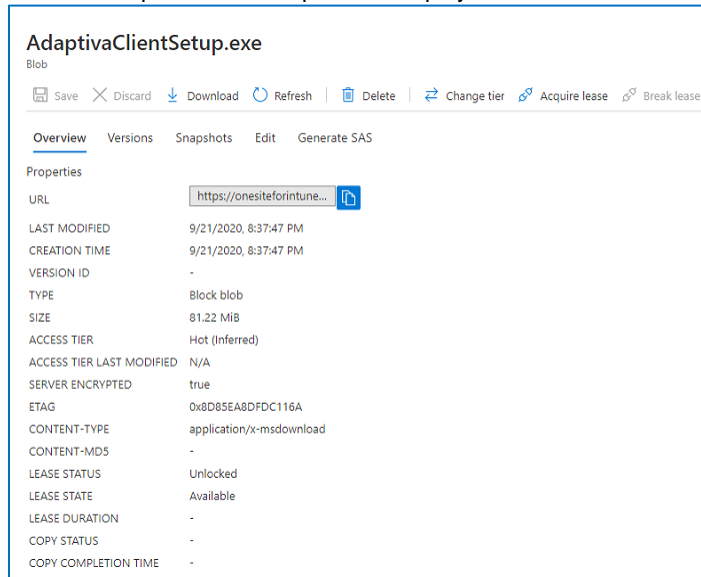


3. Click on Upload



4. Click on the folder icon and browse to the Adaptiva installation media in the Installers folder and select **AdaptivaClientSetup.exe** and click **Open** then click **Upload**

- Click on **AdaptivaClientSetup.exe** to display its information



AdaptivaClientSetup.exe
Blob

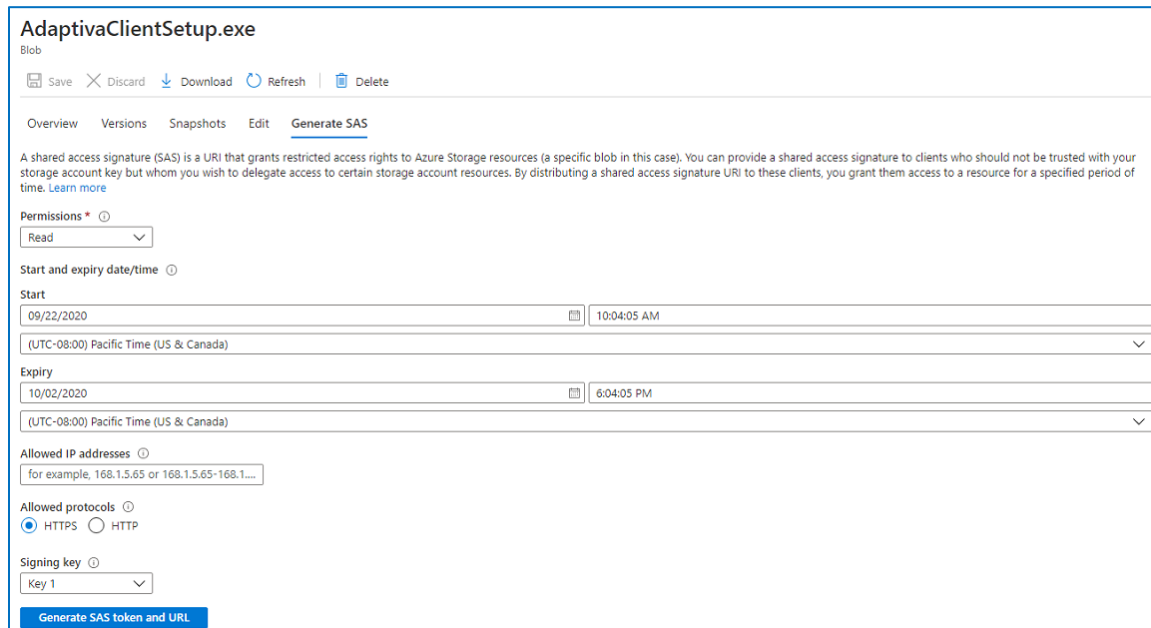
Save Discard Download Refresh Delete Change tier Acquire lease Break lease

Overview Versions Snapshots Edit Generate SAS

Properties

URL	https://onesiteforintune...
LAST MODIFIED	9/21/2020, 8:37:47 PM
CREATION TIME	9/21/2020, 8:37:47 PM
VERSION ID	-
TYPE	Block blob
SIZE	81.22 MiB
ACCESS TIER	Hot (Inferred)
ACCESS TIER LAST MODIFIED	N/A
SERVER ENCRYPTED	true
ETAG	0x8D85EABDFDC116A
CONTENT-TYPE	application/x-msdownload
CONTENT-MD5	-
LEASE STATUS	Unlocked
LEASE STATE	Available
LEASE DURATION	-
COPY STATUS	-
COPY COMPLETION TIME	-

- Click on **Generate SAS**



AdaptivaClientSetup.exe
Blob

Save Discard Download Refresh Delete

Overview Versions Snapshots Edit **Generate SAS**

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources (a specific blob in this case). You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified period of time. [Learn more](#)

Permissions * ⓘ
Read

Start and expiry date/time ⓘ

Start
09/22/2020 10:04:05 AM
(UTC-08:00) Pacific Time (US & Canada)

Expiry
10/02/2020 6:04:05 PM
(UTC-08:00) Pacific Time (US & Canada)

Allowed IP addresses ⓘ
for example, 168.1.5.65 or 168.1.5.65-168.1...

Allowed protocols ⓘ
☒ HTTPS ☐ HTTP

Signing key ⓘ
Key 1

Generate SAS token and URL

- Update the **Expiry** date. This should be long enough until the next version is deployed.
- Click on **Generate SAS token and URL**
- Copy the **Blob SAS URL** and make a note of the expiration date. This file will not be able to be downloaded using this SAS token after the expiry timestamp.
- Because this URL is really long, we need to make it shorter, use a favorite URL shortener. i.e. tinyurl.com. Copy and save the shortened URL with the original URL

Create .intunewin file

The intunewin tool was downloaded earlier. Create a folder to hold the single installation

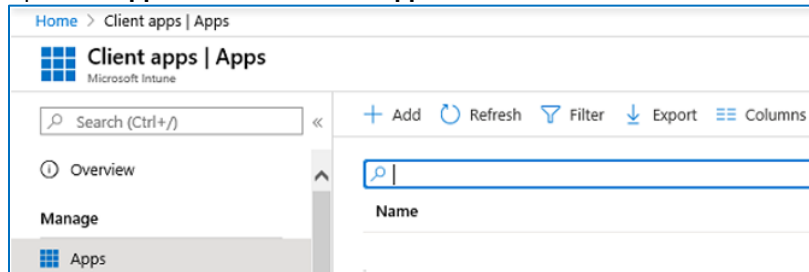
- Create a content source folder as follows:
`<ContentSource-Drive>:\<Path>\Adaptiva\P2PClient`
 Copy the `AdaptivaP2PClientInstaller.msi` from the Installation source into the `P2PClient` folder
- Open Notepad and enter the following:

```
%windir%\system32\msiexec.exe /I AdaptivaP2PClientInstaller.msi /qn WAITFORCOMPLETION=1
CLOUDRELAY=1 SERVERNAME=%1 SERVERGUID=%2 SOURCEURLS=%3 %4 %5
```

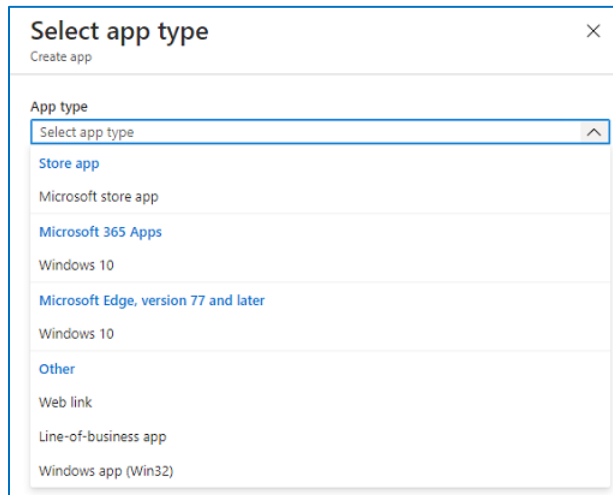
3. Save this file as **Install.cmd** in the P2PClient folder
4. Open a command prompt at the intunewin tool folder and run the following command:
`IntuneWinAppUtil.exe -c <ContentSource-Drive>:\<Path>\Adaptiva\P2PClient -s Install.cmd -o <ContentSource-Drive>:\<Path>\Adaptiva\P2PClient`

Create Intune app

1. Log into Endpoint Management (<https://endpoint.microsoft.com>) using the account with the appropriate role assignment
2. Open the **Apps** blade and click **All apps**

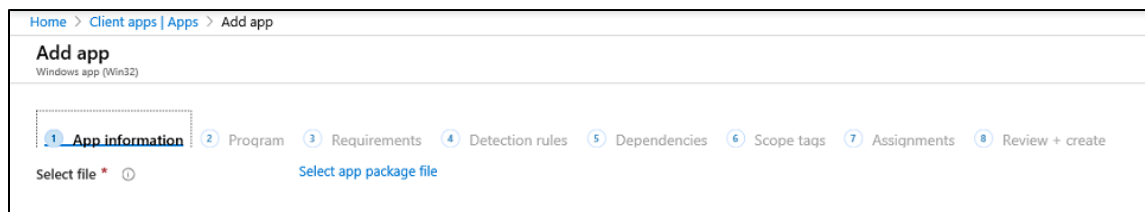


3. Click **+ Add**. The following will be displayed on the far right pane, select the app type
 Under **Other**, select **Windows app (Win32)**

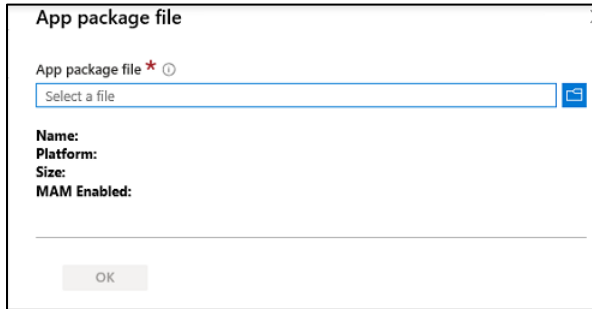


Click **Select**

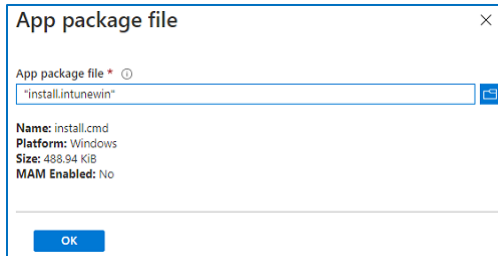
4. The **Add app** pane is displayed



- Click on **Select app package file**. The following will be displayed on the right



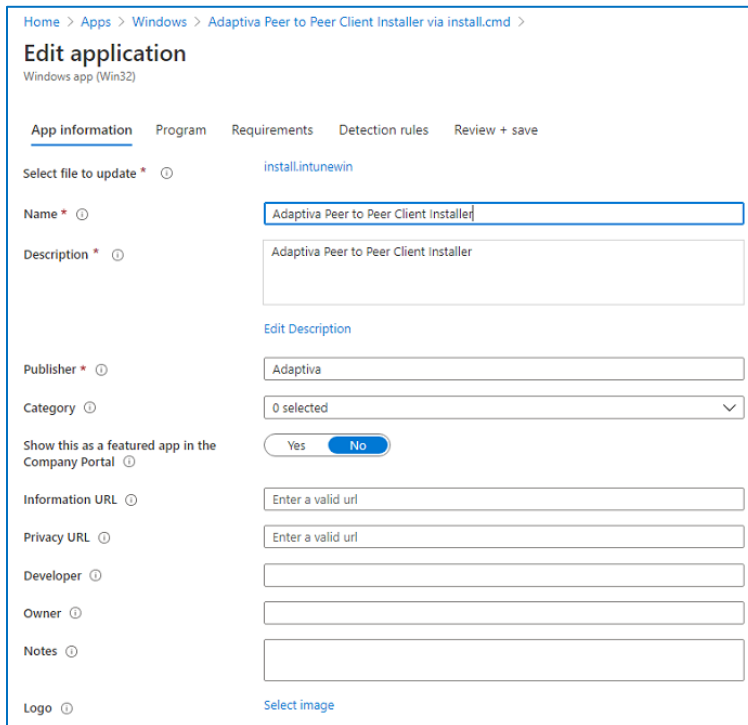
- Click on the folder icon and browse to the path with the .intunewin file: <ContentSource-Drive>:\<Path>\Adaptiva\P2PClient
- Select the Install.intunewin file and click **Open**
- The right pane will be updated



Click **OK**

- Update the rest of the **App Information**, as necessary.

The properties that are starred are mandatory



The Name field is what will display to the end-user. The other information is also available for the user to see. Make the following updates:

Name: Update the name to a friendly name with spaces.

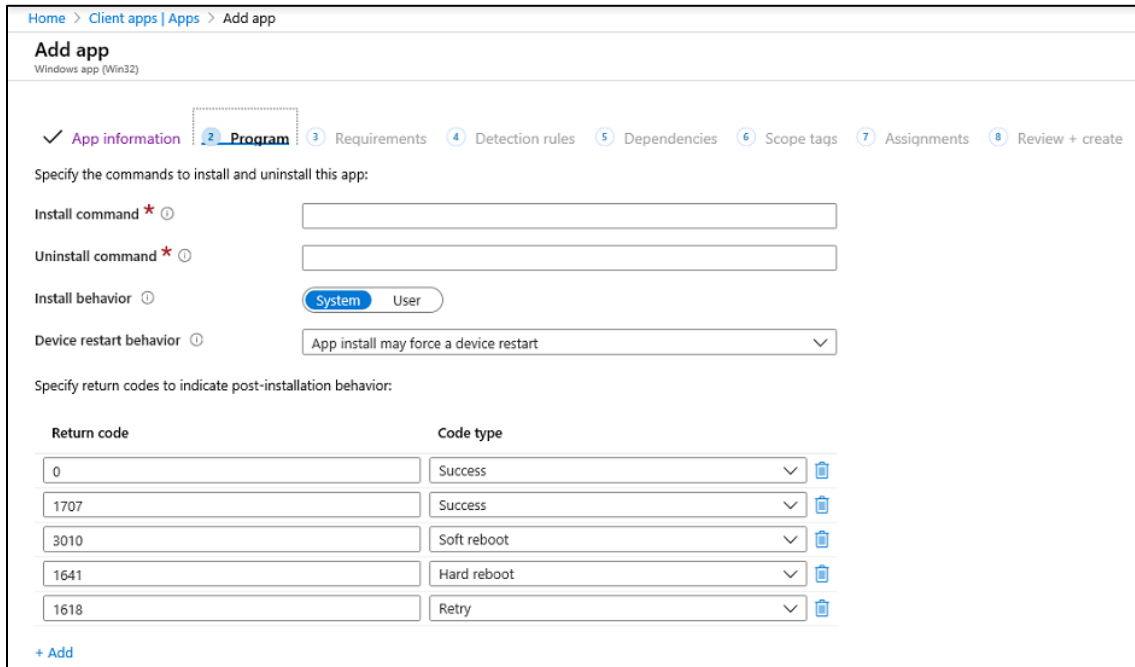
Description: Write a friendly description

Publisher: Adaptiva

Update the other fields as required by the company's standards

Click **Next**

10. On the **Program** tab



Home > Client apps | Apps > Add app

Add app

Windows app (Win32)

✓ App information 2 **Program** 3 Requirements 4 Detection rules 5 Dependencies 6 Scope tags 7 Assignments 8 Review + create

Specify the commands to install and uninstall this app:

Install command * ⓘ

Uninstall command * ⓘ

Install behavior ⓘ System User

Device restart behavior ⓘ App install may force a device restart ▼

Specify return codes to indicate post-installation behavior:

Return code	Code type
<input type="text" value="0"/>	Success ▼
<input type="text" value="1707"/>	Success ▼
<input type="text" value="3010"/>	Soft reboot ▼
<input type="text" value="1641"/>	Hard reboot ▼
<input type="text" value="1618"/>	Retry ▼

[+ Add](#)

Enter the following.

Install command:

```
install.cmd AdaptivaServer.adaptiva.com ServerGUID TinyURL [Password=Secret] [Additional parameters as required]
```

Parameters need to be in the same order as defined in Install.cmd. Be sure to replace with the specific server information.

Uninstall command:

```
%windir%\system32\msiexec.exe /i AdaptivaP2PCClientInstaller.msi UNINSTALL=1
```

Install behavior: System

Device restart behavior: No specific action

Click **Next**

11. On the **Requirements** tab

Home > Client apps | Apps > Add app

Add app

Windows app (Win32)

✓ App information ✓ Program **3 Requirements** 4 Detection rules 5 Dependencies 6 Scope tags 7 Assignments 8 Review + create

Specify the requirements that devices must meet before the app is installed:

Operating system architecture * ⓘ 0 selected

Minimum operating system * ⓘ Select one

Disk space required (MB) ⓘ

Physical memory required (MB) ⓘ

Minimum number of logical processors required ⓘ

Minimum CPU speed required (MHz) ⓘ

Configure additional requirement rules

Type	Path/Script
No requirements are specified.	

+ Add

Select the **Operating System architecture**: 32-bit and/or 64-bit

Operating system architecture * ⓘ 2 selected

Minimum operating system * ⓘ

Disk space required (MB) ⓘ

32-bit

64-bit

Select the **Minimum Operating system** where the installation can occur

Minimum operating system * ⓘ Windows 10 1607

Disk space required (MB) ⓘ Windows 10 1607

Physical memory required (MB) ⓘ Windows 10 1703

Minimum number of logical processors required ⓘ Windows 10 1709

Minimum CPU speed required (MHz) ⓘ Windows 10 1803

Windows 10 1809

Windows 10 1903

Complete the rest of the fields as necessary

Additional requirements can also be added

Click **Next**

12. On the **Detection Rules** tab

Home > Apps | All apps > Add app

Add app

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements **4 Detection rules** 5 Dependencies 6 Scope tags 7 Assignments 8 Review + create

Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ Select one

Manually configure detection rules

Use a custom detection script

Select the drop-down for **Rules format** and select **Manually configure detection rules**

Type	Path/Code
No rules are specified.	
+ Add	

13. Click **+ Add**

14. In the right-hand pane the **Detection Rule** pane will be displayed

Detection rule

Create a rule that indicates the presence of the app.

Rule type *

Select one

▼

15. Select the rule type MSI and enter the information

Detection rule

Create a rule that indicates the presence of the app.

Rule type *

MSI

▼

MSI product code *

Product code cannot be empty.

MSI product version check

Yes

No

MSI product code: Enter the Product code. E.g. {90A2F112-3EF2-4820-AF69-259AB35A566B} This will change with every version. See the Release Notes for a complete list of Product IDs.

