

Table of contents

AppVentiX Quick Start	2
Deploy, Update and Remove applications with AppVentiX	9
AppVentiX Components	
AppVentiX Agent Service	
AppVentiX Agent GUI	
AppVentiX Central View Console	
Machine Groups	
Machine Group Agent Settings	15
Manage Machines page	22
Manage Content page	23
MSIX and MSIX app attach	28
MSIX Shared containers	29
MSIX Certificate management and deployment	
Application overview	
FSlogix App Masking management	
Configuration and Activity page	
Firewall \ communication ports used by AppVentiX	
Limit access to the Central View console	
Azure Virtual Desktop (AVD) integration	
Azure AD (Entra ID) integration	
Azure file share configuration	
Advanced configurations	44
Share permissions and share configuration	44
Central View inventory	46
Central View advanced settings	46
Supported operating systems	47
Upgrade from App-V Scheduler	48
Upgrade from earlier version of AppVentiX	48
FSLogix and roaming profile settings	48
Automated image building and deployment actions	50
Image build events	50
Run the refresh cycle from the command line	51
When Central View console takes longer to start	
Example configurations of the AppVentiX Agent	52

AppVentiX Quick Start

AppVentiX works with a lightweight agent running on the same machine as the App-V and MSIX (app attach) client (part of Windows). This can either be a virtual machine (Microsoft RDS\AVD Hostpool\Windows365, Citrix VDI (PVS\MCS), VMware Horizon, etc) or physical machine (PC or Laptop). The agent can be pushed from the Central View console or easily installed silently, the silent install parameter is already populated in the Central View console and you only have to copy\paste the command from there.

The Central View console can be installed on any management machine and does not need any (SQL) back-end. AppVentiX only requires a file share, a lot of file share types are supported and proven to work with AppVentiX, to name some examples: Windows file shares (direct or DFS), Azure file shares (domain integrated and stand-alone), Nutanix and NetApp file shares. The Central View console requires a 64Bit OS (Server OS or Desktop OS). Both Server OS, Multi-session OS and Single-session OS are supported by AppVentiX. The AppVentiX solution is easy to implement and will give you complete control and insight in under 10 minutes.

The quick start steps will begin on the next page.

The following steps will help you to get up and running quickly:

Step 1

Create a new file share or use an existing one, this share will be used to store the central configuration. You can use a normal Windows file share or a DFS share to make the share high available (for example <u>\yourdomain.local\appventix\config</u>). Also Azure file shares (domain integrated or stand-alone) and shares on storage vendors like Nutanix\NetApp\Dell\HP file shares are supported.

The required share permissions can be found in the Central View console in the settings window, a screenshot is added below. Basically you can choose to use **integrated authentication** or provide a **(service) account**.

indows file share, Storage vendor file share or Azure file share that is Active Directory integrated	
ntegrated Authentication	
Vith integrated authentication the Central View console will access the share(s) with the currently logged in user. Vith integrated authentication the Agent will access the share(s) with the computer account.	
hare permissions needed for this option: User group performing management in Central View: Read\Write permissions on configurations share and content share(s) Domain Computers group (or group containing the machine accounts): Read permissions on configuration share and content sh Domain Computers group (or group containing the machine accounts): Read\Write permissions in inventory folder on configura	are(s) ion share
onfigured account (service account)	
When an account is configured in the Central View console, the account will be used to access the share(s). When an account is configured in the Agent the account will be used to access the share(s).	
Share permissions needed for this option: - Configured account in Central View: Read\write permissions on configuration share and content share(s) - Configured account in the Agent: Read permissions on configuration share and content share(s) - Configured account in the Agent: Read\Write permissions in inventory folder on configuration share	
Fip: You can silently install the agent to use the same account. The silent install parameter can be found in the Central View console (agent ribbon).	
zure file share which is Kerberos integrated, AD integrated or Stand-alone	
onfigured account (service account)	
Configure the account as follows:	
From the Azure portal copy the storageaccount name and the access key In Central View uncheck the integrated authentication checkbox and provide the following details:	

Tip: You can silently install the agent to use the same account. The silent install parameter can be found in the Central View console (agent ribbon).

For integrated authentication (default), you can configure the below permissions:

- Domain computers group read permissions on the share
- Domain computers group read/write permissions on inventory folder on the share (this folder is automatically created)
- Central View Admins (a group with users that performs the management) read\write permissions

Note:

More information about configuring an Azure file share for AppVentiX can be found in this admin guide.

Create a content share (for example <u>\\yourdomain.local\appventix\content</u>), this share will be used to store the packages on. You can also create a folder on the same share as the configuration share created in step 1. The share permissions are the same as in step 1.

For integrated authentication (default), you can configure the below permissions for the content share:

- Domain computers group read permissions on the share
- Central View Admins (a group with users that performs the management) read\write permissions

When using a (service) account you can use the permissions from the screenshot in step 1.

Step 3

Install the AppVentiX Central View console on any machine you like, only keep the following in mind:

- The machine has to be installed with a 64 bit OS (Server OS or Client OS)
- The configuration and content share needs to be accessible

After you have installed the Central View console, click on the icon to start the console. The first time configuration window will open:

💩 Central View S	ettings (k	puild 23)	_					×
Centr	ral V	/iew settings		Configuratio	on Share	Settings	Advanced	License
Please entr	er the c	entral configuration shar	e (UNC): entixconfiashare\confia					
Use integrated windows authentication for share access 3 Share permissions								
Usernan	Username: localhost\appventixconfig ?							
Passwor	d:							
More information about the share configuration AppVentiX supports multiple share configurations, for example Windows file shares (direct or DFS), shares on storage vendors like NetApp, Dell, HP and Nutanix. Also Azure File shares are supported (both AD integrated and stand-alone). When integrated authentication is enabled the Central View console will use the currently logged in account to access the shares, it's also possible to configure a service account to access the share(s). The agent will also use integrated authentication by default but can also be configured to use a service account to connect to the share(s). The same (service) account can be used by Central View and the agent. This can be easily configured with one silent install parameter. Please click on the share permissions button for more information about configuring the share or consult the admin guide for more information.								

Configure the share you created in Step1. Please note above screenshot is from an Azure file share configuration. You can enter any UNC path you like.

Note:

Most of the time the default Central View settings are sufficient, optionally you can configure additional settings when needed, you will find more information about the settings in this guide.

Click save.

Step 4

Now we will create a Machine Group, you can use machine groups to implement DTAP (test, acceptation, production environment) or separate your deployment for hybrid use cases (laptops\ virtual desktops, etc). A machine group is just a reference to an AD OU, AD Group or Azure AD tenant, there is no need to update this groups manually.

Welcome to AppVentiX!
You're just a few clicks away from taking full control of your application deployment. Start by creating a machine group with the below button, setting up a machine group allows you to define one or more content shares for storing your packages. Once you configured the content share(s) you will be able to inventory and display the content.
Create Machine Group

Select the option where the machines which you want to manage are located.

4				Manage Machine Groups		
Select machine group:		Add new Machine Group ~	Remove selecte Machine Group	ed p		
		Active Dire	ctory Group			
Machine Group	Details	Active Directory OU				
Machine Group:	Please select a machine group	p Entra ID (Azure AD)				

In this example we will create a machine group based on OU:

1	Select OU	×
Done	Select the location where your Session hosts, VDI, RDS, Hostpool VMs, Fa are located.	t or other clients
Select Do	omain	-
Select O		
	Citrix VDI	
<u></u>	Domain Controllers	
• 🐼 F	at Clients	
B	RDS-2022	
۲ 🙆 T	est	
T 🔕	est Groups	
T 🔕	est Users	
🖉 V	Vin10	
🖉 V	Vin10-Test	
Ø 1	Vin11	

Select an OU and click Ok.

Friendly Name:	VDI Production, AVD Hostpool name, RDS Environment name or F		
Content share(s	used by this group:		
- \\mydom	ain.local\appventix\config	Enable Pre-cache Skip	Application Inventory

Provide an easy to remember friendly name like RDS Production or name it the same as the Citrix Delivery group, AVD Session Host pool or group of physical machines. The content share is automatically pre-populated with the same share as the configuration share, the content share is where the packages\containers are stored. Check if the content share is accessible and configure multiple content shares if you wish.

When the pre-cache checkbox is enabled, the agent will preload (App-V) \ prestage (MSIX) packages in the cache when the machine boots or when the refresh cycle is triggered. If you disable pre-cache they will be added on the fly whenever a user needs the package, making it a real dynamic delivery mechanism. You can use a combination of both approaches: pre-cache certain packages and dynamically delivery others, you can do this by creating 2 content shares, one with pre-cache enabled and another one with pre-cache disabled. The skip application inventory checkbox will hide applications from this content share in the Central View applications overview window.

After configuring the content share(s) click on Configure Agent Settings.

Conoral Sattings	General settings	
General Settings	Enable Features	
	Enable App-V management	
	Enable MSIX management	
	Enable FSlogix app masking management	

Enable the feature(s) you want to use and click Done. In this quick start guide we will use the default settings for each feature. Please check the Agent Settings chapter for an explanation of all agent settings. **Most of the time the default agent settings are a good starting point.** Click on Save Machine Group and close the Manage Machine Groups window.

The first time inventory of the content share is now executed, if no content is found you are asked if you want to import some packages to get started.

You can now click through the console and check if you can see the content and if the machines are visible when you select the machine group in the manage machines window:

Ν	/lanage	e Machines	Manage Content	Config	jura	tion and Act	ivity		
	<u>.</u>	😂 Refresh se	elected machine group			۲	<u></u>	*	\odot
Manage Test Group						Machine	User	Process	Invoke Refresh Cycle
Conly show online machines						Inventory	Machine (Group action	s
	Machi	ne Name 🔺	Machine Actior	IS					
_					_				
¥	RDS-2	2-01							
Ţ	RDS-2	2-02	💿 👺 🛱						
Ţ	RDS-2	2-03	۵ 🍇 🔹 💿						

Step 5

Now that the Central View console is up and running we will install the agent. The agent can be pushed remotely to the machines (this can even be done when users are logged in, no reboot is needed) or you can install the agent silently using an automated procedure, like an image build procedure or pipeline. When an older version of the agent is detected, it will be upgraded automatically.

Push agent:

Select one or multiple machines and click on the Push Agent button (manage machines page):



The agent will now be installed or upgraded automatically.

Manual install:

Click on the Browse Agent button, the agent installation is now shown. Double click the installation on a machine and follow the installation prompts.

Silent install:

Click on the silent install information button, the silent install parameter will be shown.

The agent contains a small GUI (AppVentiX Agent GUI) it will show you the service state and detected machine group, if the machine group is not detected or another error is displayed, please open the agent log (button at the right) it will show you a lot of useful information.

The AppVentiX Agent GUI is great for checking the service state, but also to see which packages are deployed, see package details and to troubleshoot and manage them. You can also invoke a refresh from the agent GUI (button at the bottom). A refresh can also be invoked in the Central View console (per machine or machine group). The refresh cycle runs automatically when the machine starts, optionally it can also be configured with a timer in the agent settings. By default user publishing is refreshed when the user logs in and user publishing will also be refreshed when the refresh cycle is invoked.



Step 6

Now you are ready to deploy packages and manage your deployment.

Go back to the Central View console and see how easy it is to inventory and manage machines by clicking on the eye icon. During this quick steps you configured a content share for the machine group, if you enabled the pre-cache checkbox the packages from the content share will be pre-loaded on the machine(s) when you click the refresh cycle button. If the pre-cache checkbox is disabled (default) the packages will be loaded based on the publishing tasks you configure. The refresh cycle (blue circle) will refresh publishing for currently logged in users and perform pre-cache of new packages, also packages removed from the content share will be removed from the machine automatically. No need to configure cleanup actions yourself.

	😂 Refresh selected machi	0	<u></u>	¢*	×-	\bigcirc	
Machine	RDS 2025	~	Machine	User	Process	Event	Invoke Refresh Cycle
Groups	Show online machines		inventory	Selec	ted Machir	ne actions	Refresh Cycle
Mad	chine Name	Machine	Actions				
ВС							
	S-25-01	۵ 🖉 🛱) 👔 🔇				
	S-25-02	۵ 🖉 🛱) 👔 🕻				

If you inventory the machine with the eye icon you see the App-V and\ or MSIX packages loaded on the machine:

🎲 Ap	oVentiX Central View 🔍							AppVentiX				
Applica	tions Manage Content Man	nage Machine	configurati	ion and	Activity							
-	C Refresh selected machin	ne group	۲	ST.	•*	2 3		Show all columns	d packages	Select active featu	re: 💁 📂	0
Machin Groups	e RDS 2025		Machine Inventory	achine User Process Event Invoke entory Inventory Inventory Refresh Cycle Selected Machine actions		Remove Package Selected Item actions		v Active Feature		Push Browse Si Agent Agent In Agent Install	ilent install formation ation	
	Machine Name	Mach	nine Actions		Machine	^						
	RDS-25-01	Ø	🚓 関 🙆			Туре	Name	^	Version		Publisher	
	RDS-25-02	۲	P 👔 💿			RDS-25-01 (last invent	ory time: 10-12-2024	10:47:44)				
				Package ApplicationRefresh 2.3.2.0 AppVention		AppVentiX						
						🎁 Package	Proaz3501	100	0.0.1.1		MyCorp	
						🍍 Package	TestApplic	ation	1.2.3.0		AppVentiX	

In the machine inventory view you can right click on the column header and select filtering options to easily find a package. With the user inventory feature (user group icon) you can see in real-time which users are logged in and which packages they have published.

With the "Show online machines" button you can filter the machines that are online (they will become green) and you can also see the agent version as well.

Next steps

- Go to the manage content page in Central View, check the content on your configured content share and create publishing tasks (assign packages to users or globally to machines). A great feature of AppVentiX is that unmanaged packages (when you remove a publishing task or remove a user from AD group assigned to a publishing task) will be unpublished\removed automatically for users. Please note that there should be at least one user publishing task configured in Central View to make the deployment managed. User published packages will not be automatically unpublished\removed when there are 0 user publishing tasks configured in Central View.
- Explore all Agent Settings, check the settings to meet your deployment goals, for example AppVentiX has different options to accommodate each scenario (for example persistent\non-persistent). Read through this admin guide to read more about configuration options, use cases and managing the deployment.
- Explore the Central View console and Agent GUI and check out all the options and features.

Deploy, Update and Remove applications with AppVentiX

With AppVentiX it is easy to deploy and update applications in real-time. It is possible to run multiple versions of an application side by side or replace an application with a new version immediately. There are a couple of approaches, and they are largely the same for App-V and MSIX, we would suggest trying out the different approaches to get familiar with them, you will see results in real-time. Managing applications with AppVentiX puts you back in control and will make you confident about application deployment and updates.

Deploy a new application:

- Place the new package containing the application on the content share
- Create a publishing task for the application
- When a user logs on the new application is published automatically, also when you run the refresh cycle (can be invoked centrally or on the machine itself) the user will receive the new application without having to log off and on again.

Update an existing application, approach 1 (run old and new side by side):

- You can either choose to create a new package or update the existing package, save the package as new package after updating (to allow old and new version to run side by side)
- Place the package containing the updated application on the content share
- Create a publishing task for the updated application (you can first assign this updated application to a test group for example)
- When a user logs on it will receive the new updated application, also when you run the refresh cycle (can be invoked centrally or on the machine itself) it will receive the updated application without having to log off and on again
- After your test users have verified the updated application, you can edit the new publishing task and assign the production group
- Remove the old publishing task, after doing this the old version will be removed for the user automatically

Update an existing application, approach 2 (run new version on test machine group):

- Copy the updated application to a content share which is configured for your test machine group
- Create a publishing task and filter this to only apply for the test machine group
- Let users log in to the test machine group so they can test the application
- Copy the package to the production content share after tests has finished
- Edit the publishing task so it will also apply on the production machine group

Update an existing application, approach 3 (replace old version with new version):

- Save the package as new package after updating or save the package with the same package name\id to increment the version number
- Place the package containing the updated application on the content share
- Create a new publishing task for the updated application and assign the same group as the old publishing task from the previous version
- Already logged in users will receive the updated application when the refresh cycle runs and new users when logging on, the already active users can continue to work in the old version. The new version will be active automatically when the user closes and re-opens the application
- If you want to immediately replace the old version with the new one (force), remove the old
 publishing task (or configure the force upgrade option in the new publishing task), the old
 version will be closed and the new version is active immediately. Please note that the
 application will be forcible closed, so when the user should keep the old version open leave
 the old publishing task in place and remove it later

Remove application, approach 1 (remove application for certain users):

- Remove users from the AD group assigned to the publishing task
- The application will be automatically removed for the users that are removed from the AD group

Remove application, approach 2 (remove application for all users, soft remove):

- Remove the publishing task for the package
- The application will be removed for the users
- After a while remove the package from the content share, it will be removed from the cache on the machines by the balance cache mechanism of AppVentiX

Remove application, approach 3 (remove application for all users, hard remove):

- Remove the publishing task for the package
- The application will no longer be published for users
- Remove the package from the content share and invoke the refresh cycle, this will prevent the package from being pre-cached and it will be removed from the cache on the machines by the balance cache mechanism of AppVentiX

Remove application, approach 4 (remove application using the drain mechanism):

- Remove the publishing task for the package
- The application will no longer be published for users

- Open the package options for the package which you want to remove, select drain this package. The package will no longer be deployed and removed from the cache when the refresh cycle runs. You can leave the package on the content share.

Remove application, approach 5 (by using inventory):

- Inventory the machine(s)
- Filter the package you want to remove on name
- Select the package (on one or multiple machines)
- Click remove package, the package will now be removed immediately

AppVentiX Components

AppVentiX consists of 3 main components:

- The AppVentiX Agent Service
- The AppVentiX Agent GUI
- The AppVentiX Central View Console

Please find more information about installing the agent in the quick start steps.

AppVentiX Agent Service

The service is responsible for deploying and managing packages, for publishing packages for users that are logging on and for users that are already logged on. The agent makes smart decisions, it will only publish new packages to users and it will unpublish packages for users automatically when they are no longer managed (when you remove the publishing task or remove a user from a group for example). The agent service can be configured with Agent Settings to fine tune your deployment. This settings will be discussed in detail later in this guide.

Every action of the service is logged in a dedicated eventlog, to make troubleshooting easy and will give you good insight in your AppVentiX deployment.

The AppVentiX Agent eventlog can be found directly under Applications and Services Logs :

Event Viewer (Local)
 Event Viewer (Local)
 Custom Views
 Windows Logs

Applications and Services Logs
 AppVentiX Agent

You can open the eventlog very easily from the Agent GUI with the Open Agent log.



You can also inventory the log remotely from Central View console, by clicking on the log icon next to a machine:



The agent service is event driven and the actions can be configured with Agent Settings. For example you can configure the agent to clear the cache at machine start, publish packages at user login etc. One of the most important events is the refresh cycle:

The Refresh cycle

The refresh cycle handles the deployment of new packages by comparing which ones are already present in the cache with the ones on the content share(s). The refresh cycle also refreshes the publishing tasks for currently logged in users. The refresh cycle runs at machine start-up and while the machine is running it can be triggered in four ways:

- Through a configurable timer (in the Agent Settings)
- Manually on the machine through the AppVentiX Agent GUI (Run Refresh cycle button)
- With the following Powershell command: (Get-Service 'AppVentiXService').ExecuteCommand(252)
- Remotely by the AppVentiX Central View console

You can recognize the Refresh Cycle by the blue circle:



In Central View you can invoke the refresh cycle for a single machine (blue circle next to the machine) or for the whole machine group (machine group actions).

The refresh cycle does the following things on the agent:

1: Pre-cache packages from content shares (only when pre-cache is enabled for the content share) (App-V and MSIX)

2: Remove packages from the cache that are no longer on one of the configured content shares (when this setting is enabled in the agent settings). Default this setting is enabled. (App-V and MSIX)

3: Execute global publishing tasks (App-V only)

4: Execute user publishing tasks for currently logged in users (App-V and MSIX)

5: Execute drain tasks, remove packages from the system when it still exists and a drain package option is configured for the package (App-V and MSIX)

Optionally the below PowerShell commands can be used to initiate the refresh cycle, for example as scheduled task or an automation solution:

Refresh cycle action	Powershell Command
Refresh both cache and publishing tasks	(Get-Service 'AppVentiXService').ExecuteCommand(252)
(default)	
Refresh only cache: balance cache to	(Get-Service 'AppVentiXService').ExecuteCommand(242)
remove old packages, pre-cache packages	
when enabled for a content share, process	
package drain tasks	
Refresh only publishing tasks for currently	(Get-Service 'AppVentiXService').ExecuteCommand(241)
logged in users and refresh global	
publishing tasks (App-V)	

AppVentiX Agent GUI

The AppVentiX Agent GUI can be used for:

- Checking the service state
- See details about deployed packages
- Troubleshoot packages
- Check the App-V and MSIX client state and configuration
- Invoke the refresh cycle

Example screenshots of the Agent GUI:

	- 🗆 🗙	September Agent GUI	- ×
September 2.2.24	Community license	Provide AppVentiX Agent 3.2.24	Community license
WIN10-20H2-01 is member of the following machine groups:		Currently deployed Packages:	
FriendlyName FullName AgentSettings		General Package Name Version Published Globally Published to User In Use Percent Loaded Size	E Publish Package
App-V Test Group OU+Wint0-20H2,DC+bwleb,DC+local Active		App-V DWGsee Pro 2016 BOOLT True False False False 100 54.32 MB	Lough Antiberting
5 1/1 1/2		Firefox ESR 52,7,1 0,0,0,1 True Faite Faite 100 103,75 MB	
ALCM		MSK	Launch CMD
App Mask The following content share(s) are used by this machine:		App Mask	Launch Regedit
Content Share Precache Enabled			Package Datails
\uk01\content/lab True			2 Ramove Package
upwabacchie.core.windows.neruppications. Hase			S Release
		Currently deployed Connection groups:	
AppVentiX Service details	Configure Service	Connection Group Name Enabled Globally Enabled for User In Use Priority	
Application contractions interest and a state of the stat	C Restart service	TOP-TOPOLOGIC AND ADDRESS AND THE PARK IN	
Approvide Approximation (a contract of the con			Sa Refresh
Apprenta Agent service status: Numming	ing open Agenciog		
		App-9 Cherri delatis Arrad Clard Maximus 5200 Initial site of parkanes 158.12 h	46 App-V Client log
		Shared Content Retro Mode: On App-V Cache location: %programdata%A	/pp-V @Nurning Processes
		App-V Client Service status: Running	ation Pending Tesis
Bun refresh cycle	Close	🔞 Run refresh cycle	📭 Close
R tarthant familie		A subolition of a	
	Community license		Community license
AppVentiX Agent 3.2.24		AppVentiX Agent 3.2.24	
General Currently deployed Packages:		Ceneral Currently deployed App Masking rules and assignments:	
General Currently deployed Packages: Q	Register Package	Ceneral Currently disployed App Masking rules and assignments: Q	
General Padage New Works (Inf Kine Control Padage New New New New New New New New New Ne	Helizo, Hostik ode: Helizo, PostalCode:	Centeral Currently deployed App Marking rules and assignments: Q. None type (activated App-V Processing App Activated Processing App App Activated App App App Activated App App App Activated App App App Activated App App Activated App App Activated App App Activated App App Activated App Activated App App Activated App Act	
General Currently deployed Peckages: Public Package New Jewissis Public Public App V Intraserutive Vision Fall New Sci 2014 (expression) Public 1628 1000 Fall New Sci 2014 (expression) Outsigneets (clinit): Appliced, clinit): Appliced, clinit, DisAppliced, clinit, Di	Helico, Instalcade Helico, PostalCade Helico, PostalCade	Centertill Currently deployed App Masking rules and assignments: App-V None Nym (est-tabled) Mode: Nym (est-tabled) (est-tabled) Mode: Nym (est-tabled) (est-tabled) Mode: Nym (est-tabled) (est-tabled) MSX MSX (est-tabled) (est-tabled)	
General G	-Hridoo, Hostal Code Elicitoo, Postal Code Hicitoo, Postal Code Hicitoo, Postal Code Elicitoo, Postal Code Il Code Code Elicitoo, Postal Code Il Code Code Il	Centeral Currently deployed App Masking rules and assignments:	
General Centrently deployed Peckages: Public App V Produce rates 52/2 Produce rates 52/2 Public App V Instance rates 52/2 Produce rates 52/2 Public Childree	-Nidoo, Hvidal Cade El Class, Rotal Cade Hildios, Rotal Cade Hildios, Rotal Cade El Class, Rotal Cade El	Centernial Currently deployed App Masking rules and assignments: Q App-V Massaching and assignments: Q Massaching and ass	
General Commits designed Peckages: Output App V Package New Vacion full New X-27.8 at segments the Characteristic X-27.8 at segments the Characteristic X-27.8 at segments the Characteristic X-27.8 at segments the Characteristic X-27.8 at segments the Characteristic X-27.8 at segments the Characteristi	Helico, Yindak ada Helico, Yindak ada Helico, Yoshalicida Helico, Postalicida Helico,	Centertill Centertil Centertill Centertill Centertill Centertill Centertill C	
General Carterial depayse Processor Carterial App V Postor full have Postor full have Postor full have App V Postor full have Postor full have Postor full have App V Postor full have Postor full have Postor full have Mode Postor full have Postor full have Postor full have Mode Notification Postor full have Postor full have Mode Notification Postor full have Postor full have App Mask Notification Notification Postor full have	Holico Positión Holico Positió	Centeral App-V App-V MSX > App Mask	
General Carrently deployed Packages: Package App V Package New Vectors full Name Package New Vectors full Name Package New Vectors full Name App V Package New Vectors full Name Package New Vectors full Name Package New Vectors full Name MSIX Package New Vectors full Name Package New Vectors full Name OcharageNew Xet Into OcharageNew Xet Int	Hallon (Yotalicato) Hallon (Y	Centernial Currently deployed App Masting rules and assignments: App-V Internet type (rational assignments) MSX MSX > App Mask	
General Protografile Protografile Respect Public App V Transacrate Rodal Constructions (22.9.8.4 singeboard) Publice Transacrate Rodal Constructions (22.9.8.4 singeboard) Publice Chargeboard, Charlo (20.6.4 singeboard) MOIX Rodal Constructions (22.9.8.4 singeboard) Chargeboard, Charlo (20.6.4 singeboard) Chargeboard, Charlo (20.6.4 singeboard) App Mark App Mark State State Objective (Charlo (20.6.4 singeboard))	Andro, retardo Andro, retardo Helso, Rotaldo Helso,	Cerrentyl deployed App Makling rules and assignments: App-V Most Pape Instruction Pape-Onto-State Approx. Pape-Onto-State Ap	
General App V Pological Pological Pological App V Pological Pological Pological Pological Pological Pological	Andron market Andron	Centerful App-V App-V A	
General App V Protect and young Packages: Package Protect and young Packages Package Protect and young Packages Package Packa	Andrin valkes Andrin valkes an	Cerrential Currently deployed App Masking rules and assignments: Appr-V MSX Appr-V App Other (Constraint) Appr-Other (Constr	
Gorneral App V Pakage Weaks Pakage Weaks Pakage Weaks Pakage Wea	Adda, saida Adda, saida, saida Adda, saida, saida, saida Adda, saida Adda, saida Adda, saida Adda, sai	Cerrentyl deployed App Makling rules and assignments: Q how hyn (stabuled MASX MASX > App Mask	
General App V App V Make Padage Mexico, Ida	Antion indexection index index indexection index index	Centernial Currently deployed App Masting rules and assignments: Q App-V MSX App-Mask App-Mask App Mask	Prove Selected
General App: V Protoconter 0-200 generative segments Protoconter 0-200 genet Protoconter 0-200 generative segments Protoconter 0-20	Andrin valkes Andrin valkes an	Centertial Centertial Control deployed App Making rules and assignments: Centertial Control to the approximation of the approximation o	
General App V Protect Attributes Protect Protect Attributes Protect Prote	Andio, handback Andio, handback and handba	Cerrentyl App-V Ap	Inner Selected Prove Selected Prove Selected Prove Selected Prove Selected Prove Make ing
General App V Protect App App App App App App App App App Ap	Andron State Bandford Andron State Bandford State Bandford	Cerrential	and a second sec
General App V App	Andron van de service de la construir de la co	Cerrential Cerrential Cerrential Cerrential Cerrential Conversion Type Type Type Type Type Type Type Type	estady

The AppVentiX agent is configured centrally in the Central View console. There are a couple of settings you can configure when you click on the Configure Service button:

Provide a state of the second	-		×
Dease enter the central configuration share (LINC):			
\\appventixconfig.file.core.windows.net\appventixconfigshare\config			
Authentication			
Enable Debug mode			
Please note: You need (runas) administrator permissions to modify this settings			
Save Configuration	k	Cance	

In the agent configuration you can change\update the configuration share. You can also provide a user account which the service will use to access the configuration share and content share(s). By default the service will use integrated authentication.

Debug mode will log more information to the eventlog for troubleshooting purposes, make sure to disable this option after troubleshooting.

You can export these settings to a registry file to import on other machines. This settings can also be provided for silent installation of the agent, click on the silent install button in the Central View console (agent ribbon) to see the prepopulated silent installation parameter. Please note that all other Agent Settings are configured and stored centrally.

AppVentiX Central View Console

Central View is the centre piece of your deployment. It is a lightweight, easy to use real-time management console. Central View does not need a dedicated back-end server.

It gives you complete control and insight in your App-V and MSIX deployment, you can use this console to perform every step in the lifecycle process of a package.

Machine Groups

Central View reads Active Directory group(s), Active Directory OU's or Azure AD to retrieve the machines in a specific machine group. The agent will automatically detect in which machine group it belongs. Please read the quick start steps at the beginning of this guide to get an impression how to create a machine group.

When creating a machine group based on AD group instead of OU, make sure you enable below option in Active Directory when adding machines to the AD group, or else you can't find machine accounts to add to the AD group:

Object Types
Select the types of objects you want to find. Deject types: Contacts Contacts Contacts Computers Computers Users Users
OK Cancel

Note:

You can create multiple machine groups and machines can be member of multiple machine groups, you can also configure multiple content shares for a machine group. The agent will retrieve packages from all configured content shares. The agent will only apply Agent Settings from the first Machine Group it is member of. You can always edit a machine group and change Agent Settings, please note that the Agent Service on the machine needs to be restarted before the new settings will be activated.

When creating a machine group you can configure content share(s) for the group, next to the content share you have the option to select a checkbox: Enable - Precache.

When pre-cache is enabled for a content share the agent will deploy packages from the content share in the cache when the refresh cycle runs. Use pre-cache when you want packages to be available on the agent before a user logs in (for fast publishing). For App-V this options means packages are loaded on the machine, for MSIX this means packages are staged on the machine (when used in combination with app attach, the disk is attached and the package staged).

Don't enable pre-cache for a content share if you want packages to be deployed on the fly at user login using publishing tasks. This is supported for all package formats, App-V, MSIX + app attach.

Machine Group Agent Settings

Configure Agent Options to fine tune your deployment. Agent options are retrieved and applied by the agent running on the client machine. Agent settings are applied when the agent service (re)starts.

General Settings

Here you can enable App-V and\or MSIX, you can also enable them both to use them side by side. The settings are split between the features to easily navigate through the settings.

General Settings	General settings	
Machine Start actions	✓ Enable App-V management	
	✓ Enable MSIX management	
Refresh Cycle actions	✓ Enable FSlogix app masking management	
Client settings	🤪 App-V 🍵 MSIX	
	General settings	
	✓ Enable user publishing at login ? ✓ Enable user publishing refresh at reconnect and unlock ?	
	✓ Automatically unpublish unmanaged packages and connectiongroups (?)	
	Publish packages globally when there is no user publishing task configured	
A duran and a still and		
Advanced settings		
	0	Done
Conoral Cattings	General settings	Done
General Settings	General settings	Done
General Settings Machine Start actions	General settings Enable Features ✓ Enable App-V management	Done
General Settings Machine Start actions	General settings Enable Features ✓ Enable App-V management ✓ Enable MSIX management	Done
General Settings Machine Start actions Refresh Cycle actions	General settings Enable Features ✓ Enable App-V management ✓ Enable MSIX management ✓ Enable FSlogix app masking management	Done
General Settings Machine Start actions Refresh Cycle actions Client settings	General settings Enable Features Enable App-V management Enable MSIX management Enable FSlogix app masking management MSIX	Done
General Settings Machine Start actions Refresh Cycle actions Client settings	General settings Enable Features Enable App-V management Enable MSIX management Enable FSlogix app masking management App-V MSIX General settings	Done
General Settings Machine Start actions Refresh Cycle actions Client settings	General settings Enable Features ✓ Enable App-V management ✓ Enable MSIX management ✓ Enable FSlogix app masking management ✓ Enable FSlogix app masking management ✓ Enable Slogix app masking management ✓ Enable settings ✓ Enable user publishing at login ?	Done
General Settings Machine Start actions Refresh Cycle actions Client settings	General settings Enable Features Enable App-V management Enable FSlogix app masking management App-V MSIX General settings Enable user publishing at login ? Enable user publishing refresh at reconnect and unlog Automatically unpublish unmanaged packages ? Prevent package cleanup by Window	Done
General Settings Machine Start actions Refresh Cycle actions Client settings	General settings Enable Features Enable App-V management Enable FSlogix app masking management Enable FSlogix app masking management General settings Enable user publishing at login ? Enable user publishing refresh at reconnect and unlo Automatically unpublish unmanaged packages ? Prevent package cleanup by Window Enable MSIX app attach ?	Done
General Settings Machine Start actions Refresh Cycle actions Client settings	General settings Enable Features Enable App-V management Enable MSIX management Enable FSlogix app masking management App-V MSIX General settings Enable user publishing at login Enable user publishing refresh at reconnect and unlog Automatically unpublish unmanaged packages Prevent package cleanup by Window Enable MSIX app attach Automatically detach unused app attach disks at logoff Allow AppVentiX to register packages containing a service for normal users	Done
General Settings Machine Start actions Refresh Cycle actions Client settings Advanced settings	General settings Enable Features Enable App-V management Enable MSIX management Enable FSlogix app masking management App-V MSIX General settings Enable user publishing at login Automatically unpublish unmanaged packages Prevent package cleanup by Window Enable MSIX app attach Automatically detach unused app attach disks at logoff Allow AppVentiX to register packages containing a service for normal users MSIX data roaming configuration: Second State Containing a service for normal users	Done

The most Agent Settings speaks for themselves they will be described below. The most settings applies to both App-V and MSIX. Where they are different you will find them in their own groupbox.