MSI product version check: No

Click **OK**

Click **Next**

16. On the **Dependencies** tab

Add app

Windows app (Win32)

✓ App information

✓ Program

✓ Requirements

✓ Detection rules

Dependencies

Scope tags

Assignments

Review + create

Software dependencies are applications that must be installed before this application can be installed. There is a maximum of 100 dependencies, which includes the dependencies of any included dependencies, as well as the app itself. [Learn more](#)

Name

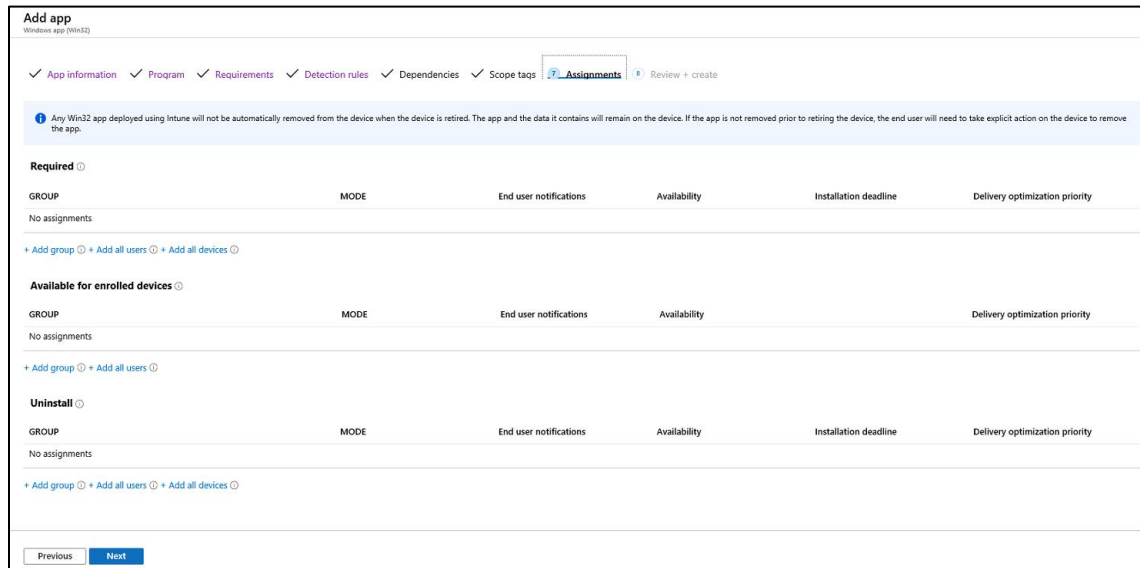
Automatically Install

No results.

[+ Add](#)

Click **Next**

17. On the **Assignments** tab.



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

All users or all devices can also be added

Click **Next**

18. Review the Summary information provided and click **Create**

Full Client Installer using AdaptivaClientSetup.exe

There is no application type that supports a .EXE, so we have to create a .intunewin file so it can be imported using the Windows app (Win32) type. This is the same process that Adaptiva will use to automate the creation of apps, but it will not have the connection to Adaptiva to download the content via Adaptiva technologies.

This process will download the full Adaptiva client (approx. 75MB) using Intune. It is recommended to use the P2P Client Installer method as that will only download 1Mb using Intune.

Follow the steps below to create the .intunewin file and create the Intune app

Create .intunewin file

The intunewin tool was downloaded earlier.

1. Create a folder to hold the single installation
2. Create a content source folder as follows:

<ContentSource-Drive>:\<Path>\Adaptiva\FullClient

Copy the **AdaptivaClientSetup.exe** from the Installation source into the FullClient folder

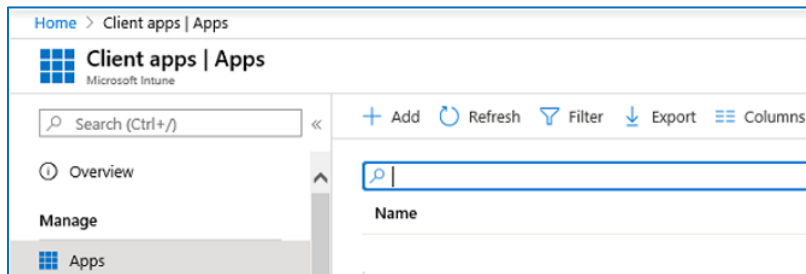
- ☐ Open a command prompt to the folder where the intunewin tool is located
- ☐ Type the following command or just run the command to be prompted:

```
Intunewinapputil -c "<ContentSource-Drive>:\<Path>\Adaptiva\FullClient" -s
AdaptivaClientSetup.exe -o "<ContentSource-Drive>:\<Path>\Adaptiva\FullClient"
```

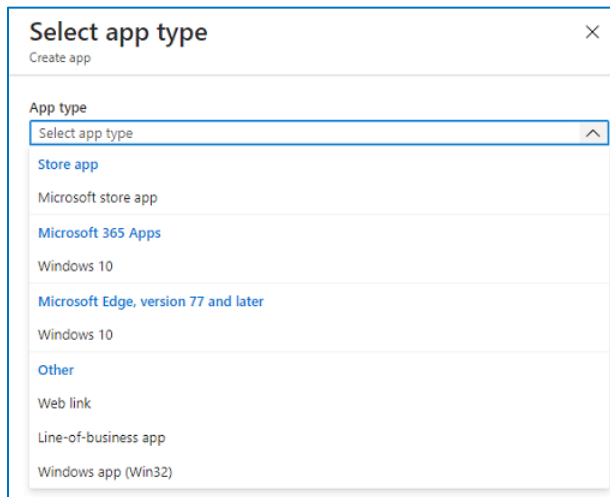
- ☐ The AdaptivaClientSetup.intunewin will be created in the FullClient folder

Create Intune app

- ❑ Log into Endpoint Management (<https://endpoint.microsoft.com>) using the account with the appropriate role assignment
- ❑ Open the **Apps** blade and click **All apps**

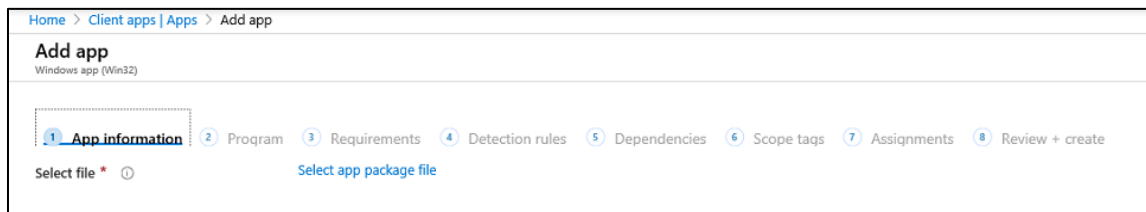


- ❑ Click **+ Add**. The following will be displayed on the far right pane, select the app type
Under **Other**, select **Windows app (Win32)**

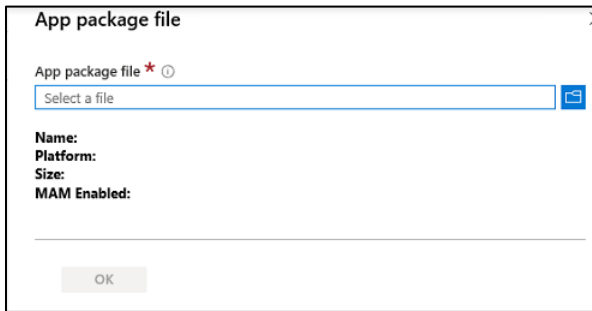


Click **Select**

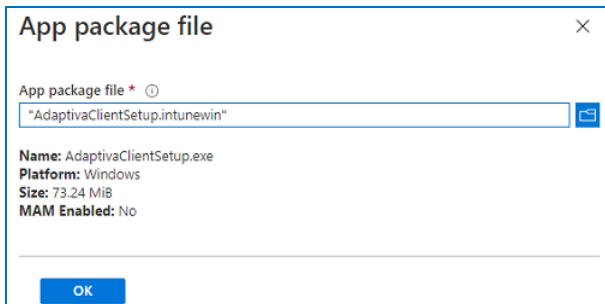
- ❑ The **Add app** pane is displayed



- ❑ Click on **Select app package file**. The following will be displayed on the right



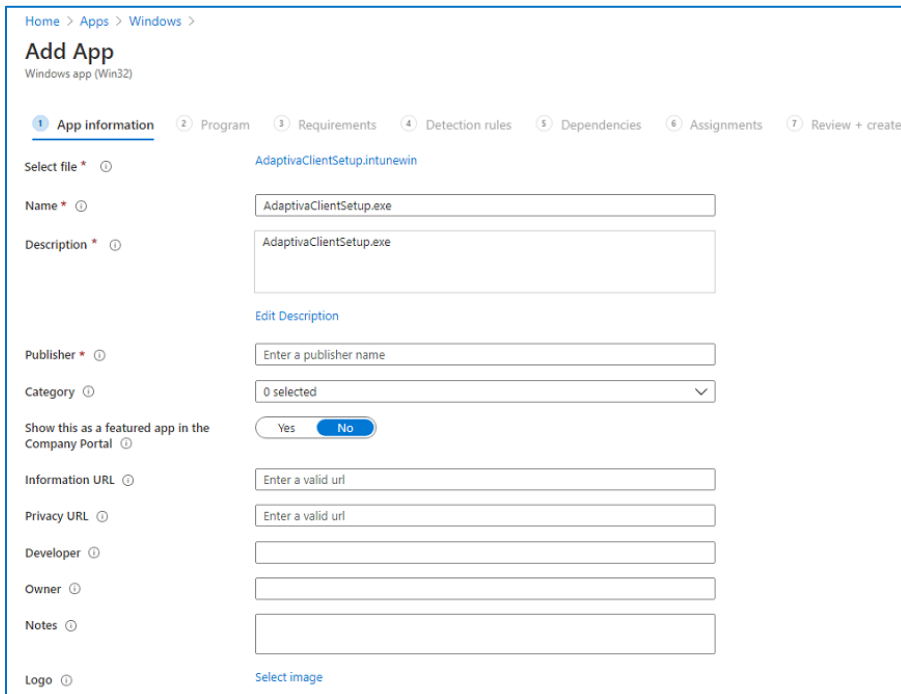
- ❑ Click on the folder icon and browse to the path with the .intunewin file: <ContentSource-Drive>:\<Path>\Adaptiva\FullClient
- ❑ Select the .intunewin file and click **Open**
- ❑ The right pane will be updated



Click **OK**

- ❑ Update the rest of the **App Information**, as necessary.

The properties that are starred are mandatory



The Name field is what will display to the end-user. The other information is also available for the user to see. Make the following updates:

Name: Update the name to a friendly name with spaces. Remove the .exe

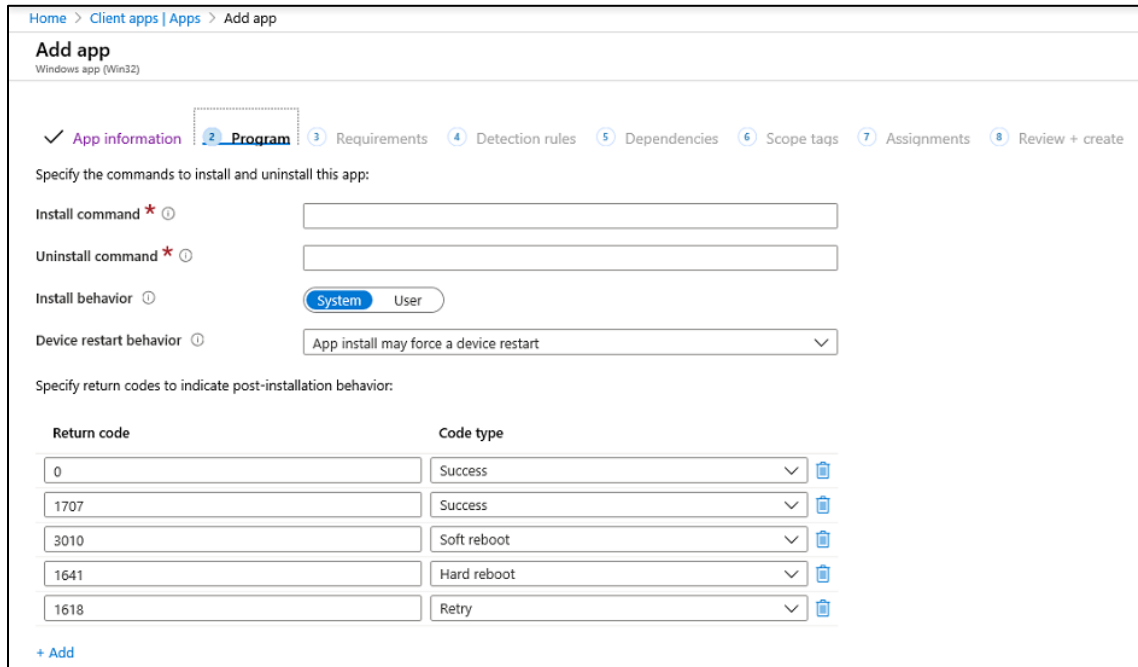
Description: Write a friendly description

Publisher: Adaptiva

Update the other fields as required by the company's standards

Click **Next**

1. On the **Program** tab



Home > Client apps | Apps > Add app

Add app

Windows app (Win32)

✓ App information 2. **Program** 3. Requirements 4. Detection rules 5. Dependencies 6. Scope tags 7. Assignments 8. Review + create

Specify the commands to install and uninstall this app:

Install command * ⓘ

Uninstall command * ⓘ

Install behavior ⓘ System User

Device restart behavior ⓘ App install may force a device restart ▼

Specify return codes to indicate post-installation behavior:

Return code	Code type
<input type="text" value="0"/>	Success ▼
<input type="text" value="1707"/>	Success ▼
<input type="text" value="3010"/>	Soft reboot ▼
<input type="text" value="1641"/>	Hard reboot ▼
<input type="text" value="1618"/>	Retry ▼

[+ Add](#)

Enter the following.

Install command:

```
AdaptivaClientSetup.exe -InstallorUpgrade -ServerName AdaptivaServer.FQDN -
CloudRelay -ServerGUID <GUID> [-Password <password>] [additional parameters]
```

IMPORTANT: Include the following switches as required if the Cloud Relay service or if HTTP client communications will be used:

Cloud Relay service: -CloudRelay, -ServerGUID <GUID>, -Password <auth. Secret>

HTTP communications: -ServerURL <ServerURL:port>

Uninstall command:

```
AdaptivaClientSetup.exe -Uninstall
```

Install behavior: System

Device restart behavior: No specific action

Click **Next**

❑ On the **Requirements** tab

Home > Client apps | Apps > Add app

Add app

Windows app (Win32)

✓ App information ✓ Program **3 Requirements** 4 Detection rules 5 Dependencies 6 Scope tags 7 Assignments 8 Review + create

Specify the requirements that devices must meet before the app is installed:

Operating system architecture * ⓘ 0 selected

Minimum operating system * ⓘ Select one

Disk space required (MB) ⓘ

Physical memory required (MB) ⓘ

Minimum number of logical processors required ⓘ

Minimum CPU speed required (MHz) ⓘ

Configure additional requirement rules

Type	Path/Script
No requirements are specified.	

+ Add

Select the **Operating System architecture**: 32-bit and/or 64-bit

Operating system architecture * ⓘ 2 selected

Minimum operating system * ⓘ

Disk space required (MB) ⓘ

32-bit

64-bit

Select the **Minimum Operating system** where the installation can occur

Minimum operating system * ⓘ Windows 10 1607

Disk space required (MB) ⓘ

Physical memory required (MB) ⓘ

Minimum number of logical processors required ⓘ

Minimum CPU speed required (MHz) ⓘ

Windows 10 1607

Windows 10 1703

Windows 10 1709

Windows 10 1803

Windows 10 1809

Windows 10 1903

Complete the rest of the fields as necessary

Additional requirements can also be added

Click **Next**

❑ On the **Detection Rules** tab

Home > Apps | All apps > Add app

Add app

Windows app (Win32)

✓ App information ✓ Program ✓ Requirements **4 Detection rules** 5 Dependencies 6 Scope tags 7 Assignments 8 Review + create

Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ

Select one

Manually configure detection rules

Use a custom detection script

Select the drop-down for **Rules format** and select **Manually configure detection rules**

Type	Path/Code
No rules are specified.	
+ Add	

- ❑ Click [+ Add](#)
- ❑ In the right-hand pane the **Detection Rule** pane will be displayed

Detection rule

Create a rule that indicates the presence of the app.

Rule type *

Select one

▼

- ❑ Select the rule type Registry and enter the information

Detection rule

Create a rule that indicates the presence of the app.

Rule type *

Registry

▼

Key path *

Value name

Detection method *

Select one

▼

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

Yes

No

Key path: HKEY_LOCAL_MACHINE\Software\WOW6432Node\Adaptiva\Client

Value name: slm.version

Detection method: Value exists

NOTE: For clients that are on the internet that already have Adaptiva installed, use the Detection method Version comparison, operator: Equals, Value: Enter the version being installed, e.g. 8.0.923.0

Associated with a 32-bit app on 64-bit clients: Yes

Click [OK](#)

Click **Next**

- ❑ On the **Dependencies** tab

Add app

Windows app (Win32)

✓ App information

✓ Program

✓ Requirements

✓ Detection rules

5 Dependencies

6 Scope tags

7 Assignments

8 Review + create

Software dependencies are applications that must be installed before this application can be installed. There is a maximum of 100 dependencies, which includes the dependencies of any included dependencies, as well as the app itself. [Learn more](#)

Name

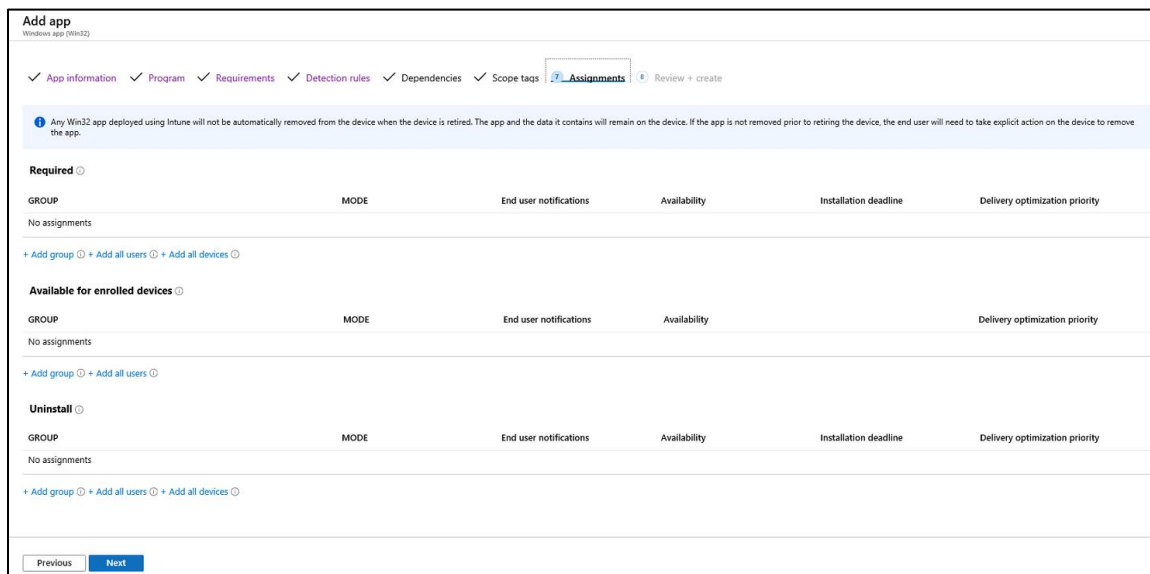
Automatically Install

No results.

[+ Add](#)

Click **Next**

- ❑ On the **Assignments** tab.



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

All users or all devices can also be added

Click **Next**

- ❑ Review the Summary information provided and click **Create**

Client Installation using Workspace ONE

When integrating OneSite with Workspace ONE, the Adaptiva Client will need to be deployed to target devices.

P2P Client Installer

AdaptivaP2PClientInstaller.msi is a 1MB download that will install and query the computers on the local subnet to see if any device has the Adaptiva client installed. If there is, the AdaptivaClientSetup.exe will be transferred via Peer to Peer over the local subnet and installed. If no device on the subnet has Adaptiva installed, it will copy the AdaptivaClientSetup.exe from a network share or an internet-based URL and install.

Complete the following prerequisites to deploy the Adaptiva P2P Client Installer to WorkspaceONE clients

Share AdaptivaClientSetup.exe

Share this for the on-premises users

- ❑ Create a content source folder as follows:
<ContentSource-Drive>:\<Path>\Adaptiva\FullClient
Copy the AdaptivaClientSetup.exe from the Installation source into the FullClient folder
- ❑ Share this folder on the server as **AdaptivaClient**
Share permissions: Everyone: READ
NTFS permissions: Domain Computers: Read and Execute, List, Read

NOTE: It is also possible to host the AdaptivaClientSetup.exe on a web-based URL for clients on the internet to be able to download. The URL must point explicitly to the AdaptivaClientSetup.exe.

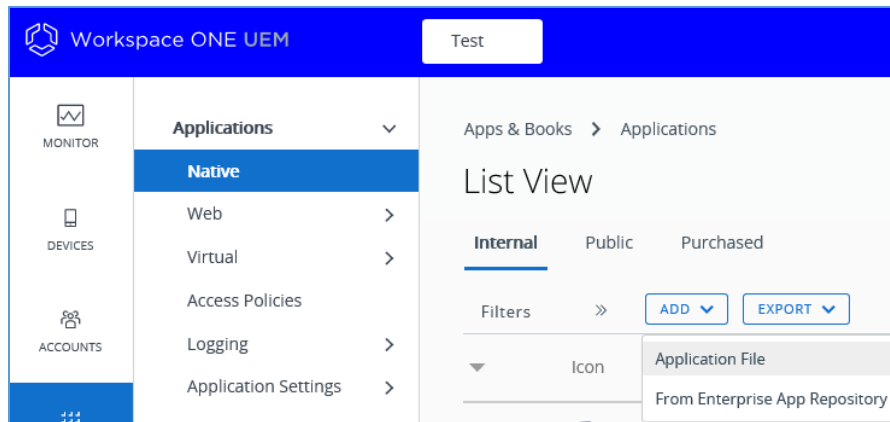
Create WorkspaceONE application

Clients MUST be on-premises to be able to download the Full client installer from the Server UNC. A web-based URL may also be used if clients will not be on-premises.

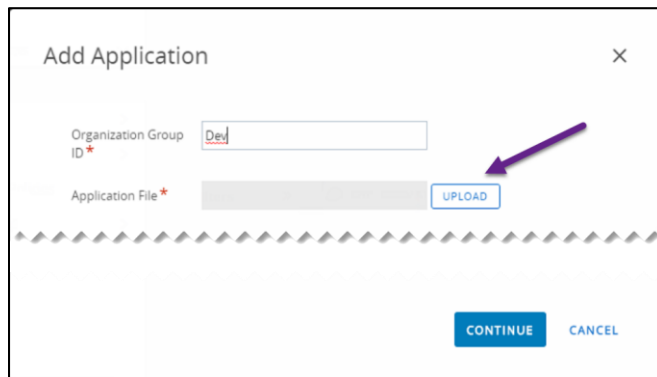
- ❑ Open **Workspace ONE** console

NOTE: The Workspace ONE console is updated regularly so screens may have changed

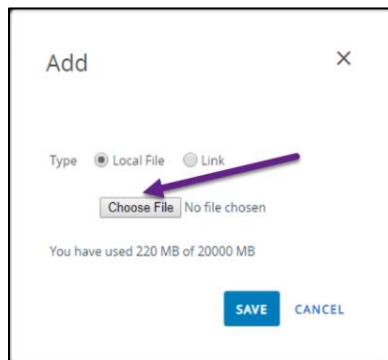
- ❑ Navigate to **Apps & Books** and select **Native**
- ❑ Click the **Add** and select **Application File**



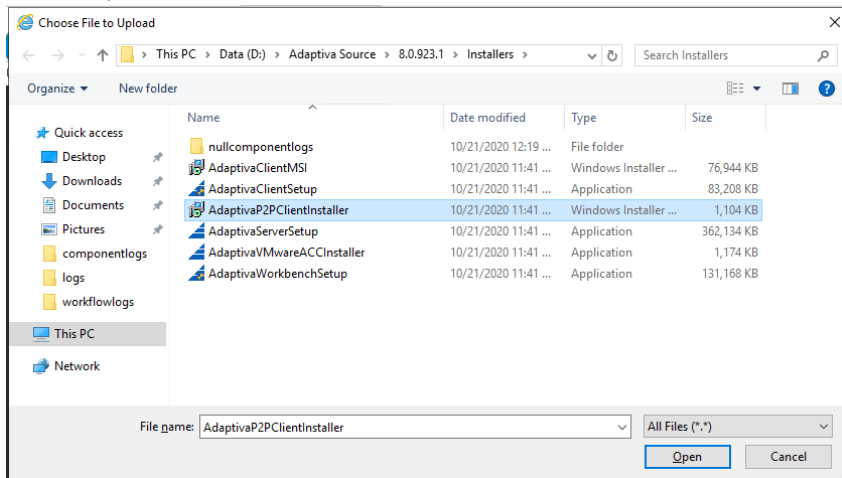
- ❑ Click the **Upload** button



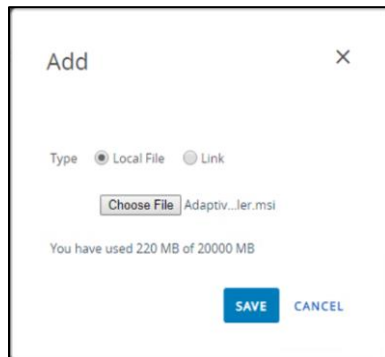
- ❑ Select **Local File** and click on **Browse**



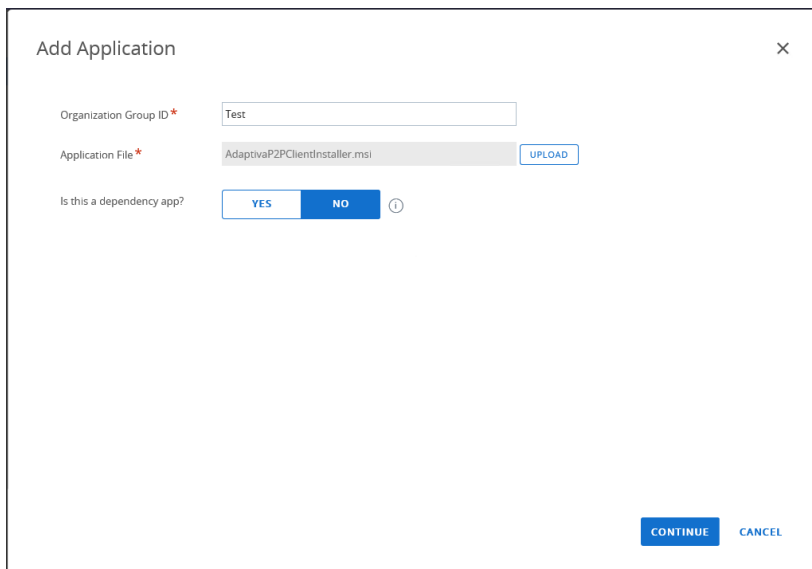
- ❑ Navigate to the file to be published, **AdaptivaP2PClientInstaller.exe**, and click **Open**



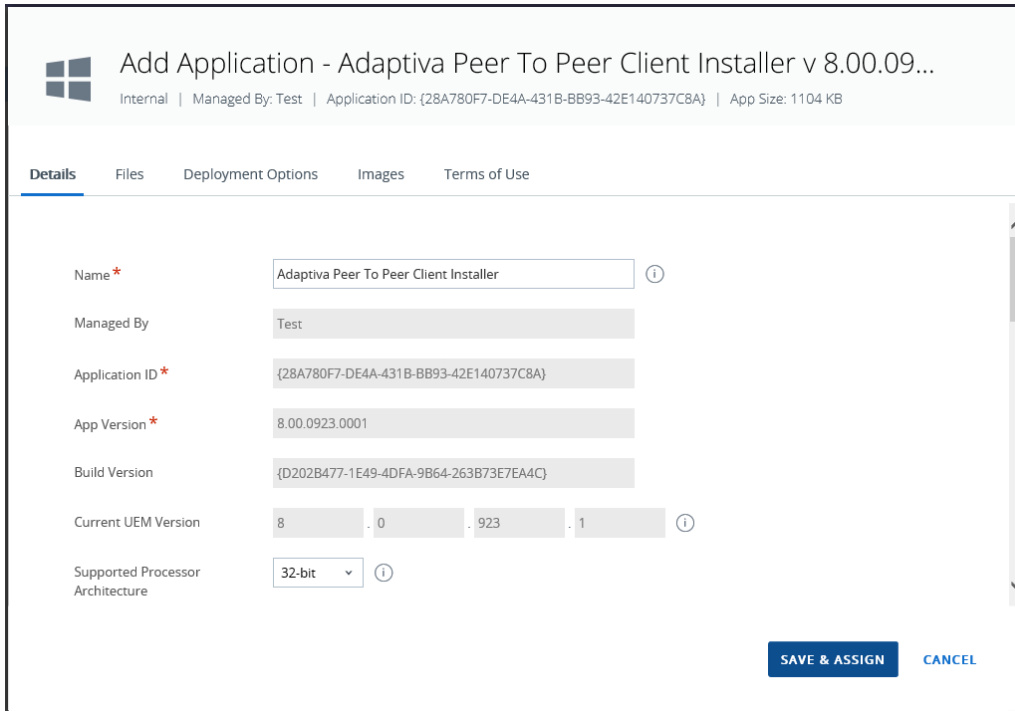
- ❑ Click **Save** and file will upload to Workspace ONE



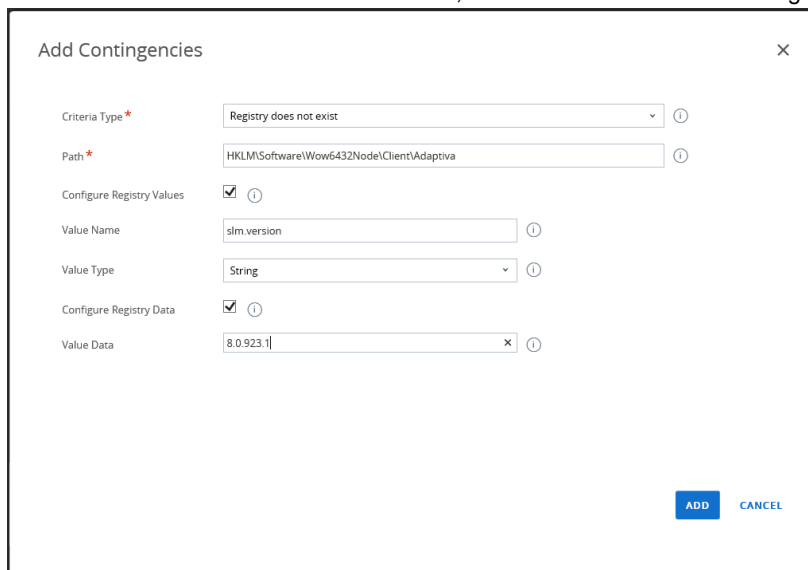
- ❑ Validate that file name is correct and click **Continue**



- ❑ The Application properties will be displayed. Because this was an MSI package, many of the required fields have already been completed



- On the **Details** page
 - Name: (Optional) Change the name of the application
 - Supported Processor Architecture: Leave at 32-bit
 - Minimum OS: (Optional) Change the minimum Windows 10 OS version where this can be installed
 - Supported Models: Desktop
- On the **Deployment Options** page
 - Data Contingencies: (Optional) Add a Data Contingencies to determine if the registry key for the to be installed version exists. If this is not added, installation will occur for all targeted devices.



Criteria Type: Registry does not exist

Path: Enter HKLM\Software\Wow6432Node\Client\Adaptiva

Configure Registry Values: Checked

- Value Name: Enter slm.version
- Value Type: string
- Configure Registry Data: Checked
- Value Data: Enter the version that is to be installed. i.e.: 8.0.926.0
- Disk Space Required: (Optional) Enter 250MB
- Install Context: Device
- Install Command:

NOTE: If the Adaptiva Client has already been deployed using AdaptivaClientSetup.exe then the MSI Product key will not be registered, and clients will reinstall.

Also, it is NOT recommended to mix the installation of the MSI and the EXE. Different values are registered in Add/Remove Programs and one product cannot uninstall the other completely.

If an MSI must be used to deploy the Adaptiva client, deploy the AdaptivaP2PClientInstaller.msi

```
Msixexec.exe /i AdaptivaP2PClientInstaller.msi /qn SERVERNAME=ServerFQDN
SOURCEUNCPATH=\\ServerFQDN\AdaptivaClient\AdaptivaClientSetup.exe
WAITFORCOMPLETION=1
```

NOTE: When using the AdaptivaP2PClientInstaller.msi, a share must be created with the full Adaptiva client on a server or AdaptivaClientSetup.exe can be hosted on an internet-based URL.

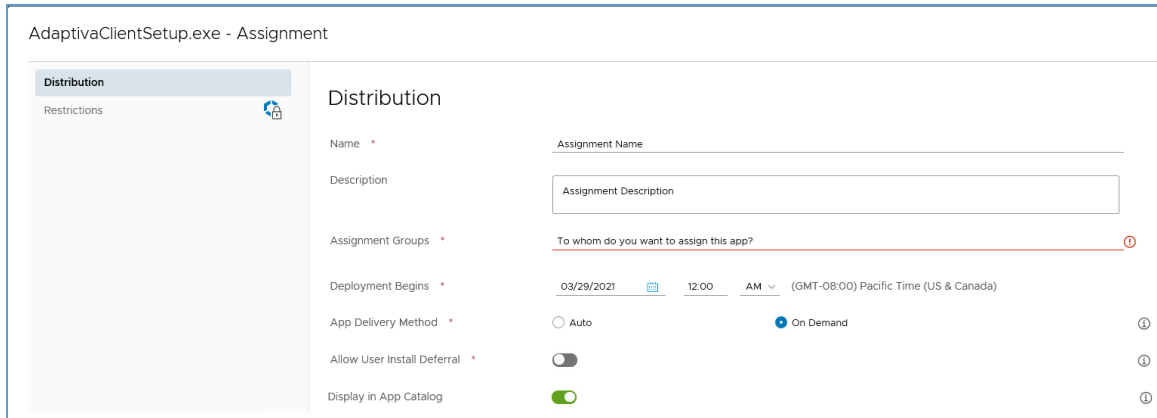
When a URL is used, add the parameter: SOURCEURLS=http[s]://<url>

IMPORTANT: Include the following switches as required if the Cloud Relay service or if HTTP client communications will be used:

Cloud Relay service: CLOUDRELAY=1, SERVERGUID=<GUID>, PASSWORD=<auth. Secret>

HTTP communications: SERVERURL=<ServerURL:port>

- Retry Count: 3
- Retry Interval: 5
- Install Timeout: 60
- ☐ Click **Save & Assign**
- ☐ On the Distribution page



- Name: Enter the assignment Name
- Assignment Groups: Enter the Assignment group(s)
- App Delivery Method: Select Auto or On Demand
- Allow User Install Deferral: Enable or Disable

- ☐ Click **Create**, then **Save**. Finally, click on **Publish**

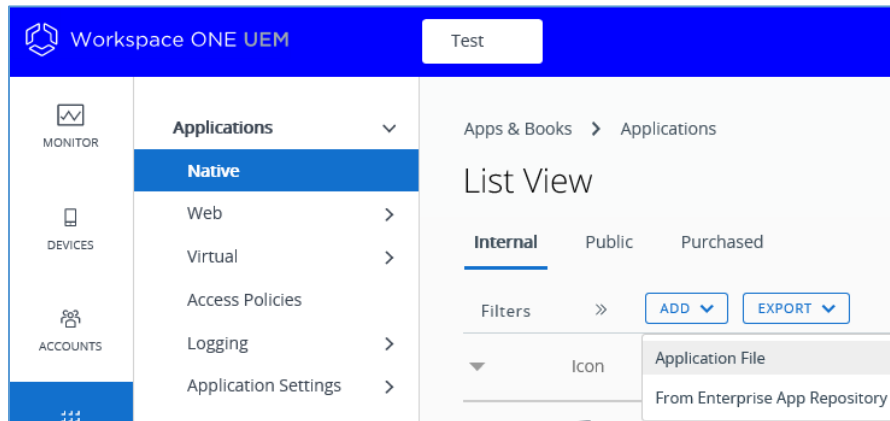
Full Client Installer using AdaptivaClientSetup.exe

Follow the steps below to use the Full Client installer .EXE via WorkspaceONE.