General settings	
Enable user publishing	Enables the service to process user publishing tasks when a user logs in (App-V and MSIX)
Enable user publishing at	Enabled the service to process user publishing tasks when a user
session reconnect	reconnects or unlocks his session (App-V and MSIX)
Publish packages globally	Instructs the agent to deploy packages globally when there is no
when there is no user	user task configured for the package (App-V only)
publishing task configured	
Automatically unpublish	This setting makes the deployment fully managed. When you
unmanaged packages	remove a publishing task the package will be unpublished \
	removed for the user automatically (App-V and MSIX)
Enable MSIX app attach	This enabled the app attach integration in the agent (MSIX only)
Automatically detach unused	Default this setting is disabled. By default app attach disks are
app attach disks at logoff	automatically detached when the machine is rebooted, optionally
	you can enable this setting if you want to detach unused app attach
	disks at logoff. When enabled, the service will check 30 seconds
	after a user logoff if the app attach disk is still in use, if not it will be
	detached. This allows you to cleanup old disks from the content
	share without rebooting the machine also the number of attached
	disks on a machine will be lower. This feature is especially useful
	for shared OS (like RDS \ multi-user OS) and when you have a lot of
	app attach disks to manage and the machines are rebooted less
	frequently. Events about the auto detach feature are logged in the
	AppVentiX eventlog.
Allow AppVentiX to register	MSIX packages containing a service can only be added with
packages containing a service	elevated permissions, AppVentiX can add the package to allow the
for normal users	service to install and will then register it for a normal user account
Prevent package cleanup by	When you use FSlogix or another profile container solution and a
windows	user logs off the profile is removed from the machine. Windows
	can detect that a package is no longer needed on the machine and
	removes the package. It will be deployed automatically again when
	the user logs in again, but with this setting the package will stay on
	the machine when the user logs off. Then you can remove
	packages using the balance cache feature of AppVentiX, which will
	automatically remove packages from the cache that are no longer
	on one of the content share(s).
MSIX data roaming	This setting will allow you to configure the profile solution you are
	using. By default the profile container option is enabled, this will
	make sure the package deployment is compatible with container
	based profile solutions. Please contact support if you need more
	information about this setting.

Machine start actions

With machine start actions you can configure the machine start configuration.

General Settings	When the machine starts	
Machina Start actions	Disable logons to the machine until the cache is up to date ?	E
	✓ Run refresh cycle to update the cache ?	
Refresh Cycle actions	Detect image state (Enable Citrix PVS/MCS integration)	
Client settings		
	 App-V <a>MSIX Clear App-V cache before updating the cache Enable Application pre-Launch for selected applications 	
Advanced settings		

When the machine starts	
Disable logons to the machine until the cache is up to date	The agent will disable logins while the cache is updated at machine start. It will enable logins again when the cache is up to date
Run refresh cycle to update the cache	Invoke the refresh cycle at machine start to pre-cache packages from the content share(s) (when enabled for the content share)
Detect image state (Citrix PVS\MCS integration)	When the machine starts, the agent can detect the image state (read only or read\write). It can make smart decision how to deploy packages. Other agent settings are updated automatically when you enable this feature. There are 2 supported scenario's:
	Scenario1: Private mode: Stop Refresh cycle, this will prevent packages from being deployed while the image is in private mode. Read-only mode: Deploy packages
	This scenario is often used for non-persistent RDS environments, you can redirect the cache to a persistent drive.
	Scenario2: Private mode: Deploy packages in the cache Read-only mode: Deploy new packages using optimized delivery (App-V Shared Content Store mode or MSIX AppAttach)
	This scenario is often used for non-persistent VDI environments. Leave the cache in the default location. When the image is build or opened for Windows Updates for example, the agent will automatically pre-cache all packages from the configured content- shares. When the image is running in read-only mode you can deploy new packages or package updates. The agent will automatically use SCS mode (App-V) or AppAttach (MSIX) to make sure the write cache is not polluted.

Clear cache	This setting will instruct the agent to clear the cache at machine start before the packages from the content share(s) are pre-cached. Clear cache is an advanced feature: It will first remove packages and then remove any left overs in the cache to make sure it's empty. This setting is often used for non-persistent environments where the cache is redirected to another drive.
Enable application pre- launch	In the Central View console you can configure applications that you want to pre-launch at machine start. This will speed up the second launch by users. Only use this for applications that has a clear benefit from this.

Refresh Cycle actions

Here you can configure the refresh cycle actions.

	Execute cache management at time interval	
60 Minutes 🧃	Execute publishing tasks at time interval	
Pre-cache packages from content sh	ares with the pre-cache option enabled 🕜	
Execute user publishing tasks for cu	rrently logged in users when the refresh cycle runs ?	
Only process publishing tasks for pa	ckages on content share(s) configured for the machine group ?	
·····		
 Remove packages from the cacl Process Deployment configurat 	he that are no longer on the configured content share(s) ?	
 Remove packages from the cacl Process Deployment configurat Process Global pending tasks 	he that are no longer on the configured content share(s) ? ion files ? Remove User pending tasks ?	
 Remove packages from the cach Process Deployment configurat Process Global pending tasks Enable Registry pre-staging for 	he that are no longer on the configured content share(s) ? ion files ? Remove User pending tasks ? selected packages and connectiongroups ?	

Refresh cycle actions	
Timer when the refresh	You can configure the refresh cycle to run every x minutes. The
cycle runs	refresh cycle already runs at machine start-up to perform cache
	management, you can enable a timer how often the refresh cycle
	should run during machine uptime and which part of the refresh
	cycle to invoke at the configured interval
Pre-cache packages from the	This is a mandatory setting, you can control if you want to pre-cache
content shares with the pre-	packages using the checkbox next to the content share in the
cache option enabled	machine group configuration window.
Execute user publishing	With this option you can publish new or updated packages to users
tasks for currently logged in	while they are logged in. They do not have to logoff and back on
users	again.
Only process publishing	Publishing tasks are executed for users on machines regardless of
tasks for packages on	where the package is stored, so a package could be added to a
content share(s) configured	machine from a content share which has not been configured for a
for the machine group	machine group. With this setting only publishing tasks are executed
	for packages that are on one of the content share(s) configured for

	the machine group.		
Remove packages from the cache that are no longer on the configured content share(s)	This option will remove packages from the cache when they are no longer found on one of the configured content share(s). This settings is especially handy for persistent environments to keep the cache clean and up to date. This setting is often not needed when you enabled the clear cache at machine start action.		
Process Deployment configuration files	When this setting is enabled, the AppVentiX agent will process the deployment configuration file that's in the same folder as the package. The configuration file needs to have the .appd extension instead of .xml. This makes sure only configuration files are processed that are meant to be processed, without deploying all configuration files by default. (Applies to App-V only)		
Process global pending tasks	When a global published package is in use when a newer version is deployed the App-V client will generate a pending task to publish the package when the machine reboots. This is often not desired and the package needs to be available without the users logging off and having to reboot the machine. With this setting enabled the AppVentiX agent will detect global pending tasks and process them automatically when the package is no longer in use. The user only have to close the application and the agent will publish the new version immediately when it's no longer in use without a machine reboot. (Applies to App-V only)		
Remove user pending tasks	Remove user pending tasks before executing user publishing tasks to make sure the publish operation is retried when a package was in use the previous time the publishing operation was executed (Applies to App-V only)		
Enable registry prestaging	The pre-stage virtual registry option makes sure the virtual registry of the package is already loaded on the machine directly after the package is added (this is normally done when the user starts the application for the first time which can cause launch delays). This feature is especially for bigger packages in combination with non- persistent environments. You need to configure a service account if you want to use this feature.		
Enable draining	Enable this option if you want to use the draining feature. When selecting packages in Central View you can select "Drain this package" in the package options. The agent will remove packages that are on the drain list and will prevent them from deploying again.		

Client settings

With client settings you can configure the App-V and\or MSIX client. You don't have to configure any GPO's, the agent will configure the settings for you. A single point of configuration.

Client configuration (The agent will configure the client, no GPO's needed)	Canadal Cattings	Client configuration (The agent will configure the client, no GPO's needed)
🥥 App-V 🦉 MSIX	General setungs	🥹 App-V 🏾 🍯 MSIX
C Enable App-V Client App-V Cache Location: Sprogramdata(S)App-V	Machine Start actions Refresh Cycle actions	MSIX Default volume:
Enable Shared Content Store (SCS) mode 7 Enable Dynamic Virtualization 8	> Client settings	Skip and hide Microsoft parkages
Enable Peckage Scripts 77 Enable Package Scripts 77 Enable A3 name creation on App-V package drive 29 Inable Offica365 integration with App-V packages 29		Side Load O Developer mode
Cache mode Mount all packages Mount all packages Managed moder. Mount selected packages, use SCS mode for the rest	Advanced settings	
		O Done

Enable App-V Client	The AppVentiX agent will enable the App-V client for you, no need to enable the App-V client on the machines manually
Cache location	The location where the package cache is stored
Enable SCS mode	Here you can configure if SCS mode should be enabled or disabled (it
	will be enabled by default). The service will configure SCS mode
	automatically when the service starts. (Applies to App-V Only)
Enable dynamic	This setting is default on but you might check to turn this off, this
virtualization	feature will integrate packages automatically with internet explorer
	and windows explorer (for example for plugins and context menus in
	explorer). If you want to have more isolation and control turn this
	setting off. (Applies to App-V only)
Enable package scripts	This setting is default off, if you enable this setting the App-V client
	will allow the use of package scripts. (Applies to App-V only)
Enable 8.3 name creation	The App-V client requires 8.3 name creation to be enabled on the
	disk containing the packages, this option will make sure it is enabled
Enable Office 365	With this setting you can enable virtual applications to be integrated
integration	with the installed Office 365 installation (applies to App-V only)
Cache mode	Here you can configure the desired cache mode, you can choose
	from the following options:
	When Shared Content Store (SCS) mode is enabled:
	Cache mode
	O Mount all packages ??
	Mount configured packages, use SCS mode for the rest
	O Use SCS mode only
	Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u> : Cache mode
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages ?
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand Stream packages on demand
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages ? Mount configured packages, stream the rest on demand Stream packages on demand ? Mount all packages will always mount (pre-cached) all packages in the cache
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages ? Mount configured packages, stream the rest on demand Stream packages on demand ? Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages ? Mount configured packages, stream the rest on demand Stream packages on demand ? Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages ? Mount configured packages, stream the rest on demand Stream packages on demand ? Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand Stream packages on demand Stream packages on demand Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For other packages SCS mode is used or they are streamed to
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand Stream packages on demand Stream packages on demand Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For other packages SCS mode is used or they are streamed to the cache when SCS mode is disabled
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand Stream packages on demand Stream packages on demand Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For other packages SCS mode is used or they are streamed to the cache when SCS mode is disabled Use SCS mode only, no packages will be mounted (pre-
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand Stream packages on demand Stream packages on demand Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For other packages SCS mode is used or they are streamed to the cache when SCS mode is disabled Use SCS mode only, no packages will be mounted (precached) in the cache, every package uses SCS mode and
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand Stream packages on demand Stream packages on demand Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For other packages SCS mode is used or they are streamed to the cache when SCS mode is disabled Use SCS mode only, no packages will be mounted (pre-cached) in the cache, every package uses SCS mode and reads the content directly from the network share
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand Stream packages on demand Stream packages on demand Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For other packages SCS mode is used or they are streamed to the cache when SCS mode is disabled Use SCS mode only, no packages will be mounted (precached) in the cache, every package uses SCS mode and reads the content directly from the network share Stream packages on demand (when SCS mode is turned off)
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand Stream packages on demand Stream packages on demand ? Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For other packages SCS mode is used or they are streamed to the cache when SCS mode is disabled Use SCS mode only, no packages will be mounted (precached) in the cache, every package uses SCS mode and reads the content directly from the network share Stream packages on demand (when SCS mode is turned off) packages are loaded in the cache when they are started
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand Stream packages on demand Stream packages on demand Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For other packages SCS mode is used or they are streamed to the cache when SCS mode is disabled Use SCS mode only, no packages will be mounted (precached) in the cache, every package uses SCS mode and reads the content directly from the network share Stream packages on demand (when SCS mode is turned off) packages are loaded in the cache when they are started (applies to App-V only)
	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages Mount configured packages, stream the rest on demand Stream packages on demand Stream packages on demand Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For other packages SCS mode is used or they are streamed to the cache when SCS mode is disabled Use SCS mode only, no packages will be mounted (precached) in the cache, every package uses SCS mode and reads the content directly from the network share Stream packages on demand (when SCS mode is turned off) packages are loaded in the cache when they are started (applies to App-V only)
Deployment mode	 Use SCS mode only When Shared Content Store (SCS) mode is <u>disabled</u>: Cache mode Mount all packages ? Mount configured packages, stream the rest on demand ? Stream packages on demand ? Mount all packages will always mount (pre-cached) all packages in the cache Mount configured packages (this is the recommended cache mode) (you can configure packages that should be mounted (pre-cached) in the cache in the Central View console. For other packages SCS mode is used or they are streamed to the cache when SCS mode is disabled Use SCS mode only, no packages will be mounted (precached) in the cache, every package uses SCS mode and reads the content directly from the network share Stream packages on demand (when SCS mode is turned off) packages are loaded in the cache when they are started (applies to App-V only)

information (applies to MCIV only)	
information. (applies to wisix only)	information. (applies to MSIX only)

FSlogix App Masking feature	
Enable App Masking management	This feature can be enabled with only one checkbox, when enabled you can centrally manage FSlogix App Masking rules and assignments. In the same way as you manage packages.