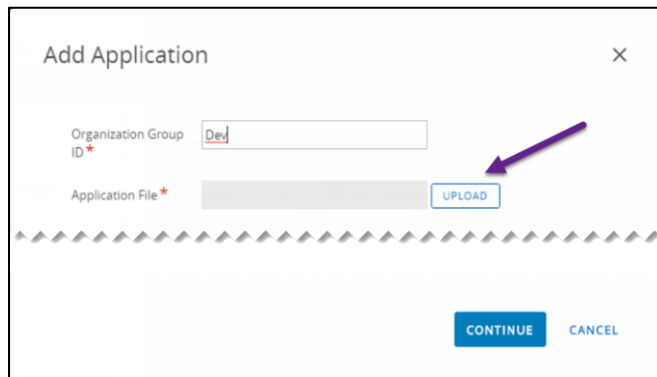
- ☐ Open WorkspaceONE console

NOTE: The Workspace ONE console is updated regularly so screens may have changed

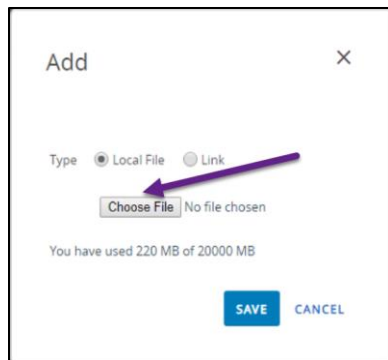
- ☐ Navigate to **Apps & Books** and select **Native**
- ☐ Click the **Add** and select **Application File**



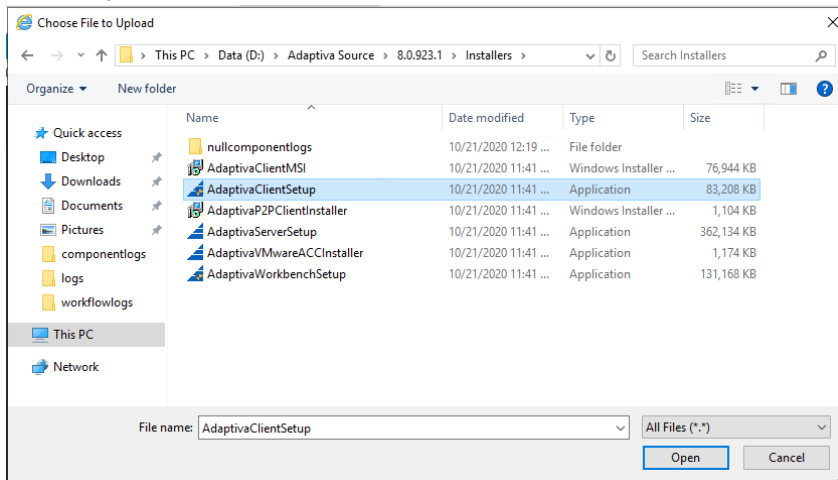
- ☐ Click the **Upload** button



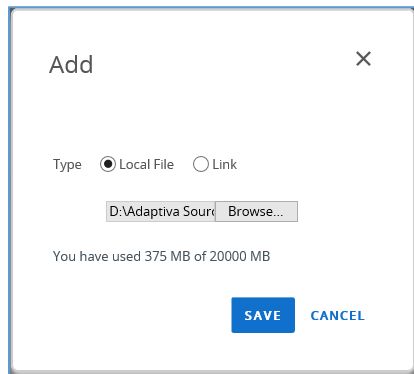
- ☐ Select **Local File** and click on **Browse**



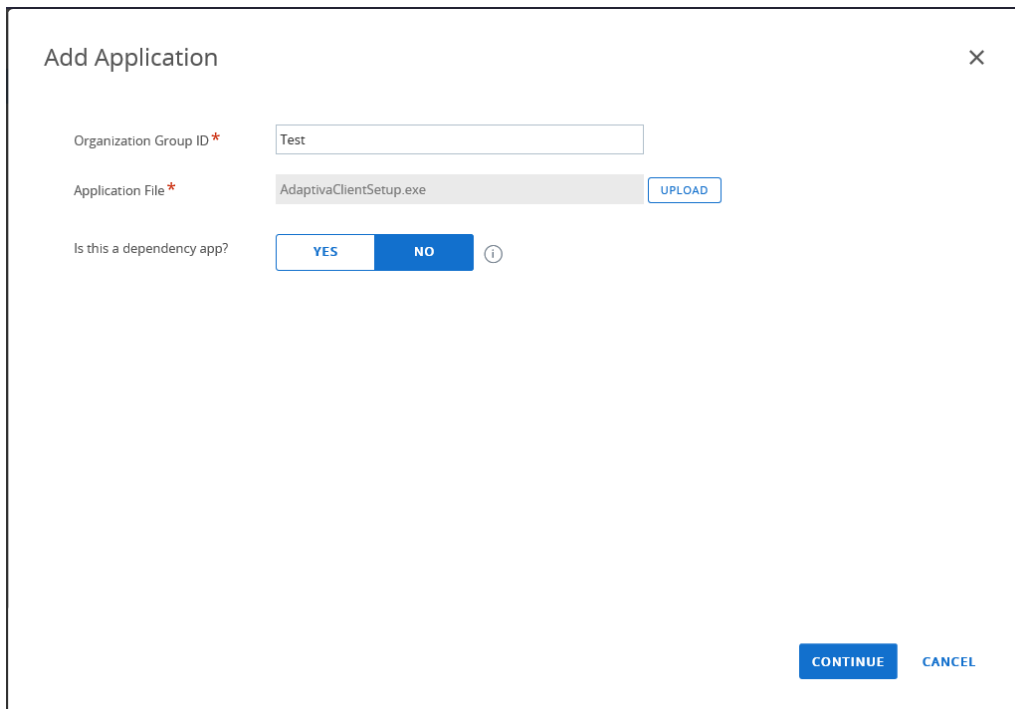
- ❑ Navigate to the file to be published, **AdaptivaClientSetup.exe**, and click **Open**



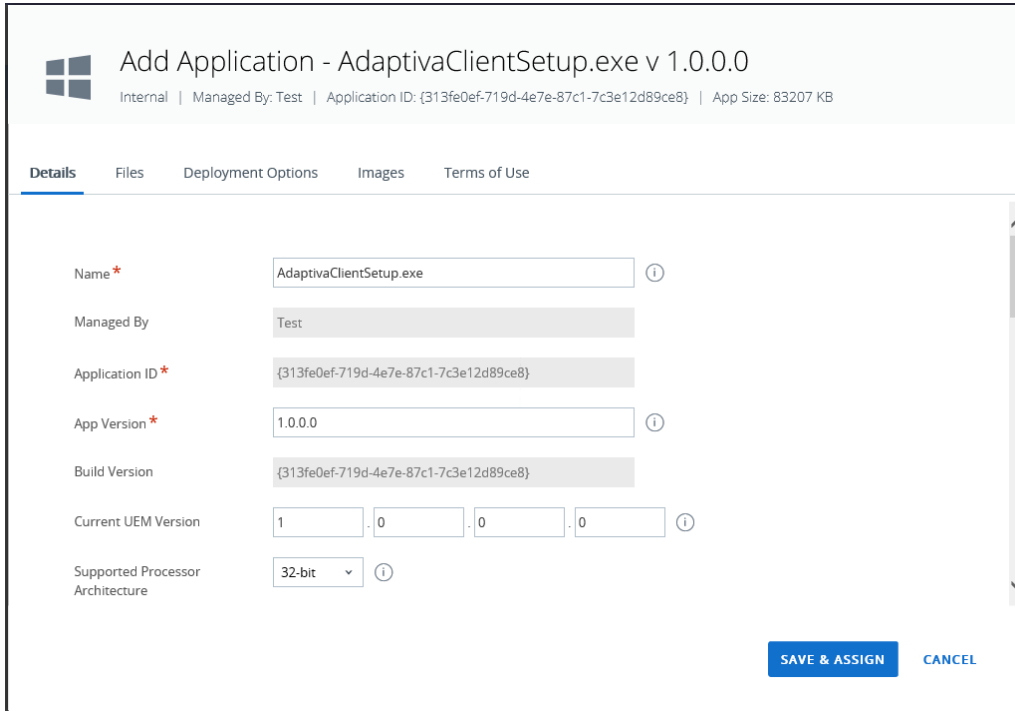
- ❑ Click **Save** and file will upload to Workspace ONE



- ❑ Validate that file name is correct and click **Continue**



- ❑ The Application properties will be displayed:



Add Application - AdaptivaClientSetup.exe v 1.0.0.0
Internal | Managed By: Test | Application ID: {313fe0ef-719d-4e7e-87c1-7c3e12d89ce8} | App Size: 83207 KB

Details | Files | Deployment Options | Images | Terms of Use

Name* ⓘ

Managed By

Application ID*

App Version* ⓘ

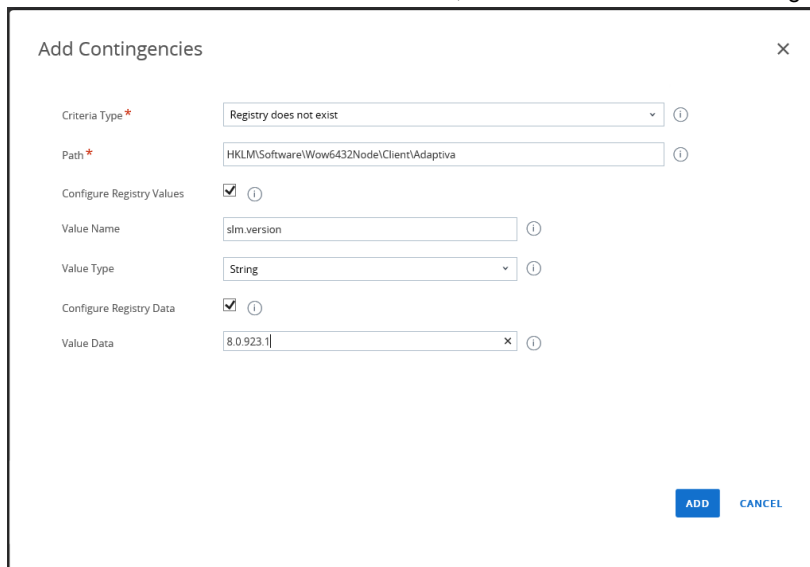
Build Version

Current UEM Version . . . ⓘ

Supported Processor Architecture ⓘ

SAVE & ASSIGN **CANCEL**

- On the **Details** page
 - Name: (Optional) Change the name of the application
 - App Version: The version cannot be automatically read from the .exe, so update the version
 - Current UEM Version: (Optional) Adaptiva Client version can be entered here.
 - Supported Processor Architecture: Leave at 32-bit
 - Minimum OS: (Optional) Change the minimum Windows 10 OS version where this can be installed
 - Supported Models: Desktop
- On the **Files** page, scroll down
 - Uninstall command: AdaptivaClientSetup.exe -uninstall
- On the **Deployment Options** page
 - Data Contingencies: (Optional) Add a Data Contingencies to determine if the registry key for the to be installed version exists. If this is not added, installation will occur for all targeted devices.



Add Contingencies ✕

Criteria Type* ⓘ

Path* ⓘ

Configure Registry Values ☒ ⓘ

Value Name ⓘ

Value Type ⓘ

Configure Registry Data ☒ ⓘ

Value Data ⓘ

ADD **CANCEL**

Criteria Type: Registry does not exist

Path: Enter HKLM\Software\Wow6432Node\Client\Adaptiva

Configure Registry Values: Checked

Value Name: Enter slm.version

Value Type: string

Configure Registry Data: Checked

Value Data: Enter the version that is to be installed. i.e.: 8.0.926.0

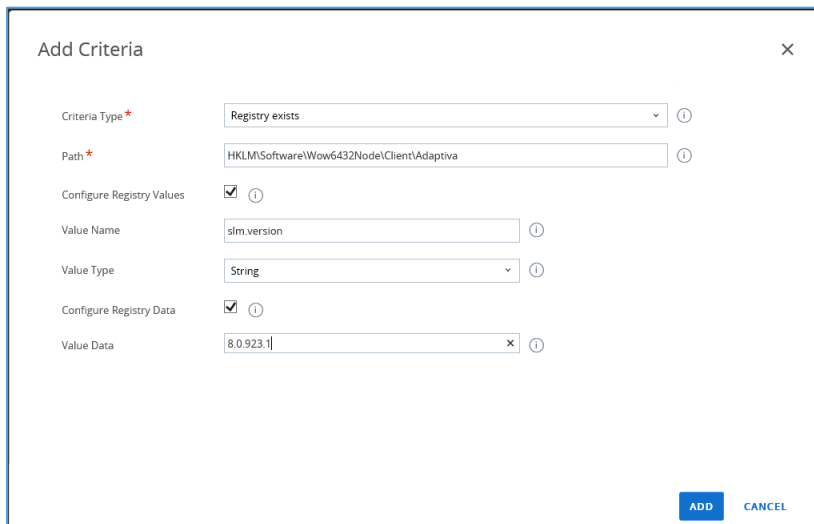
- Disk Space Required: (Optional) Enter 250MB
- Install Context: Device
- Install Command: AdaptivaClientSetup.exe -INSTALLORUPGRADE -SERVERNAME serverfqdn | -SERVERIP serveripaddress

IMPORTANT: Include the following switches as required if the Cloud Relay service or if HTTP client communications will be used:

Cloud Relay service: -CloudRelay, -ServerGUID <GUID>, -Password <auth. Secret>

HTTP communications: -ServerURL <ServerURL:port>

- Retry Count: 3
- Retry Interval: 5
- Install Timeout: 60
- Identify Application By: Select **Defining Criteria** and click on **+Add**



Criteria Type: Registry exists

Path: Enter HKLM\Software\Wow6432Node\Client\Adaptiva

Configure Registry Values: Checked

Value Name: Enter slm.version

Value Type: string

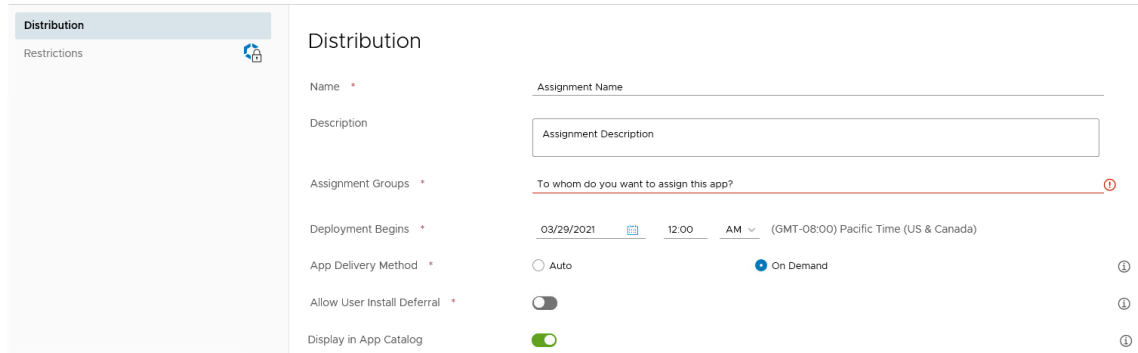
Configure Registry Data: Checked

Value Data: Enter the version that was installed.

- Click on **Add**
- ❑ Click **Save & Assign**

❑ On the Distribution page

AdaptivaClientSetup.exe - Assignment



Name: Enter the assignment Name

Assignment Groups: Enter the Assignment group(s)

App Delivery Method: Select Auto or On Demand

Allow User Install Deferral: Enable or Disable

❑ Click **Create**, then **Save**. Finally, click on **Publish**

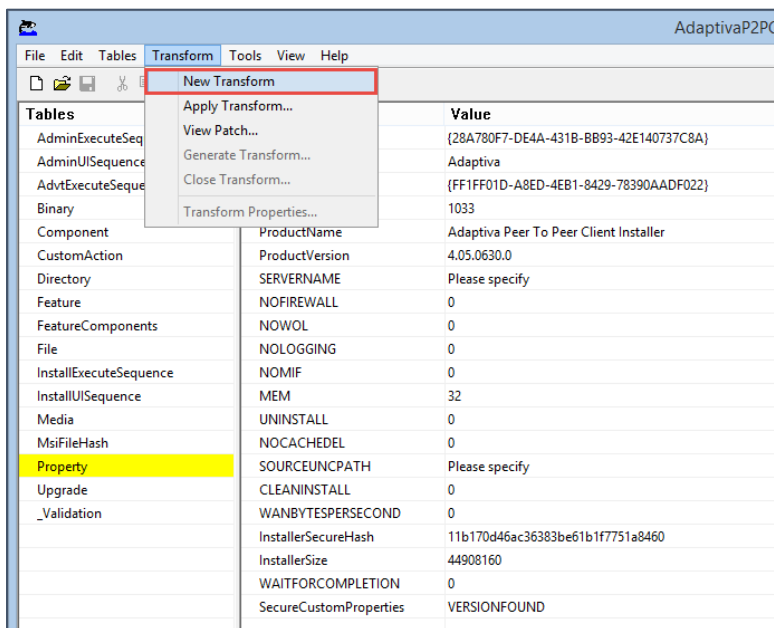
Client Installation using Group Policy

Deploying software through Group Policy cannot use the standard command line syntax. The properties that are set via the command must be set in a Windows Installer transform file. A variety of tools are available that can be used for this task. Orca is a free tool available from Microsoft and is part of the Windows SDK.

Create MST

To create the MST with Orca, follow these steps:

1. In Orca, in the menu bar, select **File / Open** and select the AdaptivaP2PClientInstaller.msi.
2. In the menu bar, select **Transform / New Transform** to create a new transform file.
3. Select the Property table in the Tables list on the left.



4. At a minimum, modify **SOURCEUNCPATH** and either **SERVERNAME** or **SERVERIP**

IMPORTANT: Include the following properties as required, if the Cloud Relay service will be used:

Cloud Relay service: **CLOUDRELAY=1, SERVERGUID=<GUID>, PASSWORD=<password>**

or if using HTTP client communications

HTTP communications: **SERVERURL=<ServerURL:port>**

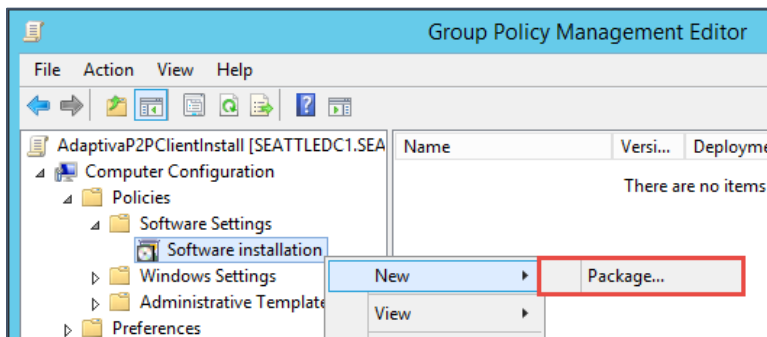
5. In the menu bar, select **Transform / Generate Transform** and save the transform file. Then **Close** the Transform.

Create File Share

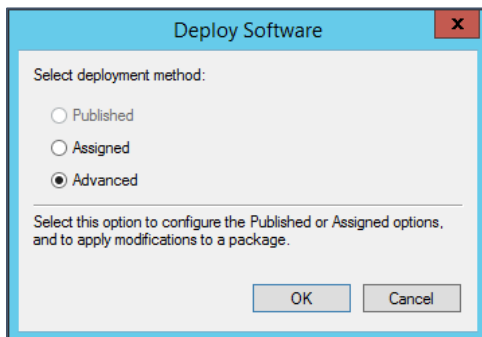
- ❑ Create a content source folder as follows:
<ContentSource-Drive>:\<Path>\Adaptiva\Client
Copy the MSI and MST files into the Client folder
- ❑ Share this folder on the server as **AdaptivaClient**
Share permissions: Everyone: READ
NTFS permissions: Domain Computers: Read and Execute, List, Read

Create Group Policy Object

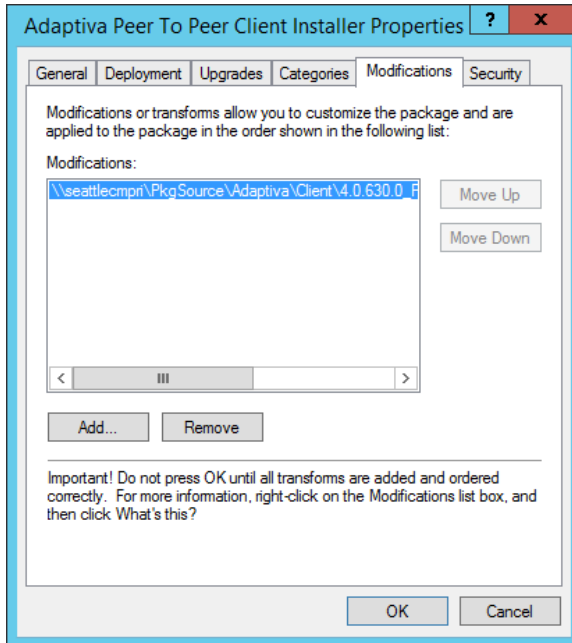
1. To create the group policy, open the Group Policy Management snap-in and create a new or edit an existing GPO.
2. In the Group Policy Management Editor, expand **Computer Configuration / Policies / Software Settings** then right-click the **Software installation** node.
3. In the context menu, select **New / Package**.



4. In the **Open** dialog, navigate to the share location where the MSI is stored and select the **AdaptivaP2PCClientInstaller.msi**
5. In the **Deploy Software** dialog, select **Advanced** and then click **OK**.



6. In the Adaptiva Peer to Peer Client Installer Properties dialog, select the **Modifications** tab, and click the **Add** button to select the MST file.



7. Once complete, click **OK** to save the policy.
8. Target the group policy appropriately. Computers targeted will run the install at next system restart.

Client Installation on macOS or Linux

1. Update the following two parameters (minimum, required) in the ClientSetupConfig.xml file:
 - server_host_name
 - server_guid
 - Use the format `<keyname="Key Name">value</key>`
 - Use information specific to the Adaptiva Server installation environment.
 - See the table below for additional parameters and descriptions available in the ClientSetupConfig.xml file.
2. Create a .zip or .tar.gz file that includes the ClientSetupConfig.xml file and the appropriate installation package for the target Mac or Linux platform.
 - Include only one ClientSetupConfig.xml and one .rpm, .pkg, or .deb file included in the .zip or .tar.gz file.
 - Do not place these files into a folder prior to compressing.
3. Copy the .zip or .tar.gz file and the client_install.sh to the device to install the Adaptiva Client.
4. Open a command shell to the location of the two files:
 - a. Run the command below to verify that _client_install.sh is executable:


```
chmod 744 ./<path>/client_install.sh
```
 - b. Run the following command to install the Adaptiva Client:


```
sudo ./<path>/client_install.sh install <filename.zip> | <filename.tar.gz>
```

For example, to install use:

```
sudo ./client_install.sh install rpmpackage.zip
```

To reinstall and reset the configuration of the Client use:

```
sudo ./client_install.sh reinstall rpmpackage.zip ClientSetupConfig.xml
```

NOTE: When running the client_install.sh interactively, the following message may be returned:

N: Download is performed unsandboxed as root as file './<path-to-install-package>' couldn't be accessed by user '_apt'. - pkgAcquire::Run (13: Permission denied)

This error can be ignored.

ClientSetupConfig.xml Parameters

Key name	Value	Description
location_type	1 use server_host_name 2 use server_ip_address	Determines whether to use server_host_Name or server_ip_address or to provide it to the installation configuration.
server_host_name server_ip_address	Fqdn IP Address	FQDN or IP Address of the Adaptiva Customer Server.
Use_adaptiva_cloud_relay	true false	Enables (true) or disables (false) whether the client uses the Adaptiva Cloud Relay Service to connect when off-premises.
use_client_auth_password	true false	Provides additional security. Set to true if a password is to be used. Requires client_auth_password setting to be entered with the password.
client_auth_password	Password from gear, settings, Client Authorization	Provides additional security. Enter the password that was created on the Adaptiva Server under Security > Settings > Client Authorization .
use_server_guid	true false	If a Server GUID is required set this value to true
server_guid	Server GUID from gear, settings, Server Activation	The Adaptiva Admin can provide the GUID of the Adaptiva Server. Required for clients using the Internet. To use this property, make sure to set the use_adaptiva_cloud_relay to true .
use_server_http_url	true false	If the server_url is to be used, set this to true
server_url	server-url:port	Configures the client to communicate with the Adaptiva Server using HTTP instead of using UDP.
Tenant_guid	Tenant GUID created from Assets, Tenants	Use this to access the Managed Services Provider (MSP) functionality and create and maintain multi-tenant environments This must be added to the provided ClientSetupConfig.xml file

Upgrading

When upgrading the Adaptiva infrastructure to a newer version it is important to follow a top-down upgrade model. The order of upgrade should be as follows:

1. Adaptiva Server component
2. Adaptiva Client on the Adaptiva Server
3. Adaptiva Workbench on the Adaptiva Server (if applicable)
4. Adaptiva Workbench on administrator systems
5. All Adaptiva Clients
6. OneSiteDownloader in Boot Images (if applicable)

IMPORTANT: Elevated SQL permissions (sysadmin) is required to successfully complete the upgrade for both the account running the upgrade as well as the Adaptiva Server SYSTEM account.

The following table describes the options for upgrading each individual component:

Component	Method	Execution
Adaptiva Server	Manual	Manually execute the new version of AdaptivaServerSetup.exe and select the Upgrade option. Click next through each screen. No changes are required.
Adaptiva Workbench	Manual	Manually execute the new version of AdaptivaWorkbenchSetup.exe and select the Upgrade option.
	Unattended	AdaptivaWorkBenchSetup.exe -installorupgrade
Adaptiva Client	Manual	Manually execute the new version of AdaptivaClientSetup.exe and select the Upgrade option.
	Unattended	AdaptivaClientSetup.exe -installorupgrade -servername <serverFQDN> <i>NOTE: When upgrading Adaptiva clients using the -installorupgrade option, the current configuration, content cache, and all settings will be preserved. The P2P Client MSI Installer can also be used to perform a client upgrade as described above.</i> IMPORTANT: When adding Cloud functionality, be sure to include the appropriate command line parameters to enable this feature.
Boot Image	Manual	See the Adaptiva OneSite OSD User Guide to update the Boot image with the new OneSiteDownloader.exe. Recommend using the OneSite Boot Image Powershell Script here Alternatives: Use DISM or 7-Zip

Server Upgrade

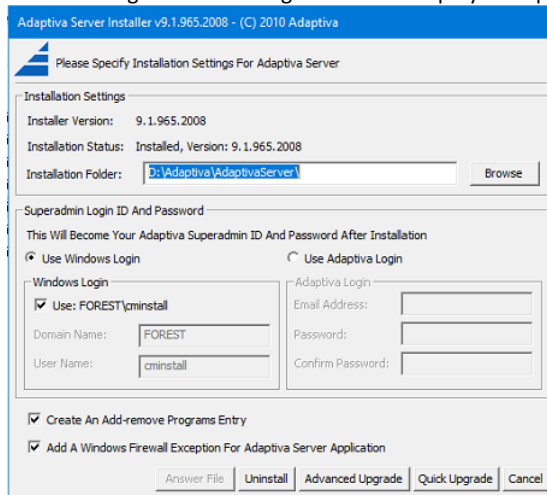
IMPORTANT: Be sure to review the database permissions as documented in the [Installation Prerequisites](#) section here: [SQL permissions](#)

New Antivirus Exclusions

IMPORTANT: For information about new required antivirus exclusions, see the [Antivirus Exceptions](#) section.

New Installation Screens

- The following screen is changed and will simplify the upgrade process.

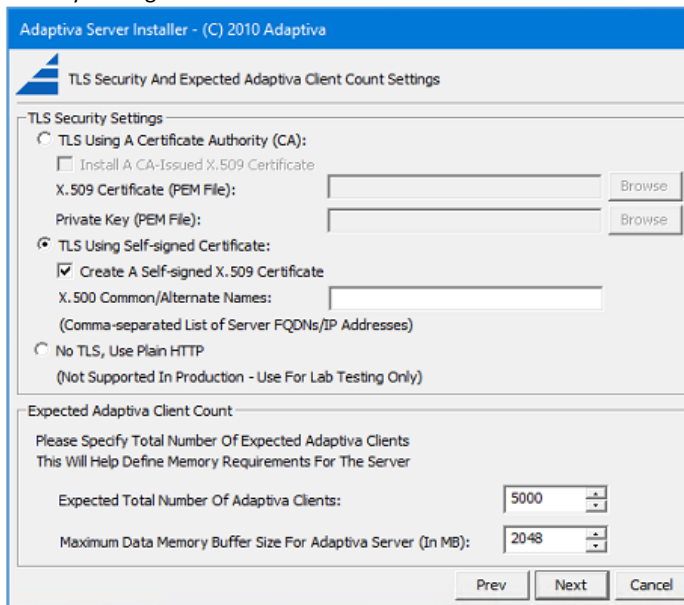


- Click on **Quick Upgrade** (Recommended) to keep all the settings unchanged and begin the installation. TLS Settings (see below) will default to self-signed with the server's FQDN and IP Address(es) in Subject Alternate Name list.
A SQL login account will be created on the Adaptiva SQL Server. If the Adaptiva SQL Server is a remote server this will cause AdaptivaServerSetup to fail.

IMPORTANT: If the [TLS Settings](#) and the [Adaptiva Reporting Account](#) have never been set click on [Advanced Upgrade](#)

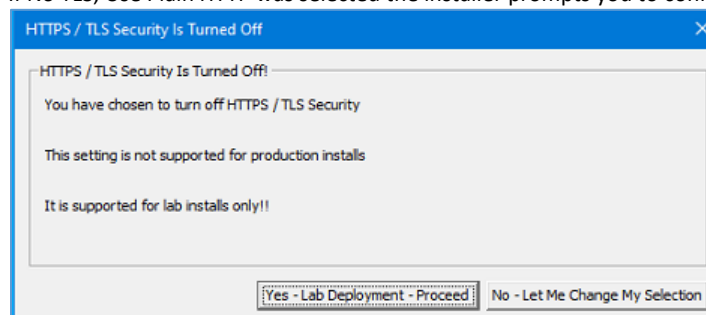
- Click on **Advanced Upgrade** to review each setting.

2. The following screen is used to provide the TLS Certificate configuration for use with the Admin Portal. Select which TLS Security Setting will be used to secure the Admin Portal



Select one of the following TLS security settings, based on the preferences of your organization. These settings allow secure access to the Adaptiva Admin Portal for devices with the certificate:

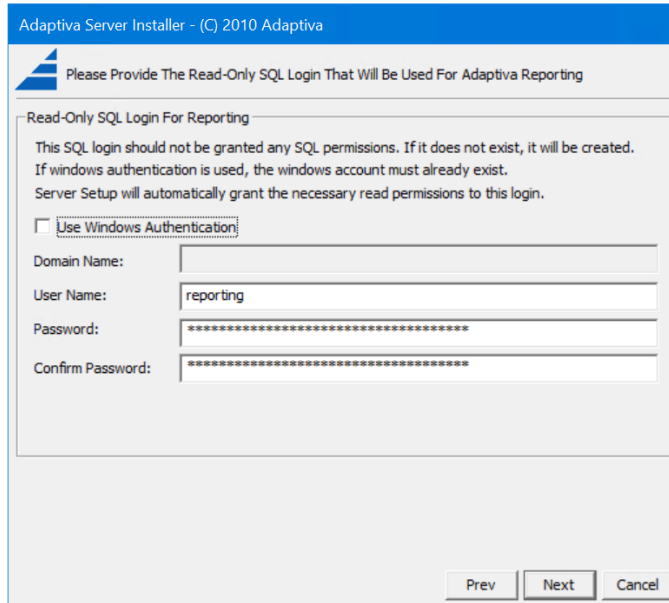
- Select **TLS Using A Certificate Authority (CA)** to use a certificate you exported from a Certificate Authority. If you choose this option, the CA-based certificate must be installed on the devices requiring access to the Adaptiva Admin portal. An auto-enrollment GPO can be configured and targeted to specific devices or a wild-card certificate can be used.
 - i. Click **Install A CA-Issued X.509 Certificate**.
 - ii. Click **Browse**, and then navigate to the location of the Certificate PEM File.
 - iii. Click **Browse**, and then navigate to the location of the Private Key PEM File.
- Select **TLS Using Self-signed Certificate** to use a self-signed certificate. If you choose this option, you must provide the certificate to every Adaptiva Administrator who must add it to the Certificate store on the device from which they access the Adaptiva Admin Portal. See Post-Install Instructions, Add Certificate to the Root Store
 - i. Click **Create A Self-signed X.509 Certificate**.
 - ii. Enter the **names or IP addresses** associated with the servers that host the Adaptiva Admin Portal. For example, include server details for NETBIOS, FQDN, DNS Alias or IP Address. Separate each entry by comma.
- Select **No TLS, Use Plain HTTP** if your organization does not require TLS to access the Adaptiva Admin Portal.
- Click **Next**
- If No TLS, Use Plain HTTP was selected the installer prompts you to confirm that this is a lab server.



- i. Click **Yes - Lab Deployment - Proceed**
 - ii. Click **No - Let Me Change My Selection** to return to the TLS Security Settings and try again.
3. The following screen is new. For more information, see the Installation Prerequisites section for the Database Reporting Account.

This account should be a NEW account. Do NOT use an existing account.

At the **Read-Only SQL Login for Reporting** screen, complete the fields as follows:



Use Windows Authentication – Check this if the reporting account has been created in the domain.

This box will be checked and greyed out when Windows Authentication mode has been specified in SQL Server.

Domain Name – Enter the NETBIOS domain name used for the reporting account.

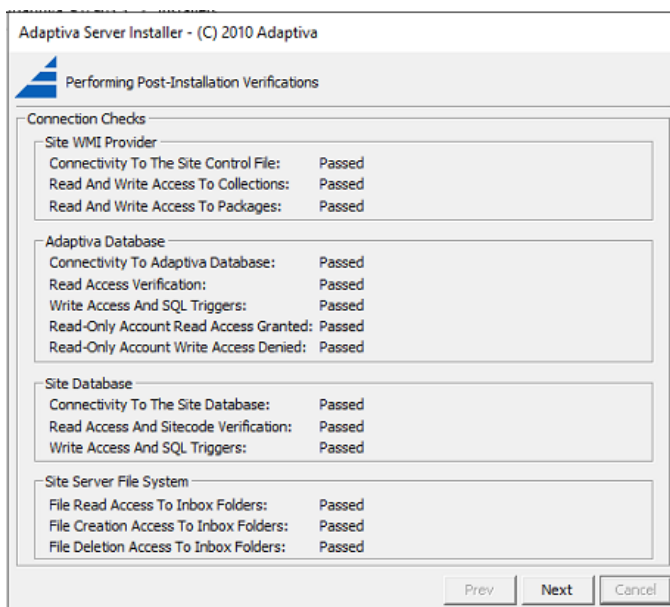
Leave blank if **Use Windows Authentication** is unchecked and a SQL Login account is to be used.

User Name – Enter the account name to use for the reporting account.

Password – Enter the password for the reporting account.

Confirm Password – Confirm the password that you entered above.

4. The completion screen has new entries.



Read-Only Account Read Access Granted will check if the Adaptiva Reporting account can read the Adaptiva database.

Read-Only Account Write Access Denied will check if the Adaptiva Reporting account can write to the Adaptiva database.

NOTE: Some of these will be skipped based on the integrations selected.

Also, there is a known issue when the Kerberos authentication protocol is selected for the Adaptiva database: The Read-Only Account Write Access Denied will report Failed. This can be ignored.

Add Certificate to the Root Store

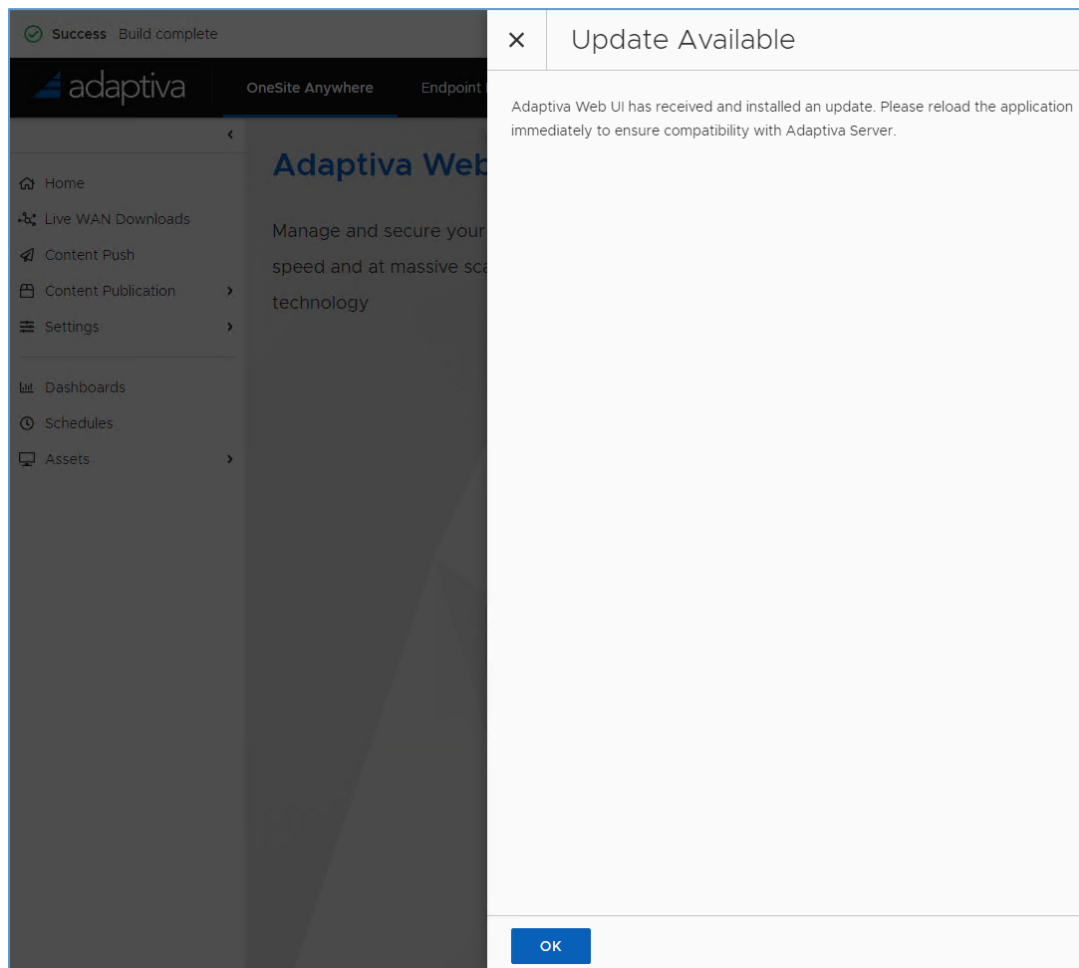
The Adaptiva Server will default to enabling TLS for the Admin Portal via a self-signed certificate. The self-signed certificate should be imported into the Trusted Root Certification Authorities container. Each Adaptiva Administrator who will use the Admin Portal from a remote device will need to import the certificate.