Advanced settings

Only change advanced settings when you have a special use case for it.

ackup;dfsrprivate;	lependencies				
Enable remote	1anagement ?				
ventory through	configuration share:	Inv	entorv refresh interv	al in seconds (default 5)	:5 🕜
·····, ····j			,	. ,	
🥥 App-V 🔰	MSIX				
		0		•	
Show save pack	age data progress at logoff:	⊖ On ⊖ Off	 Not configured 	•	

Advanced settings	
Enable remote management	This setting will enable WinRM on the agent, this is only needed when the inventory through configuration slider is disabled. In this case inventory will be done on the agent directly instead of through the configuration share.
Inventory through	The agent will check every x seconds (5 by default) if an inventory is
configuration share	needed, if there is no request to do an inventory the agent will do nothing. Inventory is saved in the inventory folder on the
	configuration share.
Exclude the following	A list of folder names that are skipped by the agent. By default a
directory names on the	folder containing the name backup and dfsrprivate is excluded. The
configured content share(s)	list is separated with a semicolon (;)
Wait time before executing	Normally not needed, but here you can configure a specific timeout
user publishing tasks	after a user login before the user publishing tasks are executed
Boot time value	The time the service detects that the machine has just rebooted and
	machine start-up actions are executed. By default this is 900
	seconds. Increase this value if your machines have a very long start-
	up time.
Enable staged package load	In some cases, when a lot of packages are loaded in the cache at the

procedure (App-V)	same time, the App-V client doesn't load some packages correctly.
	When this feature is enabled, packages will be loaded using an
	interval to prevent this issue from occurring.
Enable App-V Cache	This feature will validate the App-V cache and reload packages that
validation after loading	are not loaded in the cache correctly. This feature makes sure the
packages	App-V cache is always healthy.
Prevent package cleanup by	This feature will add a regkey with the full package name to the
windows	allusers package store, this prevents Windows from cleaning up the package when no user has this package registered. Because package removal is already managed by AppVentiX as part of the cache management feature (removed packages from the content share will be removed from the agents automatically) automatic cleanup by Windows is not needed and can cause the package to be re-added more often unnecessarily
Persist MSIX appdata method	By default MSIX appdata is saved at logoff so it will be able to roam with the user, at logoff is the recommended setting. At session end will save the package state when the session is ending (earlier then the logoff process), only enable this setting when you can't use the logoff method. This feature works exactly the same for normal deployed MSIX packages and MSIX packages delivered with app attach. The log file for the persist MSIX app data at logoff setting can be found in: %appdata%\AppVentiX

Manage Machines page

The manage machines page in Central View allows you to inventory machines, easily check which packages are deployed on a machine. Compare machines with each other (check if they have similar packages deployed). You can also search packages by name:

Machine				joh	n	⊗ ×
Туре	Name	Version	Globally	In Use	Loaded	
4 🗌 📮 VDIW10UP0008					Cou	int=1
Package	Johnson Controls 1.6	0.0.0.2	True	False	100	
4 🗌 📮 VDIW10UP0016					Cou	int=1
🗌 🥥 Package	Johnson Controls 1.6	0.0.0.2	True	False	100	
4 🗌 🖵 VDIW10UP0026					Cou	int=1
Package	Johnson Controls 1.6	0.0.0.2	True	False	100	

It's also possible to right click on a column header and set a filter to easily find the packages you are looking for:



You can select multiple packages and then click on Remove Package, this will remove a package from the machine(s) in real-time. (in the selected items ribbon menu). You can also filter machines so you

only see machines that are online, you will find this filter underneath the select machine group dropdown box.

Actions can be performed per machine (for example inventory or refresh) or per machine group (using the machine group actions ribbon menu).



If you enabled both App-V and MSIX for a specific machine group you will be asked which feature (App-V or MSIX) you want to manage, you can switch the active feature with the dropdown box you will find in the ribbon menu. You can manage App-V and MSIX side by side.

With the show virtual process button, you can inventory the virtual processes on machines and close them if needed (for example if you want to remove a package that is in use).

With the user inventory button you can see in real-time which users are logged in and which packages they have published. You can also invoke a repair from there.

The event inventory will allow you to see all the latest events from the agent.

All Publishing All Packa Tasks Option	ge Delete from disk	Package Analy: Details with TM	te Edit Convert	Crea	ite Edit (n Group	Connection Group	Create Package Pa	Edit Re ackage Pac	esign Convert to Ci ckage AppAttach	reate shared container	Open with Editor	Create	e certificate for MSIX	Import 1 Microsoft	rom Import Store AppV	Shi Ski I from lentiX	ow all column ip hidden fold	s 📄 ers 🖌	
Show	Select	ted Item Actions		App	-V Actions			м	ISIX Actions	,	App Masking	g MS	SIX Deployment	Imp	ort Packages		View		
Content Share	^	Actions	Skip Inventory		ontent Share	^													
\\dc01.bwlab.local\cc	ntent\win25						Type	~	Name		V	/ersion	Publishing Ta	sks	Packa	ge Options	Publ	isher	Last Updat
\\dc01\content				- 4	📃 🐸 W	dc01.bwlab.	local\conten	t\win25											
						SIX asix	Shared	container	SC_ApplicationRef	resh_TestApplic	ation2		👺 Publish		Configu	re			21-11-202
						💮 АРРМА	SK Rule Se	et	Citrix_Citrix Works	pace.fxr									25-11-202
						🕀 АРРМА	ASK Rule Se	et	BentlyNavigatorCo	nnectEdition.fx	r								25-11-202
						🎯 APPV	Packag	e	ApplicationRefresh		0	0.0.0.2	👺 Publish 🔎	Show	Configu	re			6-12-2024
						🍵 MSIX	Packag	e	Proaz3501100		0	0.0.0.1	👺 Publish		Configu	re	CN=	MyCorp	19-11-202
						🎁 MSIX	Packag	e	Proaz3501100		0	0.0.1.1	👺 Publish 🔎	Show	Configu	re	CN:	MyCorp	18-11-202
						🎁 MSIX	Packag	e	Microsoft.Microsof	tPowerBIDeskt	op 2	2.138	👺 Publish		Configu	re	CN-	Microsoft	14-11-202
						🎁 MSIX	Packag	e	ApplicationRefresh		2	2.3.2.0	👺 Publish		Configu	re	CN	AppVentiX	14-11-202
						🎁 MSIX	Packag	e	TestApplication		1	1.2.3.0	⁸ Publish	Show	Configu	re	CN:	AppVentiX	14-11-202
						🍅 APPV	Packag	e	Proaz_3501.100		0	0.0.0.1	👺 Publish		Configu	re			22-10-202
						🍅 APPV	Packag	e	Archi_530.100		0	0.0.0.1	👺 Publish 🔎	Show	Configu	re			22-8-2024
						🍅 APPV	Packag	e	TestApplication		0	0.0.0.1	2 Publish		Configu	re			26-11-202
						appv 🏭	Group		CG_Archi_530.100	_TestApplicatio	n		2 Publish		Configu	re			5-12-2024
						🧕 MSIX	Certific	ate	PrivateSigning.cer										13-11-202

The manage content page allows you to inventory the content share(s) and manage the central configuration. Click on the eye icon next to the content share to inventory the share. Here you will find a lot of information about the packages, do not forget to select the Show All\Hidden columns checkbox to see even more information, like package size etc.

Double click on a package (or select the package and click on the Configure Package button in the selected item actions ribbon menu). To open the package options:

Manage Content page

-	Selected it	em: Microsoft MicrosoftPowerBIDesktop	
	Selected It		
ackage Details	Publishing Task	Package Options	
Create Publishing task	Configure Package options		
Details			
Package name: Microsoft Microso	oftPowerBIDesktop		
Version:			
2.138.782.0			_
D -41-			
Patn:	Contont/win25/Mic	rosoft MicrosoftPowerRIDesktop 2,138,782,0, v64, 94	alayb3d8bb
((dco1.bwiab.ioca	I(content (winzo (win	105011.WICIOS011F0WeiDiDesktop_2.156.762.0_x046	rekyb5d6bbf
Full package nam	e:		
Microsoft.Microso	ftPowerBIDesktop_2	.138.782.0_x648wekyb3d8bbwe	
Dependencies:			
Microsoft.VCLibs.	120.00.UWPDesktop	Microsoft.VCLibs.140.00.UWPDesktop Microsoft.VC	Libs.110.00.
Dependency package	s can be placed in the D	ependencies folder next to the package, they will be deployed a	utomatically
Applications in th	is package		
Microsoft.Micro	- softPowerBIDesktop	#bin\pbidesktop.exe	1

Here you can find details about the App-V or MSIX package and also create a publishing task or configure package options for the selected package. You can also click on the publish and options button next to the package it will take you to the new publishing task or package options window immediately.

Creating a publishing task

MSIX (app attach):

		em. microsorciviic	05011-Ower DIDesk	аор	
ckage Details	Publishing Task	Package Optio	15		
Save publishing	Show existi	No. na publishina			
Task	tasks for t	his package			
elect publishing ty	rpe				
user publi 🕐 🖉	ish task ns automatically wh	en the publishing ta	k is removed		1
When the MSIX pac	kage is not alread	y staged on the ma	achine while execut	ting this task	
ᡖ 🔿 Stage the	e package			Skip the publish	task
ublishing details					
	oup:				
Select user gr				A Colora	
Select user gr				Select	
Select user gr				Select	
Select user gr Apply this pull	blishing task only t	o the following ma	chine group:	Select	
 Select user gr Apply this pul All Machine 	blishing task only t Groups	o the following ma	chine group:	v select	
Select user gr Apply this pul All Machine Execution pric 100	blishing task only t Groups vrity:	o the following ma When the user h Leave the app	ichine group: as an older versior lication running	of this application open:	
 Select user gr Apply this pul All Machine Execution pric 100 Publish a 	blishing task only t Groups Xrity: Pplications from th	o the following ma When the user h Leave the app Force the app is package as rem	ichine group: as an older versior lication running ication to close oteapp	of this application open:	
 Select user gr Apply this pul All Machine Execution pric 100 Publish a Auto star 	blishing task only t Groups rity: Pplications from th t applications from	o the following ma When the user h Leave the app Force the app is package as rem	achine group: as an older versior lication running (ication to close (steapp gin	of this application open:	

App-V:

	•		Selected iter	m: Proaz_3501.10	00		
blis	shing Task						
Sav	ve publishing Task	Show e tasks	xisting publishin for this package	ng :			
elec	ct publishing type						
w.	O User publish	task			R	G	obal publish task
0 U	Inpublish happens a	utomatically	when the publis	hina task is remov	ed		
-							
Vne	n the package doe	esn't exist o	in the machine v	while executing ti	his publish ta	ask	
-	O Add the pac	kage			٥	💮 Skip	p the publish task
-	Add the pac	kage			٥	🔵 Skip	p the publish task
a ubli	Add the pac	kage			0	🔵 Skij	p the publish task
ubli	Add the pace	kage x			٥	🔵 Skij	p the publish task
ubli 2	Add the pace	kage x			٥	🔵 Skip	p the publish task
ubli 28	Add the pace ishing details Select user group	kage x	file (LINC path):		0	Skip	p the publish task
∎ ubli ≫	Add the pao ishing details Select user group Dynamic user con	kage): nfiguration	file (UNC path):		C	Skip	P the publish task
eubli Se Se S	Add the pace Add the pace ishing details Select user group Dynamic user con None Annyc this public	kage n: nfiguration	file (UNC path):	ing maching are	0	Ski	the publish task
eubli Se Se Se Se Se Se Se Se Se Se Se Se Se	Add the pace ishing details Select user group Dynamic user cor None Apply this publis All Machine Group	kage nfiguration hing task o	file (UNC path): nly to the follow	ing machine gro	C) nup:) Skij	p the publish task
eubli Se	Add the pace ishing details Select user group Dynamic user cor None Apply this publis All Machine Gre	kage x higuration hing task o pups	file (UNC path): nly to the follow	ing machine gro	C) hup:	Skip	p the publish task
eubli Se Se Se Se Se Se Se Se Se Se Se Se Se	Add the pace shing details Select user group Dynamic user cor None Apply this publis All Machine Gre Execution priority	kage x nfiguration hing task o bups r	file (UNC path): nly to the follow	ing machine gro ublish this packa	up: ge at login	 Skip Skip Skip 	p the publish task
eubli Se Se Se Se Se Se Se Se Se Se Se Se Se	Add the pace ishing details Select user group Dynamic user con None Apply this publis All Machine Gro Execution priority 100	kage r: hing task o hing tas	file (UNC path): nly to the follow Always pr Publish tl	ing machine gro ublish this packa	up: ge at login sally for this I	Skip	p the publish task
eubli S S S S S S S S S S S S S S S S S S S	Add the paolishing details Select user group Dynamic user cor None Apply this publis All Machine Grr Execution priority 100 Publish appl	kage r: figuration hing task o bups r: @ ications from ications from	file (UNC path): nly to the follow Always pr Publish tl m this package.	ing machine gro ublish this packa his package glob	up: ge at login hally for this i	Skij	p the publish task
eubli Se Vubli	Add the paolishing details Select user group Dynamic user cor None Apply this publis All Machine Gro Execution priority 100 Publish appl	kage infiguration hing task o pups r o kations fro h t t t t t t t t t t t t	file (UNC path): nly to the follow Always pr Publish th m this package	ing machine gro ublish this packa his package glob as remoteapp	up: ge at login hally for this r	Skij	p the publish task

When creating a publishing task, you can configure various options to suit your needs. Most options are straightforward. For instance, you can set the package to be published globally (making it available to everyone on the machine, applicable to App-V only) or restrict it to specific user groups (supported by both App-V and MSIX).

Unpublish tasks are unnecessary, as deployment is fully automated. Removing a publishing task will automatically unpublish the package for the user or machine.

You can define actions for cases where the package is missing during task execution. Options include dynamically adding the package or skipping the task altogether.

Using the machine group filter, you can restrict task execution to specific machine groups. By default, tasks apply to all machine groups.

Execution priority lets you control the order in which tasks are executed. Lower values indicate higher priority, which is useful if certain packages need to be published before others.

The agent checks for already-published packages and skips redundant tasks. However, the "Always publish this package even when already published" option overrides this behavior, ensuring the package is always published. Use this setting only if necessary, such as when dealing with profile solution issues (not typically required if the entire profile is maintained at logoff).

Some App-V packages, like Adobe Acrobat, must be published globally and do not support per-user publishing. The "Publish this package globally for this user group" setting allows the agent to globally publish packages based on user groups when required.

Desktop and Seamless application scenario

AppVentiX supports full desktop and seamless application publishing scenarios. Full desktop doesn't need any additional configuration, just create and save the publishing task. For seamless application publishing all you have to do is check the "Publish as remoteapp" checkbox. The window will be extended:

Publishing task Select publishing type Select publishing type Select publishing type Image: Computer the publishing type Select publishing type Select publishing type Image: Computer the publishing the	*		Selected	item: Proa	z_3501.100					\times
Select applications from this package which you want to publish as remotapp Select applications from this package which you want to publish as remotapp Select applications from this package which you want to publish as remotapp Select applications from this package which you want to publish as remotapp When the package doesn't exist on the machine while executing this publish task Publishing details Publishing details Publishing task only to the following machine group: Image: Machine Groups Select applications from this package at login Select appl	Publishing Task									
Select publishing type Select publish task Implication from this package which you want to publish as remoteapp Implications from this package which you want to publish as remoteapp Implications from this package which you want to publish as remoteapp Implications from this package which you want to publish as remoteapp Implications from this package which you want to publish as remoteapp Implications from this package which you want to publish as remoteapp Implications from this package which you want to publish as remoteapp Implications from this package as remoteapp Implications from this package as remoteapp Implications from this package as togin	Save publishing Task	Show existing publishing tasks for this package								^
Solution priority: Al Mays publish this package as remoteapp O Auto start applications from this package as remoteapp	Select publishing type	2		Select	t applications from this pa	ackage which you want to p	publish as remoteapp			
 Unpublish happens automatically when the publishing task is removed When the package doesn't exist on the machine while executing this publish task Publishing details Publishing details Publishing details Publishing user configuration file (UNC path): None Popymanic user configuration file (UNC path): None Publish this package at login Browse Publish this package at login 	🐸 🔘 User publish	task	🗟 🔵 Global publish task		Application		Argument (Optional)	lcon	Сору	
When the package doesn't exist on the machine while executing this publish task Publishing details Publishing details Select Dynamic user configuration file (UNC path): None Publishing details Publishing details If (Common Programs!)/USOFT Nederland B.VAProazReportViewer/ProazReportVi	 Unpublish happens 	automatically when the publishing ta	sk is removed	0	3 I	~				
	When the package do When the package do Add the po Publishing details Select user grou Dynamic user co None Apply this publi All Machine Go Eucurion priori 100 O Publish app C Auto start do	esen't exist on the machine while e ckage ip: onfiguration file (UNC path): shing task only to the following m rooups by: Publish this package as rem applications from this package at le	executing this publish task		[[Common Programs]] [[Common Start Menu [[AppVPackageRoot]] [[AppVPackageRoot]] [C powershell.exe Ir cmd.exe Ir cmd.exe You can retrieve an applic	JUSOFT Nederland B.V.Pro JJ.PROAZ.Ink Proaz.exe ReportViewer\ProazRepor	azReportViewer\ProazReport	Viewer.Ink	I + - ^ L able for th	ne

Now you can select the application you want to publish, or configure a powershell or cmd script to run. Scripts can run inside or outside the virtual environment.

When you click on the copy button next to the selected application the command to publish the application is copied to your clipboard, just paste this command in your seamless application delivery solution (RDS, Citrix, VMware, etc).

There is also a direct integration with Azure Virtual Desktop (AVD), this integration will publish the application directly in AVD, and also remove the application when the publishing task is removed. You can read more about this integration later in this guide.

Note:

In full desktop scenarios the publish as remoteapp checkbox is not needed.

Auto start applications

Selected it	em: Proaz_3501.100	×			
Publishing Task					
Save publicing Lask Pone existing sublishing tasks for this package					
Select publishing type	Select applications from this package which you want to	auto start			
O User publish task Global publish task Urqublish task is removed	Application	Argument (Optional)			
When the package clean it exist on the nucline while executing this publish task C Add the package C Skip the publish task Publishing densis Select user group: A Select	[[Seemon Program@IGCT Netherland (IV/Insu/Rport/Sear/Bport/Sear/Bport/Sear-Isk [[Germon Stat Merg]/IVID/Lik [[Apy/WolageRoot[]/IVID/Lik [] [Apy/WolageRoot[]/Ivia:ee [] [Apy/WolageRoot[]/ivia:ee [] Merginal Search (Ivia:ee) [] [Apy/WolageRoot[]/ivia:ee [] Merginal Search (Ivia:ee) [] [Apy/WolageRoot[]/ivia:ee [] [Apy/Wola				
Vynamic user configuration file (UNC part): None Vanie Apply this publishing lask only to the following mechine group: All Michine Groups					
feedfor priority:					
bilishing Task Id:		c8e3db4t-1at9-4ta3-a736-89btda3tc			

With auto start applications you can select applications from the package that should be auto started for the user. The selected application(s) will be started automatically when the user logs in.

Configure package options

When you click on configure package options, you will see the following window:

-		×
Package Options		
Save package options	Show configured package options for this package	^
Options		
🥒 📃 Drain (r	emove) this package	

When you enable drain for a package, the agent will remove the package and prevent it from deploying again. Make sure that the enable drain feature is enabled in the agent settings (default). When there are publishing tasks configured for the package, they will be removed automatically.

Pre-stage registry (only applicable for App-V): use this option for very large packages, when enabled the agent will start the virtual environment of the package one time after it's deployed. This will increase the initial launch time of the application.

Machine group filter: You can filter on which machine group the configured package options should apply.

After stage actions



With after stage actions you can provide commands which are executed after the package has been staged on the machine.

For example when importing Microsoft Teams from the Import from Microsoft Store window, the following after stage action is configured automatically to install the Teams Office Addin:

msiexec.exe /i "C:\Program

Files\WindowsApps\MSTeams_24004.1309.2689.2246_x64__8wekyb3d8bbwe\MicrosoftTeamsMee tingAddinInstaller.msi" ALLUSERS=1 /qn /norestart TARGETDIR="C:\Program Files (x86)\Microsoft\TeamsMeetingAddin";REG Add HKLM\SOFTWARE\Microsoft\Teams /v disableAutoUpdate /t REG_DWORD /d 1 /f

You can separate multiple command with the ; character. Make sure to include quotes where necessary.

Show publishing tasks and Package Options

On the inventory content window, you will find two buttons:



When you click on Show publishing tasks you will see an overview of all publishing tasks. You can filter and sort the tasks, edit the tasks or delete the tasks.

The same goes for the package options, when you click on the Show Package options button you will see all configured package options.

In the selected items ribbon menu you will find different actions for selected items (depending on what package types are found in the inventory).



For example, you can create App-V connection groups by selecting specific packages or editing existing groups. Additionally, you can create MSIX shared containers directly from this page.

From the content page, you also have the option to convert App-V packages to MSIX, enabling a smooth migration at your own pace. Managing App-V and MSIX side by side is straightforward and efficient.

Please note you need a code sign certificate to sign MSIX packages, this certificate can be obtained from an internal or external Certificate Authority like Sectigo, or you can create one using the Central View console. When you create a certificate in Central View it will automatically be deployed to the machines so packages signed with this certificate are automatically trusted. More information about certificates can be found on page 30.

MSIX and MSIX app attach

With AppVentiX you can deploy normal MSIX packages and MSIX packages in a virtual disk format (called app attach mechanism). When you want to save disk space you can convert a MSIX package to app attach. This process will create an image file (VHD\VHDX or CIM) containing the extracted MSIX package. This image will be attached by the AppVentiX agent so the application can be published to users. This delivery mechanism has the advantage that no disk space is used on the agent, but please note you can also just deploy MSIX packages without app attach, they will be cached on the hard disk of the machine instead of remotely attached. You can also combine to two delivery methods. After the package is converted to app attach it will be visible in the content inventory where you can publish it to a user group, the original MSIX package is stored in the backup folder and can be found there in case you need it for example to update the application. Because the original MSIX package is placed in a folder named backup the agent will not process\precache the original package.