After the installation completes, run the following command at an Administrative Command Prompt:

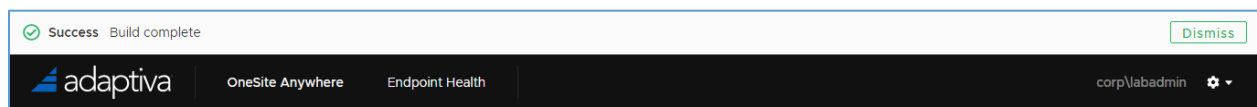
```
Certutil.exe -addstore root "%adaptivaserver%\data\security\webui\cert.pem"
```

Updated Admin Portal Build

When the Admin Portal build process completes you may see the following pop-out screen, click **OK**.



At the top of the windows, click on **Dismiss** for any notifications.



(Optional) Add New License Keys

OneSite Patch and its add-on License keys should only be added AFTER upgrading to a version of the OneSite Platform that supports that product. Contact Adaptiva Support if you have questions.

License keys can only be added in the Adaptiva Admin Portal.

Refer to the section above named **Installing the License Key**

(Optional) Publishing Content to the CDN

With build 8.0 and later, content can now be published to the Adaptiva CDN when you have add the OneSite ConfigMgr Edition license and activated your Adaptiva Server with the Adaptiva Cloud Relay Services.

Server Activation can also be completed when licensed for Autonomous Patch and Endpoint Health.

Refer to the section above named **(Optional) Post Installation Tasks**


Also, refer to **Configuring OneSite Anywhere** in the **Adaptiva OneSite User Guide**

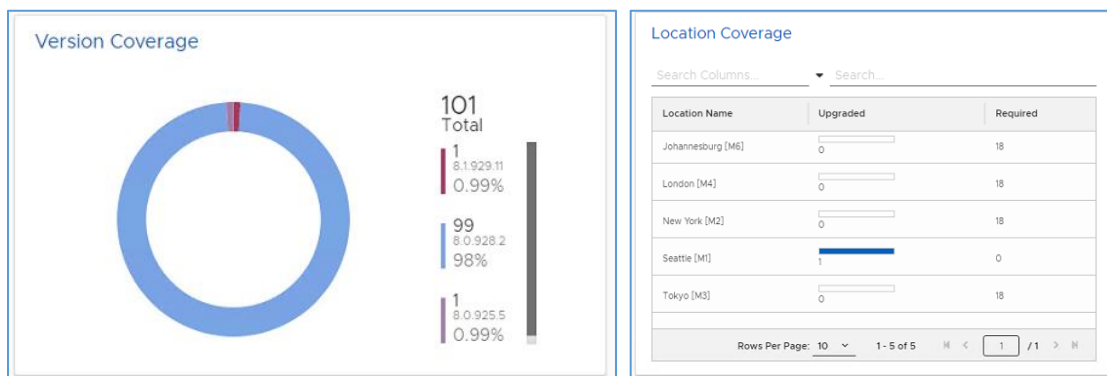
Client Upgrade

Automatic Installation

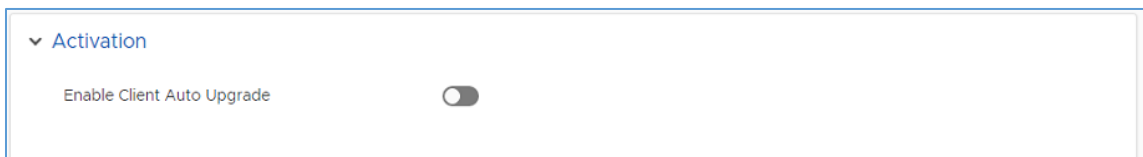
Before continuing, make sure the Adaptiva Server has been updated to the latest version of the Adaptiva Client. The Client installer will be obtained from the Adaptiva Server client install folder. This folder can be found by using the ADAPTIVACLIENT environment variable.

Using the Admin Portal

- ☐ Connect to the Admin Portal using a web browser (except Internet Explorer) – `http://AdaptivaServerFQDN[:port]`
- ☐ Enter the appropriate credentials or click on Login with Active Directory
- ☐ Click on , **Settings, Client Auto Upgrade** or **Dashboards, Client Auto Upgrade**
- ☐ At the top the dashboard will display the current coverage of the different versions in an overall chart and by location.



- ☐ The Client Auto Upgrade must be enabled before the settings can be changed. Once enabled, it will stay enabled.



▼ Activation

Enable Client Auto Upgrade ☐

If it is already enabled, the last saved configurations will be set in each section below. Update as required and click on **Save and Deploy**.


IMPORTANT: Clicking Save and Deploy, or Deploy, will immediately execute the workflow to perform the upgrade based on the settings in the form.

Toggle to the right to enable the sections below:

- **Scheduling**


▼ Schedule

Schedule Start Time

Choose Date 

Use Server Time Zone

☐

Click on  to open a calendar widget to select the date and time. Select the day and time the client upgrade should start.

May 2021

< >

S

M

T

W

T

F

S

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

☐ 24hr

01 : 40 PM

Clients that come online after the specified Start Time and have not yet received the policy will apply the policy immediately.

Click anywhere off the widget to close it. Notice the date and time has been entered into Schedule Start Time

Toggle **Use Server Time Zone** to have the specified start date and time refer to the time zone of the Adaptiva Server.

- **Target Groups**

▼ Target Groups

Use All Adaptiva Clients

☐

Target Groups

Add Groups [BROWSE](#)

Toggle **Use All Adaptiva Clients** or click on **Browse** to select one or more Adaptiva Groups or ConfigMgr collections. When selecting a Group or collection, check the box next to the item. When finished selecting all groups/collections, click on Add to List.

○ Load Balancing

▼ Load Balancing

Use Load Balancing

☒

Load Balance Over

24

Hours

▼

Toggle **Use Load Balancing** to enable load balancing. If not enabled, ALL targeted clients will execute the policy on the start date and time.

Set the Load Balance interval

The load balance interval can be between 0 and 100 Days, Hours or Minutes.

When Load Balancing is enabled, each client will be randomly divided across the load balance interval entered.

○ Installation

▼ Installation

Use Server FQDN ⓘ

☒

Use Server IP Address ⓘ

☐

Override Server FQDN ⓘ

☐

Enter Server Name

Use Cloud Relay ⓘ

☒

Bind to HTTP URL ⓘ

☐

Enter URL

No Add/Remove Programs Entry ⓘ

☐

No Firewall Entries ⓘ

☐

No WoL ⓘ

☐

Memory Allocation (in MB) ⓘ

256 ▼

CLI Input

AdaptivaClientSetup.exe -installOrUpgrade -servername ADAPTIVA.KAIBAB.FOREST.LAB -cloudrelay -mem 128 -delay 30

Choose either Server FQDN or IP Address. The Adaptiva Client can be installed using either the -servername or -serverip switches. This option determines which option is used. Notice the command line will change based on the options selected, e.g. The FQDN or IP address of the Adaptiva Server has been automatically entered.

IMPORTANT: Verify that automatic discovery found the correct Server Name or IP Address by reviewing the Command Line that was auto-generated.

To Override the FQDN or IP Address, toggle Override Server FQDN or IP Address and enter the Name or IP Address to use.

IMPORTANT: If the Name or IP Address previously used is changed, it will cause the client to be inactivated and re-activated, which will then trigger a review of all content in the AdaptivaCache folder as well as new policy downloads. If the FQDN or IP Address needs to be changed to support a DNS CNAME Alias see the

following article [here](#). [How-To: Redirect OneSite client to a different Adaptiva server – Adaptiva Support Portal](#)

Choose any of the below options:

- **Use Cloud Relay:** Allows the Adaptiva client to communicate with <http://services.adaptiva.cloud> when unable to communicate via UDP to the on-premises Adaptiva Server.

IMPORTANT: If any of the in-scope clients have been previously configured to use the Cloud Relay Service, be sure to enable this setting otherwise client communications will stop using the Adaptiva Cloud Relay server.

- **Bind to HTTP URL:** Allows the Adaptiva client to communicate with the on-premises Adaptiva Server via the defined HTTP Port. This adds the -serverurl <url> to the command line.
When the Bind to HTTP URL is enabled, enter the URL of the on-premises Adaptiva server. For example: <http://adaptivaserver.mydomain.com:9679>
- **No Add/Remove Programs Entry:** Enabling this setting will prevent Adaptive Client from being added to the Add & Remove Programs/Programs & Features list in Windows. Do not select this option if this information is required. Adds the -noarp switch to the command line.
- **No Firewall Entries:** Enabling this setting will prevent Windows Firewall entries from being created automatically. Adds the -nofirewall switch to the command line.
- **No WoL:** Enabling this setting will disable Wake on LAN. Do not select this option if it is desirable for machines to be woken using Wake on LAN magic packets in the event that content is available on the device, but the machine is offline. Adds the -nowol switch to the command line.
- **Memory Allocation (in MB):** This setting configures the maximum JVM memory allocation for the client. As of Adaptiva Client version 9.1, the default memory allocation is 512MB. Do not set this number below 512. It is recommended to set this value in powers of 2 starting at 512.

NOTE: The Memory value in the CLI Input shows the last value used and may differ from the Memory Allocation selection. Change the Memory Allocation to sync the CLI Input.


- ❑ Review the value of the Commandline to ensure that the servername | serverip is correct and that any required or desired command-line switches are present and displaying the correct values.

NOTE: Commandline will always contain the -delay 30 switch on the end. This cannot be overridden.

- ❑ Once the command-line has been validated, click **Save and Deploy** to start the upgrade process.

×

Confirm Settings

 Please confirm the commandline is correct. Incorrect commandline could cause the client to become orphaned.

Commandline

AdaptivaClientSetup.exe -installOrUpgrade -servername cmintune.puyallup.lab -mem 64 -delay 30

The command line must first be confirmed. Click **OK** after reviewing the Commandline.

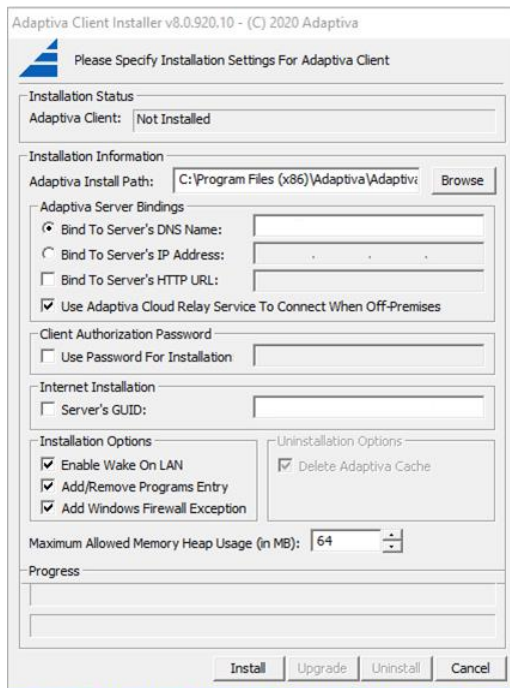
These settings are saved in the database in the table AUTOUPGRADESETTINGS. When Save is clicked, the latest Adaptiva Client will be published as Adaptiva Content, a hidden schedule, group and content push policy will be created.

When the specified start date/time is reached, the clients will download the content. The content will get unpacked into a local folder on the client %TEMP%\AdaptivaClientUpgrade (normally C:\Windows\TEMP).

To review distribution status, scroll back to the top or select Dashboards, Client Auto Upgrade Dashboard.

Manual Installation

The following screen is new with build 8.0 and later and is used to provide information on using the Cloud Relay Service.



Adaptiva Install Path – Directory where the Adaptiva client should be installed.

Adaptiva Server Bindings – Specify one of the following

- Adaptiva Server's DNS Name
- Adaptiva Server's IP Address

Adaptiva Server Bindings – Check the options as required

If the clients need to bind using HTTP, check the box: **Bind to Server's HTTP URL**

- Adaptiva Server's HTTP URL – Be sure to add the port that was used during server installation. E.g. <http://servername.adaptiva.com:9679>

If the clients will be on the internet, check the box: **Use Adaptiva Cloud Relay To Connect When Off-Premises**

For additional security check the following boxes:

- **Use Password for Installation** – Enter the password created in the Workbench
- **Server's GUID** – Enter the Adaptiva Server GUID. On the Adaptiva Server in `HKLM\Software\Adaptiva\server | client_data_manager.server_guid`
This option must be used when the client is on the internet

Enable Wake On LAN – Allows the client to be woken up using peer-to-peer WOL.

Add/Remove Programs Entry – Adds an entry allowing for uninstallation of the client agent from the Control Panel.

Add Windows Firewall Exception – Adds exceptions to the local Windows Firewall for the default client ports (see Table 11: Adaptiva Communication Ports for a list of these ports).

Maximum Allowed Memory Heap Usage – This is an internal performance optimization value. Changing this is not recommended unless recommended by Adaptiva Support.

Uninstallation

To completely remove Adaptiva OneSite from the environment or individual components, simply run the corresponding component's setup executable and select the Uninstall option. Uninstallation should be bottom-up starting with the clients, the workbench, and then the Adaptiva Server instances.

Adaptiva Client and Workbench

To run the uninstallation silently, run the corresponding installation executable with a -uninstall switch on the command-line for the Adaptiva Clients and Workbench installations.

For example:

```
AdaptivaClientSetup.exe -uninstall
```

```
AdaptivaWorkbenchSetup.exe -uninstall
```

Using the P2P Client MSI Installer

The P2P Client MSI Installer can also be used to perform a client uninstallation as described above.

For example:

```
Msiexec.exe /i AdaptivaClientP2PInstaller.msi /qn UNINSTALL=1
```

MacOS or Linux

The client_install.sh file used during installation is required. Locate the file on the device or copy to the device.

Open a command shell and run the following command:

```
sudo /<path>/client_install.sh uninstall
```

Adaptiva Server

Open a ticket with Adaptiva Support for assistance in removing the Adaptiva Server components. Uninstallation will delete the registry, content library and Adaptiva Server folder contents. It will delete the Adaptiva database and remove the Adaptiva tables, views and triggers from the ConfigMgr database.

OneSite Backup and Recovery

Overview

This section outlines the steps required to provide Disaster Recovery (DR) capabilities for Adaptiva OneSite. In general, just like installation and operation, Adaptiva OneSite is very straight-forward to backup and restore. Guidance and examples are given as appropriate but many of these tasks can be performed in a variety of ways based upon the environment where OneSite is installed. Review this entire document before implementing a solution.

Prerequisites (ConfigMgr)

Ensure there is a complete and successful backup of the ConfigMgr environment. Without this, OneSite can be restored and will function properly, but its main purpose to support, extend and supplement ConfigMgr, will not be satisfied.

The following Microsoft articles provide guidance on the backup and recovery for Configuration Manager.

Backup and Recovery for ConfigMgr Current Branch:

<https://docs.microsoft.com/en-us/sccm/core/servers/manage/backup-and-recovery>

Backup and Recovery for ConfigMgr 2012:

[https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg712697\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg712697(v=technet.10))

Scenarios

Scenario	Details
Disaster Recovery / Hardware Migration	Adaptiva Server is restored on a server with the same name, SQL server, instance name, and database name.
Adaptiva or ConfigMgr Database Migration	Adaptiva or ConfigMgr server name remains unchanged, but the SQL server name, instance name, (and/or) database name is changed.

Backup

To recover an Adaptiva OneSite instance and associated data, a successful backup must be completed. It is best practice to backup OneSite data to an alternate location, and not on the system hosting OneSite itself. The exact procedure for doing this is dependent on the backup solution(s) in use. Similar to ConfigMgr, the files and data could be copied to a specific folder and configure the backup solution to backup that location.

The following table describes the components on the Adaptiva Server which should be backed up.

Required	
Component	Details
Adaptiva SQL Database	Full SQL database backup.
Adaptiva Install Folder	<AdaptivaServerInstallPath>\AdaptivaServer
Adaptiva Driver	%systemroot%\system32\drivers\adaptivaservertransport*.sys
Adaptiva Server	HKLM\SOFTWARE\Adaptiva\server <i>Prior to version 5.5: HKLM\Software\javasoft\prefs\Adaptiva\server</i>

Registry Information	
Adaptiva Service Properties	Name: AdaptivaServer Description: The Adaptiva Server service. Provides server side support for Adaptiva products. DisplayName: AdaptivaServer Name: AdaptivaServer PathName: "<InstallPath>\Adaptiva\AdaptivaServer\bin\AdaptivaServerService.exe" ServiceType: Own Process StartName: LocalSystem Caption: AdaptivaServer
Optional	
Custom Adaptiva Reports in ConfigMgr Reporting Services Point	In the case where any custom reports were created that are not included as part of the Adaptiva Server installation, those report RDL files should be downloaded. If there are subscriptions or schedules for those reports, the Reporting Services database should be backed up.
Adaptiva Content Library	This is only applicable if the Content Library has been moved from the default location. The default location is: <InstallPath>\Adaptiva\AdaptivaServer\InstallPath>\AdaptivaServer\data\ContentLibrary If the above location is missing or there are no files within the ContentLibrary folder, check this registry key to determine if it has been moved. HKLM\Software\Adaptiva\adaptiva\server\contentsystem.lib_folder_path

Procedure and Sample Commands

The following steps and commands can be used to complete the required set of backup steps listed in the table above. Replace all sections in <> brackets with correct entries for the environment.

NOTE: The example command-lines referenced below assume the following:

The Adaptiva Server and SQL Server are installed on the same machine.

The Adaptiva database name is adaptiva.

The account used to execute these commands has sufficient privileges to perform these actions.