Converting to app attach doesn't need any prerequisites, the convert process can run on Server OS (2022 or higher) and Client OS (Win 10 20H2 or higher or Win11). When you want to convert to CIM format, please note you need Win10 20H2 or higher, also please run the Central View console as admin to make sure the convert process runs smoothly.

	App attach disk options	×
Continue		
Please select	the MSIX app attach disk type ttach disk options	
○ VHD ● VHDX ○ CIM	 ⑦ Dynamic disk size ⑦ V Automatically determine disk size 0 	

The convert to app attach feature supports different options when creating the app attach disk, all disk options are supported (VHD, VHDX & CIM), you can choose dynamic disk size or a fixed disk size, the disk size is by default automatically determined according to the size of the MSIX package, but you can also configure the disk size manually.

After converting a MSIX package to app attach it will be visible in the content inventory and you can publish it for users just like a normal MSIX package.

The AppVentiX agent takes care of all the actions needed for MSIX app attach (staging, de-staging, attach\detaching). It contains intelligent decisions and keeps track of the disks attached to the agent.

MSIX and app attach packages can be deployed and published to users even when they are not deployed\attached yet on the machine (on the fly delivery), making it a real dynamic delivery mechanism.

By default the registration for MSIX packages will be removed when the user logs off, this is done by the AppVentiX LogOff Handler (when persist MSIX app data agent setting is enabled). This process is needed when used in combination with FSlogix profile management and you want to roam the application data of the package between sessions. When you roam the profile of the user the persist MSIX app data setting is needed (enabled by default), when you have persistent machines per user (laptops etc) you can disable this setting. AppVentiX will take care of the whole process and supports both situations where the profile is roaming and non-roaming. Old (versions) of packages that you remove from the content share(s) will be removed from the agents automatically, making it a fully managed deployment solution.

MSIX Shared containers

MSIX Shared Containers are similar to App-V Connection groups, packages in a shared container will form one container so they can access each other's files and registry settings.



When you select multiple MSIX packages you can click on the "Create shared container", after you save the shared container it will be visible in the content inventory. You can then assign it to a user group and it will be enabled for the user automatically at the next refresh cycle or login.

Please note that MSIX shared containers are only supported on Windows 10 Build 22x and higher and the current implementation of shared containers requires (local) admin permissions to apply the container.

MSIX Certificate management and deployment

Requesting 3th party certificates for signing MSIX packages is time consuming and costly. With AppVentiX it is now very easy to create your own certificate directly from the console. The certificate will be deployed to the machines automatically making it a very easy and quick method to sign and deploy MSIX packages.

 \times



MSIX Deployment

Create Self Signed Certificate		-
Generate and save certificate		
Certificate Details		
riendly Publisher name:	Publisher name:	
PrivateSigning	CN=PrivateForMyCorp	
Password:	Validity period:	•
•••••	5-Year V	
\\dc01.bwlab.local\content\win25	~	
	(used to sight the MSIX packages in the packaging tool).	
Install the certificate in the person	ai certificate store	
Please note the following:		
This wizard creates a PFX file which yo	u can use to sign your MSIX packages in the MSIX packaging tool	
This wizard creates a CER file which w In the MSIX packaging tool select PEX	If be placed in the selected content share, the certificate will be deplo	yed to the machines automatically file and password in a save place
In the MSIX packaging tool you can p	ovide a timestamp server, this will make sure the package can be dep	ployed even when the certificate has e

The certificate is stored as PFX and imported in the personal certificate store so it can be easily selected when converting packages from App-V to MSIX for example.

The .CER file will be stored on the content share you select and will be deployed to the machines automatically. The certificate is also visible in the content overview:

1	Content Share	Actions		Content Share	•									Q
2	\\bwlabacc.file.core.windows.net\applica	۰ 🖆	•			Туре 🔺	Name	Version	Act	ions	Publisher	Disk Type	Last Updat.	
2	\\dc01\content\lab	ø 🞽		4 🗌 🝰 \\dc	01\content\lab	,							Count=1	1 *
					🎒 MSIX	AppAttach	CitrixXenCenter	8.2.2.0	Fublish	Doptions	CN=AppV	VHDX	4/22/2021	
					í MSIX	AppAttach	Unit4ReportManager	1.0.0.0	😽 Publish	Doptions	CN=AppV	VHDX	7/21/2021	
					í MSIX	AppAttach	PostMan	1.0.0.0	😽 Publish	Detions	CN=AppV	CIM	4/22/2021	
					🗰 APPMASK	Assignment	Project2016.fxa						4/9/2021	
					🧕 MSIX	Certificate	MyCompany.cer						7/21/2021	
					릚 APPV	Group	CG_DWGSee Pro 2016_Fi		😽 Publish	Doptions			6/8/2021	
					🥥 appv	Package	Firefox ESR 52.7.1	0.0.0.1	ᡖ Publish	Doptions			3/16/2018	
					🥥 APPV	Package	DWGSee Pro 2016	0.0.0.1	ᡖ Publish	Doptions			1/19/2018	
					🍵 MSIX	Package	WinSCP	1.0.0.0	Publish	Doptions	CN=AppV		7/9/2020	
					H APPMASK	Rule Set	Project2016.fxr						7/20/2021	
					SIX MSIX	Sharedcontainer	SC_PostMan_NotepadPlus		🔁 Publish	Detions			7/21/2021	

Application overview

The default page in Central View is the applications page:

Applications	Manag	e Content Manage M	achines C	Configuration a	nd Activity				
R efresh Applications		Group Applications by:	Create Package	Edit Package	Import from Microsoft Store	Import from AppVentiX	All Publishing Tasks	Show all columns	
Refresh			Act	tions	Impo	ort	Show	View	
Package ^	Package ^								
		Application Name						^	Startmenu Folder
		R D C							10:
🔺 📃 🗾 Арр	ApplicationRefresh - 2.3.2.0 😫 Publish								
	Application Refresh Root								
4 📄 🎯 App	A 🔰 🤪 ApplicationRefresh - 0.0.0.2 🏼 🖓 Publish 🔒 Show								
	\sim	Application Refresh							[{Programs}]
	\sim	Application Refresh							[{Common Programs}]
🔺 📄 🎯 Arch	ni_530.1	100 - 0.0.0.1			😤 Publi	ish 🔒 Show			
	٢	Archi							[{Common Programs}]\Archi
		Docs							[{Common Programs}]\Archi
🔺 📄 🤞 Mice	rosoft.!	MicrosoftPowerBIDeskto	p - 2.138.782	2.0	😤 Publi	ish			
	Image: Power BI Desktop Root								
🔺 📄 🧼 Proa	az_3501	.100 - 0.0.0.1			😤 Publi	ish			
	٥ [ز	PROAZ							[{Common Start Menu}]
) ,	ProazReportViewer							[{Common Programs}]\iSOFT Nederland B.V\ProazReportViewer

This section provides an overview of all applications within your packages. You can easily create new packages or edit existing ones from here.

When creating new packages, you can manage shortcuts, include custom files, add scripts, and more, giving you complete control over your package configurations.

FSlogix App Masking management

The software compatibility with App-V and MSIX is very high but there are situations where you need to install software onto your machines without using App-V or MSIX. With FSlogix App Masking you can configure which user group(s) can see the application and which not (by hiding files and registry items). With AppVentiX it is now easy to centrally manage FSlogix App Masking rules and assignments. Just place them on the content share and they will be deployed to the machines automatically. Also rules and assignments you remove from the content share will be automatically removed from the machines. You can modify the App Mask rules and assignments directly from the Central View console, rules are automatically updated on the machines, using the Last Updated time in the machine inventory you can clearly see which rule set and assignments are active. Java rule sets are also supported, the project file and generated rule set needs to have the same filename (before the extension) and placed in the same directory.

🗣 App	VentiX Central	View 3.2.24 🔻												-	٥	×
Manag	je Machines	Manage Content	Configu	ation and Ac	tivity							P	Community L	icense (5 Mac	hines)
Manage	😂 Refresh s	elected machine group	•	() Machine	Ser User	Process	Invoke	Remove r	ule	Show hidden columns	Select acti	ve feature: SK 💌				
Groups	Conly sho	w online machines		Inventory	Inventory Machine	Inventory Group action	Refresh Cycle	from mach Selected Iten	hine n actions	View	Active	Feature				^
Mach	iine Name 🔺	Machine Actions		Machine	*											Q
🖵 WIN	0-20H2-01	🚿 👺 🗳 🔕			1	Туре			Name		^	Last Upda	ited			
WIN	0-20H2-02	🧭 👺 🦨 💿		C	WIN10-2	0H2-01									Cour	nt=2 📩
				[Assignment			Project20	016.fxa		4/9/2021	11:08 AM			
						Rule Set			Project20)16.fxr		7/20/2021	1 3:59 PM			
				C	WIN10-2	0H2-02									Cour	nt=2
						Assignment			Project20	16.fxa		4/9/2021	11:08 AM			
					💮 F	Rule Set			Project20	016.fxr		7/20/2021	1 3:59 PM			

Import packages



With the import packages buttons you can directly import MSIX packages from the Windows store, for example PowerBI, Whatsapp, Whiteboard, the MSIX packaging tool, etc.

Import from AppVentiX will allow you to import packages created by AppVentiX, for example a test package to test your deployment and also a refresh application which allows you to publish an icon in the users startmenu that will initiate a refresh. This allows users to initiate a refresh themselves without having to logoff\login and without running a refresh cycle remotely or by timer.



Configuration and Activity page

On this page you will find all activities from the Central View console, you can also change the Central View console configuration here or apply a different theme to the console.

 Appvento 	Central view 5.	2.24 🗸							
Manage Ma	chines Ma	nage Content	Configuration and	Activity					
*			•						
Settings	Change theme 🕶	Clear backgroun tasks	d Release notes						
Configuration	Layout	Activity	Website						
Inventory WIN10-20H2-01 [12:11 PM] Completed									
Bemoving Completed	Removing selected item(s) from machine WIN10-20H2-01 [12:21 PM] Completed								
Inventory	WIN10-20H2-0	1 [12:21 PM]							
Completed				1					
Inventory	WIN10-20H2-0	1 [2:43 PM]							
Completed									
Inventory	WIN10-20H2-0	1 [2:43 PM]							
Completed)					
Inventory	WIN10-20H2-0	2 [3:10 PM]							
Completed									
🍇 User inven	tory WIN10-20	H2-01 [3:21 PM]							
Completed									
Sompleted	Ser inventory WIN10-20H2-02 [3:21 PM] Completed								



A PowerShell module is available to automate the creation of publishing tasks. With above button you can install the module on the same machine as where Central View is installed. You can also install the module from the PowerShell gallery with below command:

Install-Module -Name AppVentiX

The configuration share will be automatically detected when the module runs on the same machine as Central View, if the module runs on another machine you can set the configuration share with below command:

Set-AppVentiXConfigShare -ConfigShare "\\path\appventix\config"

By invoking below command you will get examples how to use the module:

Get-Help New-AppVentiXPublishingTask -Examples Get-Help Get-AppVentiXPublishingTask -Examples

Mandatory variables are: Type (MSIX\APPV), Group (the groupname) and Path (location to the package)

Firewall \ communication ports used by AppVentiX

By default AppVentiX doesn't use any other ports other then file share (SMB) access (445). There are a few exceptions:

- For AD domain connections (to retrieve user groups) port 389 (Idap) or 636 (Idaps) is used
- For Entra ID connections and Azure Virtual Desktop (AVD) connections the default Graph API ports (443) are used to Online Microsoft services
- When importing packages from the Microsoft store, the store URL needs to be accessible

In Active Directory (AD) domain environments, the AD connection is most of the time already possible because a lot of authentication traffic is directed to domain controllers. AppVentiX will make use of this default AD integration already known in the operating system.