1. Stop the AdaptivaServer Service.

```
net stop AdaptivaServer
```

2. Setup some variable.

```
REM Setup some Variables
set SERVERNAME=ENTER DB SERVER NAME
set DATABASENAME=adaptiva
set BACKUPLOC=DRIVE:\Backup\ServerBackup
```

3. Backup Adaptiva SQL Server database.

```
REM Backup Adaptiva SQL Server database.
set DATESTAMP=%DATE:~-4%.%DATE:~7,2%.%DATE:~4,2%
set BACKUPFILENAME=%BACKUPLOC%\%DATABASENAME%-%DATESTAMP%.bak
```

```
REM May need to enter sqlcmd path. Default path to sqlcmd: C:\Program
Files\Microsoft SQL Server\Client SDK\ODBC\110\Tools\Binn\
REM Remove/Update Named Instance \ADAPTIVASQL
```

```
"[PATH TO\]sqlcmd" -E -S %SERVERNAME%\[ADAPTIVASQL] -d master -Q "BACKUP
DATABASE %DATABASENAME% TO DISK = N'%BACKUPFILENAME%'"
```

4. Backup Adaptiva Install Folder using a command prompt.

```
REM Backup Adaptiva Install Folder using a command prompt.
md %BACKUPLOC%\AdaptivaServer
xcopy.exe "%ADAPTIVASERVER%" %BACKUPLOC%\AdaptivaServer /v /e /r /k /h /o /x
/y
```

5. Backup the Adaptive Protocol Driver using a command prompt.

```
REM Backup the Adaptive Protocol Driver using a command prompt.
md %BACKUPLOC%\AdaptivaDriver
xcopy.exe %systemroot%\system32\drivers\adaptivaservertransport*.sys
%BACKUPLOC%\AdaptivaDriver /v /e /r /k /h /o /x /y
```

6. Backup the Adaptiva Server and driver registry keys.

```
REM Backup the Adaptiva Server and driver registry keys.
REM --Version 5.5 and up
reg.exe export HKLM\SOFTWARE\Adaptiva\server %BACKUPLOC%\AdaptivaServer.reg /y
reg.exe export HKLM\SYSTEM\CurrentControlSet\services\AdaptiveProtocolServer
%BACKUPLOC%\AdaptivaDriver.reg /y

REM --Adaptiva Versions prior to 5.5
REM reg.exe export HKLM\SOFTWARE\javasoft\prefs\Adaptiva\server
%BACKUPLOC%\AdaptivaServer.reg /y
```

7. Backup the Adaptiva Content Library folder if it has been moved to a non-default location.

```
REM Backup the Adaptiva Content Library folder if it has been moved to a non-
default location.
REM Remove the REM and enter the Content Library Location if it was moved from
the default location
REM xcopy.exe <ContentLibraryLocation> %BACKUPLOC%\ContentLibrary /v /e /r /k
/h /o /x /y
```

8. Record the configuration information for the AdaptivaServer service.

```
REM Record the configuration information for the AdaptivaServer service.
wmic service where caption='AdaptivaServer' get caption, Description,
DisplayName, Name, PathName, ServiceType, StartName /VALUE >
%BACKUPLOC%\AdativaServerServiceInfo.txt
```

9. Restart the AdaptivaServer service.

```
REM Restart the AdaptivaServer service.
REM DO NOT RESTART if moving Adaptiva to a new server
net start AdaptivaServer
```

The above commands can easily be customized for any environment and combined into a single batch file for scheduled execution. Using the built-in capabilities of ConfigMgr backup, these commands can be automatically triggered by ConfigMgr itself after the ConfigMgr Backup maintenance task runs. To do this, simply insert the customized form of the above commands into a batch file called AfterBackup.bat and place the batch file in the <ConfigMgrInstallPath>\inboxes\smsbkup.box folder. More details on this feature of ConfigMgr can be found at <https://docs.microsoft.com/en-us/configmgr/core/servers/manage/backup-and-recovery#using-the-afterbackupbat-file>.

Restore

The following list of tasks outlines what must be done to restore OneSite. These tasks, similar to restoring ConfigMgr itself, assume a system with the same machine name, domain status, and drive letters as the original system and also depend on the complete and successful backup of a previously working OneSite installation using the steps outlined above. They also assume the existence of the files created by the backup tasks above.

Procedure and Sample Commands

Command-line examples are also given similar to those above in the Backup section; however, with restoration, these are typically not automated and thus using the Windows GUI to perform these processes may be easier.

1. Setup some variable.

```
REM Setup some Variables
set SERVERNAME=ENTER DB SERVER NAME
set DATABASENAME=adaptiva
set BACKUPLOC=DRIVE:\Backup\ServerBackup
set ADAPTIVASERVER=<path to AdaptivaServer i.e. d:\program
files\adaptiva\adaptivaserver>
```

1. Restore the Adaptiva SQL Server DB.

```
REM Restore the Adaptiva SQL Server DB.
set BACKUPFILENAME=%BACKUPLOC%\adaptiva-yyyy.mm.dd.bak
set BACKUPLOC=c:\users\adaadmin\downloads\ServerBackup\ServerBackup
REM Default path to sqlcmd: C:\Program Files\Microsoft SQL Server\Client
SDK\ODBC\110\Tools\Binn\
REM Remove/Update Named Instance \ADAPTIVASQL
"[PATH TO\]sqlcmd" -E -S %SERVERNAME%\[ADAPTIVASQL] -d master -Q "RESTORE
DATABASE [%DATABASENAME%] FROM DISK = '%BACKUPFILENAME%'"
```

2. Restore the Adaptiva Server registry key.

```
REM Restore the Adaptiva Server registry key.
reg.exe import %BACKUPLOC%\AdaptivaServer.reg
```

3. Restore the Adaptiva Server installation folder and Adaptive Protocol Driver file.

```
REM Restore the Adaptiva Server installation folder and Adaptive Protocol
Driver file.
xcopy.exe %BACKUPLOC%\AdaptivaServer "%ADAPTIVASERVER%" /v /e /r /k /h /o /x
/y
xcopy.exe %BACKUPLOC%\AdaptivaDriver %systemroot%\system32\drivers /v /e /r /k
/h /o /x /y
```

4. If the ContentLibrary folder had been moved to a non-default location, then it must also be restored.

```
REM If the ContentLibrary folder had been moved to a non-default location,
then it must also be restored.
REM Remove the REM and enter the Content Library Location if it was moved from
the default location
REM xcopy.exe %BACKUPLOC%\ContentLibrary <ContentLibraryLocation> /v /e /r /k
/h /o /x /y
```

5. Create the AdaptivaServer service using the service information recorded in AdaptivaServiceInfo.txt.

```
REM Create the AdaptivaServer service using the service information recorded
in AdaptivaServiceInfo.txt.
sc create AdaptivaServer type=own start=auto DisplayName=AdaptivaServer
binPath="%ADAPTIVASERVER%\bin\AdaptivaServerService.exe"
```

6. Restore the Adaptive Protocol Driver registry information.

```
REM Restore the Adaptive Protocol Driver registry information.
reg.exe import %BACKUPLOC%\AdaptivaDriver.reg
```

7. Create the AdaptiveProtocolServer service.

```
REM Create the AdaptiveProtocolServer service.
sc create AdaptiveProtocolServer binPath=%systemroot%\system32\drivers
type=kernel start=demand DisplayName=AdaptiveProtocolServer
```

8. If the Restore process was run on a different server with a different server name review the **Database Restoration Scenarios** below
9. At this point, in the process, the Adaptiva Server should be able to function, but in case there was something missed, the same version of **AdaptivaServerSetup.exe** as the restored Adaptiva Server should be run. When navigating through the installation wizard, no values should need to be modified as it will use the previous configuration as what is in the registry. See **Running Setup** below.

IMPORTANT: If the Adaptiva database was moved to a database server different from the CM database, be sure to follow the steps in Appendix B before running AdaptivaServerSetup. Select Kerberos when prompted by AdaptivaServerSetup.

Database Restoration Scenarios

If the Adaptiva or ConfigMgr databases need to be moved or restored to another SQL server, the Adaptiva Server Installer will allow for modifications of the SQL Server Machine Name, SQL encryption settings, and SQL Login information. If making changes to the Adaptiva / ConfigMgr database names, instance names, or ports, use the following table to modify the appropriate registry values before running **AdaptivaServerSetup.exe**.

Component	Registry Value
Registry Location:	
5.5 and Above: HKLM\Software\Adaptiva\server	
Prior to 5.5: HKLM\Software\javasoft\prefs\Adaptiva\server	
Adaptiva Database Machine Name	setup.adaptiva_db_machine_name
Adaptiva Database Name	setup.adaptiva_db_name
Adaptiva Database SQL Port	setup.adaptiva_db_port
Adaptiva Database SQL Instance	setup.adaptiva_db_sql_named_instance
Adaptiva Server name	setup.customer_name
ConfigMgr Database Machine Name	setup.site_db_machine_name
ConfigMgr Database Name	setup.site_db_name
ConfigMgr Database SQL Port	setup.db_port
ConfigMgr Database SQL Instance	setup.site_db_sql_named_instance
ConfigMgr Site Server Name	setup.site_server_machine_name

Running Setup

1. Run **AdaptivaServerSetup.exe** and at the **License Agreement** screen, click **Accept**.
2. At the **Status** screen, the Adaptiva configuration will be listed which includes the Adaptiva Server version, installation folder, Adaptiva database server, database name, etc. Click **Upgrade** to start.
3. In the installer fields for the ConfigMgr server and database server can be changed/updated, but if the Adaptiva database names, instances, or ports were modified, they should be modified in the registry before running setup.
4. Once complete, verify the AdaptivaServer service started correctly by reviewing adaptiva.log in the **<AdaptivaServerInstallPath>\AdaptivaServer\logs** folder for errors or anomalies.
5. Reinstall the Adaptiva Client when prompted.

6. Reinstall the Adaptiva Workbench from the installation source (if desired). Ensure the same version of the workbench is being used as that of the AdaptivaServer that was just restored.

Reporting

If the Adaptiva database was moved to a different SQL Server be sure to update the database connection in SQL Server Reporting Services for the ConfigMgr Reports

1. Browse to `http://<ReportingServer>/ConfigMgr_<sitecode>/reports`
2. Scroll to the bottom of the list and click on Adaptiva
3. Change the connection string to:
4. `Datasource=new adaptivaserver fqdn;initial catalog=adaptiva`
5. It should be using specific Credentials – the CM Reporting Services Point account. Make sure this account has db_datareader permissions on the Adaptiva database on the new server

Appendix A: Communication Ports

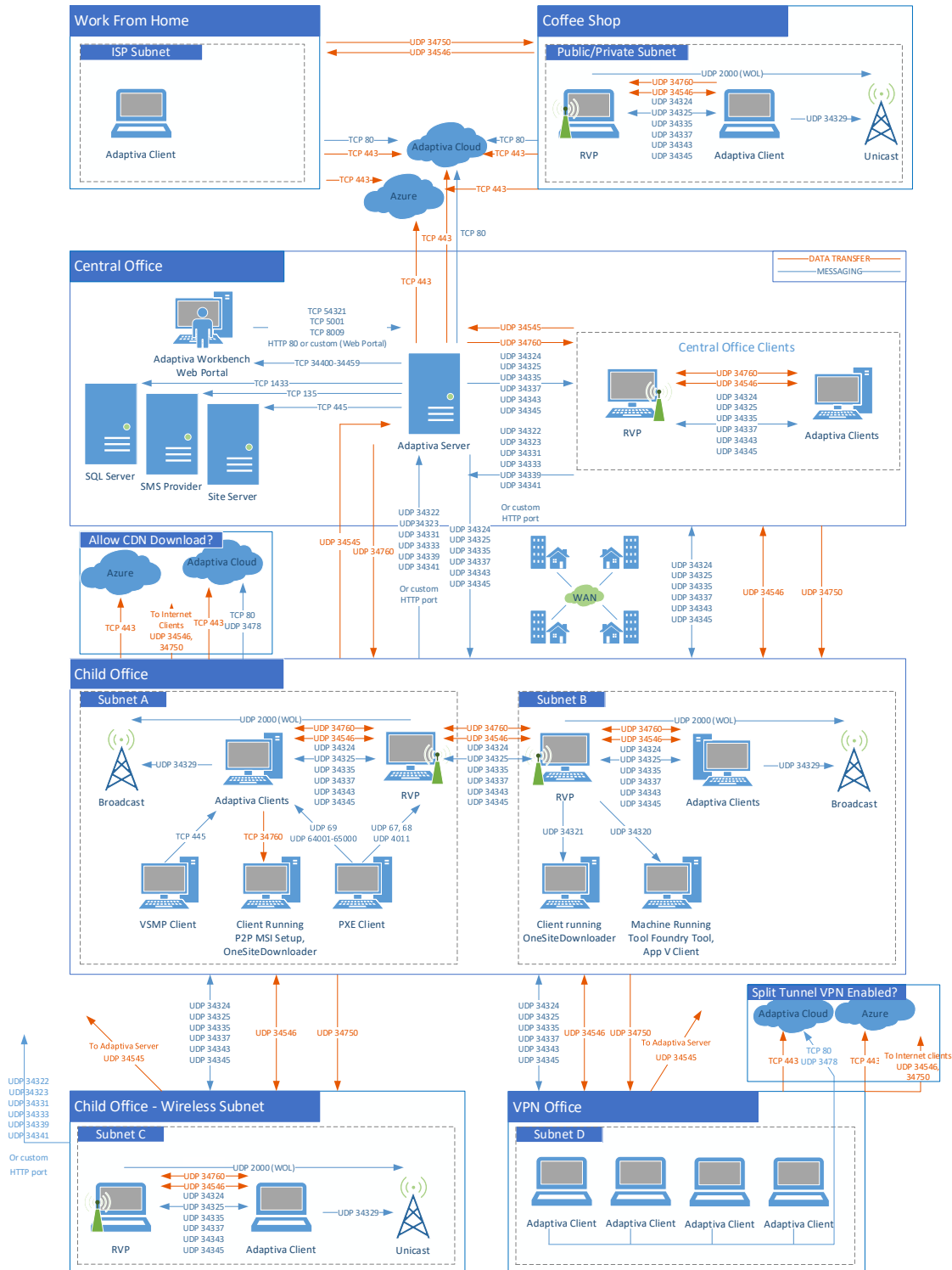
List of All Adaptiva Ports

Refer to the online documentation to download the PDF [here](#).

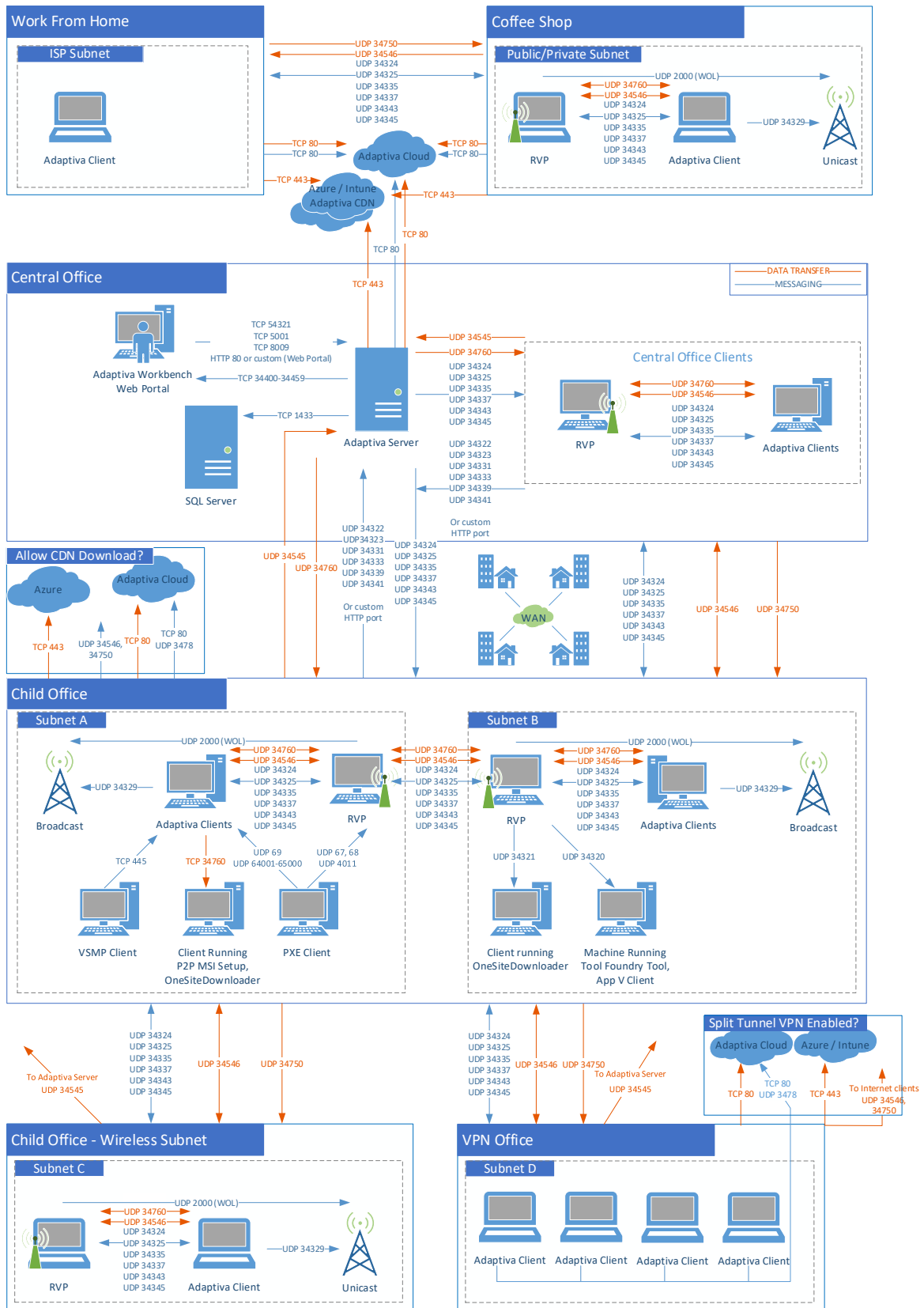
Communication Port and Flow Diagrams

These are also available [here](#).

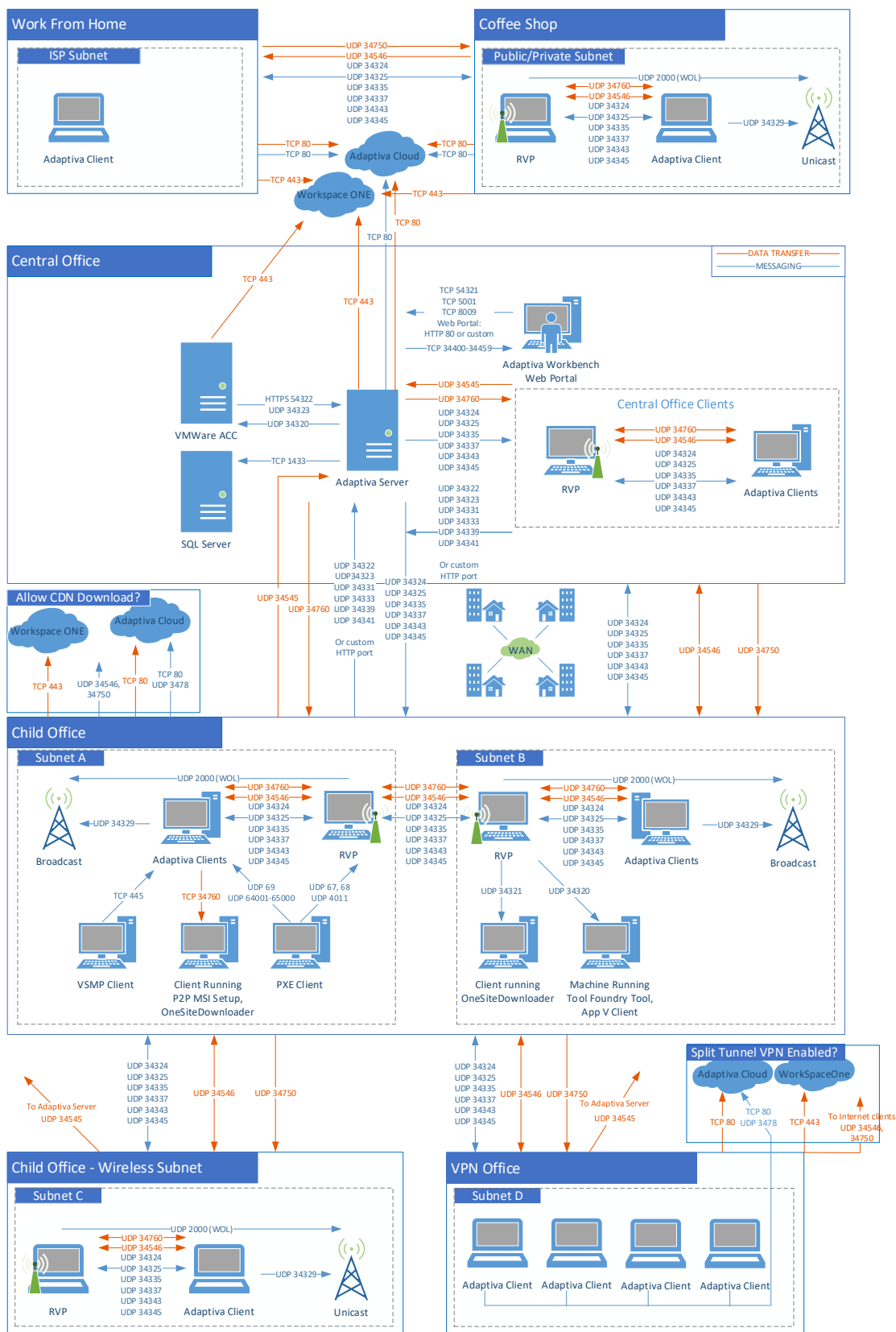
Microsoft EndPoint Manager – Configuration Manager



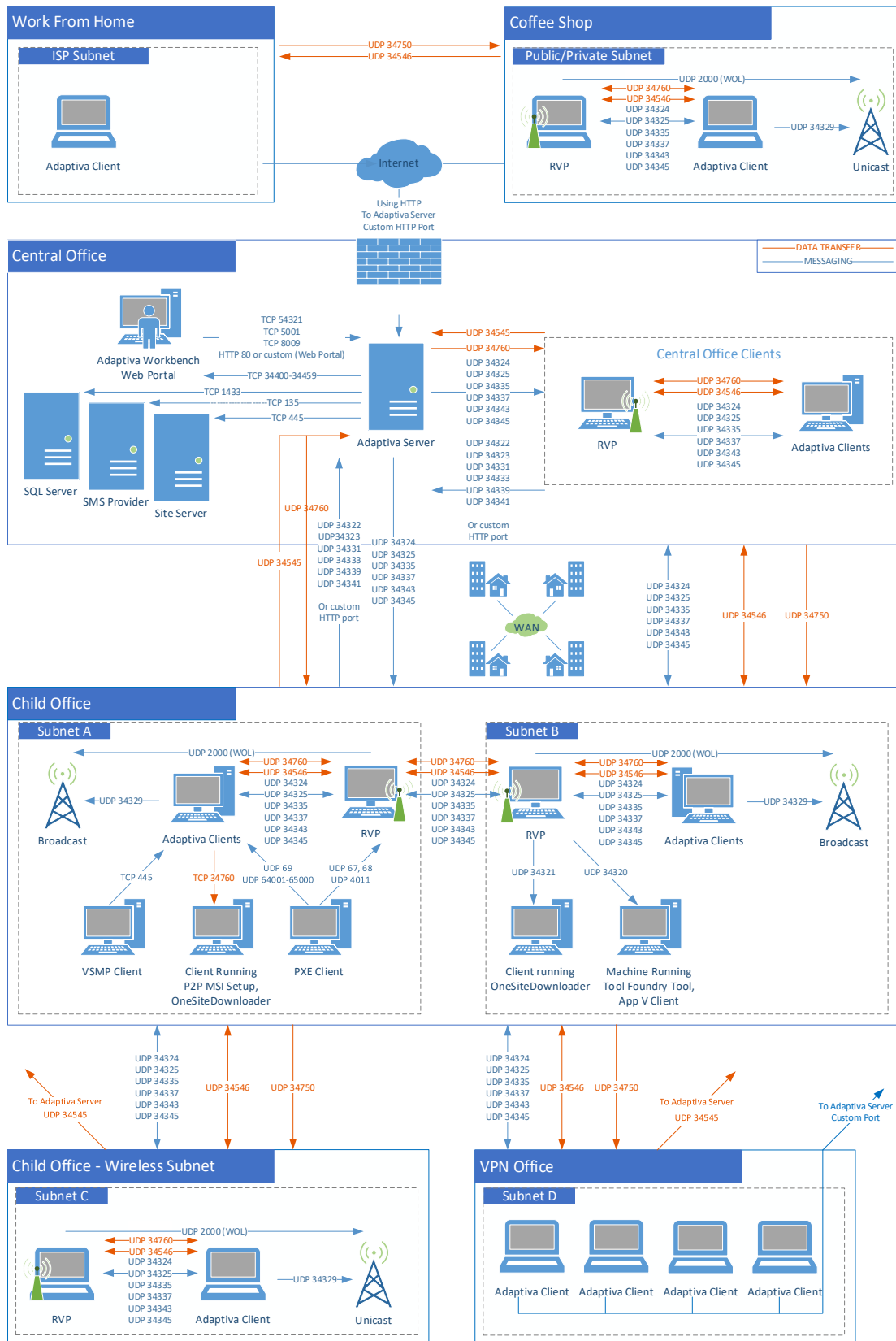
Microsoft Endpoint Manager - Intune



Workspace ONE



ConfigMgr with Custom Port Messaging (No Cloud Relay)



Additional Firewall Rules

Adaptiva Server Firewall Rule NETSH Commands

```
netsh advfirewall firewall add rule name = "Adaptiva Server - 1" action=allow dir=in enable=yes
profile=domain localport=34545 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Server - 2" action=allow dir=in enable=yes
profile=domain localport=34339 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Server - 3" action=allow dir=in enable=yes
profile=domain localport=34341 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Server - 4" action=allow dir=in enable=yes
profile=domain localport=34331 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Server - 5" action=allow dir=in enable=yes
profile=domain localport=34333 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Server Service" action=allow dir=in enable=yes
profile=domain protocol=any edge=no
program=<AdaptivaServerInstallPath>\AdaptivaServer\bin\AdaptivaServerService.exe
```

Adaptiva Client Firewall Rule NETSH Commands

Sometimes client VPN solutions or corporate Wi-Fi networks may show as Public or Private profile; therefore, it is often best to add the rule to all profiles for clients. To do this change the **profile=domain** values for each line to **profile=domain,private,public**

```
netsh advfirewall firewall add rule name = "Adaptiva Client Service" action=allow dir=in enable=yes
profile=domain,private,public protocol=any edge=no
program="<path>\Adaptiva\AdaptivaClient\bin\AdaptivaClientService.exe"

netsh advfirewall firewall add rule name = "Adaptiva Client" action=allow dir=in enable=yes
profile=domain,private,public localport=34760,34750,34546,34335,34337,34343,34345 protocol=udp edge=no
```

The following rules are deprecated:

```
netsh advfirewall firewall add rule name = "Adaptiva Client - 1" action=allow dir=in enable=yes
profile=domain localport=34760 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Client - 2" action=allow dir=in enable=yes
profile=domain localport=34750 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Client - 3" action=allow dir=in enable=yes
profile=domain localport=34546 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Client - 4" action=allow dir=in enable=yes
profile=domain localport=34335 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Client - 5" action=allow dir=in enable=yes
profile=domain localport=34337 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Client - 6" action=allow dir=in enable=yes
profile=domain localport=34343 protocol=udp edge=no
netsh advfirewall firewall add rule name = "Adaptiva Client - 7" action=allow dir=in enable=yes
profile=domain localport=34345 protocol=udp edge=no

netsh advfirewall firewall add rule name = "Adaptiva Client Service" action=allow dir=in enable=yes
profile=domain protocol=tcp edge=no program=<path>\AdaptivaClient\bin\AdaptivaClientService.exe
netsh advfirewall firewall add rule name = "Adaptiva Client Service" action=allow dir=in enable=yes
profile=domain protocol=udp edge=no program=<path>\AdaptivaClient\bin\AdaptivaClientService.exe
```

Adaptiva Workbench Firewall Rule NETSH Commands

```
netsh advfirewall firewall add rule name = "Adaptiva Workbench" action=allow dir=in enable=yes
profile=domain protocol=udp edge=no
program=<AdaptivaServerInstallPath>\AdaptivaWorkbench\AdaptivaWorkbench.exe
netsh advfirewall firewall add rule name = "Adaptiva Workbench" action=allow dir=in enable=yes
profile=domain protocol=tcp edge=no
program=<AdaptivaServerInstallPath>\AdaptivaWorkbench\AdaptivaWorkbench.exe
```

Adaptiva Server to ACC Firewall Rule NETSH Commands

This should be run on the Adaptiva Server when outbound rules are restricted

```
netsh advfirewall firewall add rule name = "Adaptiva to ACC" action=allow dir=out enable=yes  
profile=domain protocol=udp remoteport=34320 edge=no [remoteip=<ACC IP Address>]
```

This should be run on the Adaptiva Server when inbound rules are restricted

```
netsh advfirewall firewall add rule name = "ACC to Adaptiva UDP" action=allow dir=in enable=yes  
profile=domain protocol=udp localport=34323 edge=no [remoteip=<ACC IP Address>]  
netsh advfirewall firewall add rule name = "ACC to Adaptiva HTTPS" action=allow dir=in enable=yes  
profile=domain protocol=tcp localport=54322 edge=no [remoteip=<ACC IP Address>]
```

ACC to Adaptiva Server Firewall Rule NETSH Commands

This should be run on the ACC Server when inbound rules are restricted. The range 192.30.64.0-192.30.79.255 are public IP Addresses for AirWatch servers.

```
netsh advfirewall firewall add rule name = "Adaptiva to ACC" action=allow dir=in enable=yes profile=domain  
protocol=udp localport=34320 edge=no [remoteip=<Adaptiva IP Address>]  
netsh advfirewall firewall add rule name = "Airwatch" action=allow dir=in enable=yes profile=domain  
protocol=tcp localport=443 edge=no [remoteip=192.30.64.0-192.30.79.255]
```

This should be run on the ACC Server when outbound rules are restricted

```
netsh advfirewall firewall add rule name = "ACC to Adaptiva UDP" action=allow dir=out enable=yes  
profile=domain protocol=udp remoteport=34323 edge=no [remoteip=<Adaptiva IP Address>]  
netsh advfirewall firewall add rule name = "ACC to Adaptiva HTTPS" action=allow dir=out enable=yes  
profile=domain protocol=tcp remoteport=54322 edge=no [remoteip=<Adaptiva IP Address>]  
netsh advfirewall firewall add rule name = "Airwatch" action=allow dir=out enable=yes profile=domain  
protocol=tcp remoteport=443 edge=no [remoteip=192.30.64.0-192.30.79.255]
```

Appendix B: SPNs and Delegation

With more companies moving to dedicated SQL Servers or SQL Always On Availability Groups, this section is intended to help get the SPNs (Service Principle Name) configured and Kerberos delegations set up. The guidelines in this article are also helpful: <http://support.microsoft.com/kb/2443457>.

Create the SPNs

It is recommended to use the Kerberos Configuration Manager utility. This can be downloaded from [here](#).

NOTE: This utility may not work if the SQL Server is in a different domain than the SQL Service accounts or if there are many groups added to the local Administrators group.

- ☐ Log into the SQL Database server using an account in the local Administrators group
- ☐ Optionally, but recommended, install the Kerberos Configuration Manager utility
- ☐ Use the following steps in the Kerberos Configuration Manager
 - ☐ Navigate to C:\Program Files\Microsoft\Kerberos Configuration Manager for SQL Server and launch **KerberosConfigMgr.exe**
 - ☐ Click **Connect** from the menu and then click **Connect** without entering any info
 - ☐ Select the **SPN** tab
 - ☐ Scroll all the way to the right and notice the Required SPN and Status columns

NOTE: These next steps must be done with a Domain Admin account. They do not have to be executed on the database server.

- ☐ If able to modify the service accounts, click on **Fix All** (or do them individually) otherwise, click **Generate All**, enter a file name and provide that script to an administrator with the appropriate permissions.
- ☐ After the fix script(s) has been run, to confirm the SPNs have been created successfully, click on **Refresh**. Scroll to the right to confirm the status is **Good** for all rows
- ☐ Use the following steps when not using Kerberos Configuration Manager
 - ☐ Open an administrator command prompt and type:


```
Setspn -l <domain>\<serviceaccount>
```
 - ☐ For example, executing this command will return the following:


```
C:\Users\administrator>setspn -l <domain>\sqlservice
Registered ServicePrincipalNames for
CN=SQLService,OU=Accounts,DC=<DOMAIN>,DC=lab:
MSSQLSvc/SQLSERVER.<DOMAIN>.lab:1433
MSSQLSvc/SQLSERVER.<DOMAIN>.lab
```

NOTE: These next steps must be done with a Domain Admin account. They do not have to be executed on the database server.

- ☐ Create the SPNs:


```
Setspn -S MSSQLSvc/<NetBiosName> <domain>\<serviceaccount>
Setspn -S MSSQLSvc/<FQDN> <domain>\<serviceaccount>
Setspn -S MSSQLSvc/<FQDN>:<port> <domain>\<serviceaccount>
```
- ☐ Rerun the following command and confirm the SPNs exist correctly:


```
Setspn -l <domain>\<serviceaccount>
```
- ☐ If using with SQL Always On Availability Groups, then repeat the above steps on database server #2. This should ALSO be done with the AG Listener.

- ❑ After the SPNs have been setup, open Active Directory Users and Computers. Find the service account, select **Properties** and select the **Attribute Editor** tab. Find the servicePrincipalName property and open it. Confirm the SPNs are listed for the server(s) for both with and without the FQDN with port numbers.

Delegate Kerberos authentication

Because the SQL Server is on a different server than the Adaptiva Server it is required to setup Kerberos trust delegation. The following steps cannot be done if the SPNs have not been setup correctly.

NOTE: These next steps must be done with a Domain Admin account.

- ❑ Open **Active Directory Users and Computers**
- ❑ Find the SQL Service account used and select **Properties**
- ❑ Select the **Delegation** tab.

NOTE: If SPNs have not been setup correctly, then this tab will not be available

- ❑ Select **Trust this user for delegation to specified services only** and select **Use Kerberos only**
- ❑ Click on **Add...**
- ❑ Click on **Users or Computers...**
- ❑ Enter the Service account name and click **Check Names, OK**
- ❑ In the list of Available services, select all the entries with MSSQLSvc for the SQL Database server as appropriate and click **OK**
- ❑ Click OK to close the Properties box
- ❑ Log on to the SQL Server(s) and using SQL Server Configuration Manager, restart the SQL Server service (or Restart the server)

Confirm the Configuration

Once the SPNs and the Kerberos delegations have been configured, use SQL Management Studio to confirm the connection properties.

Kerberos Configuration Manager can also be used: Click on the Delegation tab to confirm the delegations have been setup correctly: The details will state: No obvious delegation issues.

- ❑ Log onto a server Different than SQL database server, but that has SQL Management Studio installed.
- ❑ Connect to the remote SQL Database server (Connect, Database Engine, enter the server name)
- ❑ Open a New Query Window on the remote database server and Execute the following query:

```
select auth_scheme from sys.dm_exec_connections where session_id=@@spid
```
- ❑ The result back should be Kerberos

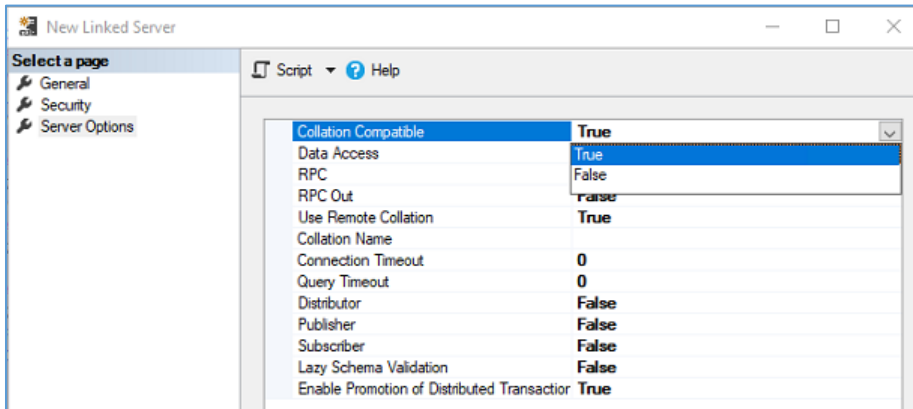
Create the Linked Servers

When the Adaptiva database is on a different SQL Server than the ConfigMgr database, the Linked Servers must be manually created.

- ❑ In **SQL Management Studio** with a connection to the ConfigMgr SQL database server, expand **Server Objects, Linked Servers**
- ❑ Right-click on **Linked Servers** and enter the following:
Linked server: <AdaptivaSQLServerFQDN>
Select **SQL Server**
- ❑ On the **Security** page, select **Be made using the login's current security context**.

IMPORTANT: The account used must not have the setting enabled. Account is sensitive and cannot be delegated.

- ❑ On the **Server Options** page, set the **Collation Compatible** field to **True**.



- ❑ Click **OK**
- ❑ If SQL Always On Availability Groups are being used, repeat the above steps connected to database server #2 and connected to the Availability Group Listener.
- ❑ Now repeat the above steps connecting to the Adaptiva SQL database server and creating a Linked Server to the ConfigMgr SQL Server FQDN.

Test the Linked Servers

It is important to confirm the linked servers are able to access the data on the other server.

- ❑ In SQL Server Management Studio, expand Server Objects, Linked Servers, FQDN of the other server, catalogs
- ❑ Notice the list of databases returned from the other server
- ❑ Expand the appropriate database and confirm that tables and views can be seen.

Appendix C: Optional Configuration Activities

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	How-to: Enable UDP v2 Large Messaging – Adaptiva Support Portal
Using Content Push to Offices with multiple subnets	How-To: Optimize "All Clients" targeted IntelliStage Content Push Policies – Adaptiva Support Portal
Exporting and Importing the Adaptiva Network Topology – Rename those Auto Created Offices	Exporting and Importing the Adaptiva Network Topology – Adaptiva Support Portal
Operating System Deployments: After installing the Adaptiva client, wait for the Adaptiva license to be applied.	Task Sequence - Wait for Adaptiva Client to get an ID – Adaptiva Support Portal
Operating System Deployments: Using the PXE Approval Workflow to ensure the correct boot image is used.	How-To: Define a Preferred Boot Image for PXE – Adaptiva Support Portal
Operating System Deployments: Getting the boot image faster by increasing the block size.	How-To: Set the Boot Image TFTP Block Size – Adaptiva Support Portal
Content Push Policy optimization techniques	How-To: Optimize "All Clients" targeted IntelliStage Content Push Policies – Adaptiva Support Portal
Perform administrative functions and test on remote machines. For example, Get logs, Check PXE, Get the RVP, Restart the Client, etc.	Administration: Adaptiva Administration Tool (AAT) – Adaptiva Support Portal
Clients not communicating with the server? Use the UDPPortChecker tool to determine which port or ports is blocked.	How-To: Check that the required ports for Adaptiva are open? – Adaptiva Support Portal
Create a Custom Security Role	How-To: Create a Custom Security Role with Limited Set of Perspectives – Adaptiva Support Portal
Viewing Adaptiva Status Messages in the ConfigMgr console	How-To: View Adaptiva Status Message Descriptions – Adaptiva Support Portal