Limit access to the Central View console

You can configure an Active Directory group or Azure AD group that will have access to the Central View console. When a user starts the console the group membership is checked, when the user is not member of the configured group access to the console is not allowed.

Г	- Central View access
	$ec $ Only allow a specific usergroup to access the Central View console $\ {f 2}$
	Configured group:
	Azure AD Group AppVentiX;9941bfa8-c7a4-4274-9f68-fae24f03552a

Azure Virtual Desktop (AVD) integration

AppVentiX supports both Desktop and RemoteApp scenarios. For AVD there is a direct integration available, you can enable this in the Central View settings:

Integrations			
🗹 Enable Azure AD (Entra ID) inte	egration ?	☑ Use AppVentiX Azure Application Registration	?
☑ Enable Azure Virtual Desktop ((AVD) integration (
Select the active subscription for	AVD:		
Pay-As-You-Go Dev/Test	-		
Update Azure Module	Status: Installed (4.0.0 + 2.0.2.180)		
Sisconnect from Azure	Status: Connected		

Configuration is simple: Click on install AVD module and wait for the process to finish (this can take a few minutes), after installation click on connect to AVD and provide your credentials in the login box.

When the integration is enabled, you can select applications from an App-V, MSIX and\or MSIX app attach package and select an Application Group in AVD to publish the application to:

Publishing Task							
Save publishing Task Show existing publishing tasks for this package	^						
Select publishing type	Select applications from this package which you want to publish as remoteapp						
3 O User publish task	Seamless application Friendly Name Argument (Optional) Icon						
Unpublish happens automatically when the publishing task is removed When the MSIX package is not already staged on the machine while executing this task	AppriestApplication(lestApplic > Test Application S						
Skip the publish task							
Publishing details	■ ₩						
Select user group:	After you click on save publishing task, the applications will be published in the selected AVD application group. When you remove the publishing task the applications will be removed from the application group automatically. Instead of selecting an application from the package, you can also manually enter an application or script.						
Apply this publishing task only to the following machine group:	Select the AVD application group where you want to publish the applications						
All Machine Groups	AVD application group:						
Execution priority:	Finance V Treate new application group						
Force the application to close 3	Active subscription: 67d17588-6e76-4a1e-8740-cf7d78391f83 (23 application groups found)						
🗇 🗹 Publish as seamless application (not needed when using desktop)	2 Change subscription						

You can also create a new AVD application group directly from AppVentiX, you can also switch the active subscription and tenant if you have multiple AVD environments to manage.

When you save the publishing task, the applications are published in AVD and are accessible by the user, the AppVentiX wrapper will take care that the application is available for the user before it is started. It's also possible to launch powershell or cmd scripts.

It is also possible to edit a publishing task (like the group or application description), the applications will be updated in AVD automatically. When you remove a publishing task, the applications are automatically removed from AVD, making it a fully managed integration which is easy to use and provides complete control and insight from one single point of management.

The manage content page in the Central View console also includes a Remote App overview button:



This will give you a total overview of all published applications in AVD, you can sort on application group, user group assignment and application name. This will provide you complete insight in one overview.

BuiltInRole

To manage application groups in AVD, you need at least contributor permissions in AVD:

Desktop Virtualization Application Group Contributor Contributor of the Desktop Virtualization Application Group.

Azure AD (Entra ID) integration

After you enabled the Entra ID integration in the Central View setting you have the option to use the AppVentiX Azure application registration or provide your own application registration. This is only used by the agent, not the Central View console. The Central View console uses the account you select to authenticate to Entra ID.

It's not needed to configure and provide secrets for AppVentiX, a basic application registration is enough for AppVentiX because AppVentiX will not connect to Entra ID by itself but instead uses the access token from the user using MSAL. This makes the solution secure because the secrets doesn't have to be stored by AppVentiX.

Integrations	
☑ Enable Azure AD (Entra ID) integration ?	Use AppVentiX Azure Application Registration ?
Enable Azure Virtual Desktop (AVD) integration ?	Tenant ID: Application ID:

For Central View to be able to retrieve user groups and devices from Entra ID, the following Graph permissions needs to be assigned to the account you use to login to Entra ID:

- Device.Read.All
- Group.Read.All
- GroupMember.Read.All

When you use the AppVentiX Azure Application registration:

The user will see a consent window after login, the only permissions requested are user.read to retrieve the group membership of the user. Recommended is to let an admin perform a consent one time (with the below checkbox checked) so users will not see the consent window at all.

Consent on behalf of your organization

When you configure your own Azure Application registration:

Create a new application registration in the Azure portal and give it a name like AppVentiX.

Supported account types Who can use this application or access this API? Accounts in this organizational directory only (only - Single tenant)

Choose this organization only.

You can enter the redirect url's later, click on save.

Go to the authentication menu in the application registration you just created.

Click on add platform and choose mobile and desktop applications.

Mobile and desktop applications Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

Enable the checkboxes and add one more redirect uri:

ms-appx-web://microsoft.aad.brokerplugin/aca5eaeb-ae60-4f0f-af22-32592d20910a

(replace the application id with your application id which can be found in the overview menu). The end result looks like this:

Mobile and desktop applications Redirect URIs	Quickstart	Docs 🖓	Ŵ
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and	The redirect their restriction	URI you ser ons _[才	nd in
 https://login.microsoftonline.com/common/oauth2/nativeclient https://login.live.com/oauth20_desktop.srf (LiveSDK) 			
msalaca5eaeb-ae60-4f0f-af22-32592d20910a://auth (MSAL only)			
ms-appx-web://microsoft.aad.brokerplugin/aca5eaeb-ae60-4f0f-af22-32592d20910a		\checkmark	

Now go to the API permissions tab, the user.read permission should be already configured by default, if not add the user.read permission (more permissions are not needed!)

Configured permissions						
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the conse II the permissions the application needs. Learn more about permissions and consent						
+ Add a permission 🗸 Grant admin consent for						
API / Permissions name	Туре	Description	Grant admin consent for			
∽Microsoft Graph (1)						
User.Read	Delegated	Sign in and read user	profile			

Click on Grant admin consent, so users are not prompted with the consent window.

Now go to the overview menu for the application registration and copy the application and tentant id:

∧ Essentials				
Display name		Client credentials	: Add a certificate or secret	
Application (client) ID	: aca5eaeb-ae60-4f0f-af22-32592d20910a	Redirect URIs	: <u>0 web, 0 spa, 4 public client</u>	
Object ID	: 6adfc1ab-a391-4366-8fde-fc87b189709a	Application ID URI	: Add an Application ID URI	
Directory (tenant) ID	: b17b9be0-6a05-42ef-af6c-/	Managed application in I	: <u>AppVentiX test</u>	
Supported account types : <u>My organization only</u>				

Paste them in the Central View settings window:

🗹 Enable Azure AD (Entra ID) integration 🛛 😮	Use AppVentiX Azure Application Registration ?
Enable Azure Virtual Desktop (AVD) integration	Tenant ID: b17b9be0-6a05-42ef-af6c-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
	Application ID: aca5eaeb-ae60-4f0f-af22-32592d20910a
Update Azure Module Status: Installed (4.0.0 + 2.0.2.180)	

You are now finished, click on save.

Advanced Azure AD settings

There are some advanced Azure AD settings that can be configured, you only have to configure them when needed:

Advanced Azure AD settings (only modify when needed)
Do not try to perform SSO when retrieving machines and user groups ?
Disable Windows token broker integration ?
□ Show authentication progress to user ?
Enable fall-back method for Azure AD authentication

By default SSO will be used in the Central View console to retrieve machines and user groups, if you don't want to use SSO you can enable this setting.

The second checkbox is to disable the Windows token broker integration (WAM), in newer operating systems (Win10\11) the integrated authentication broker will be used by default. For Azure AD joined VMs this will work out of the box and normally you don't want to disable this.

Normally the authentication and Azure AD group retrieval happens silently in the background, with the "Show authentication progress to user" option the progress will always be shown to the user. This can be used for testing, but is normally not needed to enable.

Enable fall-back method for Azure AD authentication will use older Azure AD integration, only enable this option when MSAL can't be used.

Logging:

When a user sees a popup to consent or authenticate, the silent authentication did not work. You can find more information in the log file which is stored in the users profile:

C:\Users\username\AppData\Roaming\AppVentiX

AppVentiXLogonHandlerLog.txt

Hybrid Azure AD joined machines

For machines that are both Active directory integrated and Azure AD integrated (hybrid joined), use the machine groups based on AD group or OU.

Only use the Azure AD machine group for Azure AD (only) joined machines.

Azure AD joined (only) machines are not member of an Active Directory domain.

Azure AD joined (only) machines

Machines that are only joined to Azure AD, can be configured with an Azure file share which is standalone (not AD integrated). For this you can provide the storageaccount name and access key, please find more information in the Azure File share configuration section below.

Azure file share configuration

AppVentiX supports Azure file shares that are AD integrated and\or stand-alone shares.

Using stand-alone Azure file shares (for example for Azure AD joined machines):

In the Azure portal go to Storage Accounts and click on create storage account:



No storage accounts to display

Create a storage account to store up to 500TB of data in the cloud. Use a general-purpose storage account to store object data, use a NoSQL data store, define and use queues for message processing, and set up file shares in the cloud. Use the Blob storage account and the hot or cool access tiers to optimize your costs based on how frequently your object data is accessed.

Create storage account

Give the storage account a name and selection your region:

Project details

Region (i) *

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *	Azure subscription 1	
Resource group *	(New) StorageAccounts	
Instance details		
Storage account name ① *	appventixstorageaccount]

 \sim

You can leave all settings default and click on create. Optionally you can fine tune the storage account to meet your needs, but the default settings are already enough.

(Europe) West Europe

After the storage account is created we are going to create the file share. Go to the storage account and click on file shares:

	Properties Monitoring Capabilit	ties (7) Recommendations (0)	Tutorials Tools + SDKs	
Overview			0.6.1	
Activity log	Blob service		Security	
🖉 Tags	Hierarchical namespace	Disabled	Require secure transfer for REST API operations	Enabled
 Diagnose and solve problems 	Default access tier	Hot	Storage account key access	Fnabled
 Diagnose and solve problems 	Blob anonymous access	Disabled	Minimum TLC unraine	Vanian 1.0
Access Control (IAM)	Blob soft delete	Enabled (7 days)	Winimum TLS Version	version 1.2
Y Data migration	Container soft delete	Enabled (7 days)	Infrastructure encryption	Disabled
🗲 Events	Versioning	Disabled	Networking	
Storage browser	Change feed	Disabled	Allow access from	All networks
Storage Mover	NFS v3	Disabled	Number of private endpoint connection	5 0
	Allow cross-tenant replication	Disabled	Network routing	Microsoft network routin
Data storage	1 m 1		Access for trusted Microsoft services	Yes
Containers	File service		Endpoint two	Standard
File shares	Large file share	Disabled	Endpoint type	Standard
Quarter	Active Directory	Not configured		
Queues	Default share-level permissions	Disabled		
Tables	Soft delete	Enabled (7 days)		
		at and as		

+ File share 🕐 Refresh			
File share			
Active Directory (SMB): Not configured	Default share-level permissions: Disabled	Soft delete: 7 days	Maximum capacity: 5 TiB
Security: Maximum compatibility			

We will select the default tier and settings, they have been tested to work and perform well with AppVentiX. Optionally you can decide to pick a higher or lower tier, you can always change the tier later.

Basics	Backup	Review + create	
Name *			appventixshare
Tier *			Transaction optimized \checkmark
Perform	nance		
Maximu	m IO/s 🕕		1000
Maximu	m capacity		5 TiB
Large fil	e shares		Disabled

Click on create to create the file share. After the file share is created, click on Browse and then Add directory:

appventixshare Bro	owse
	Ø Connect ↑ Upload + Add directory ひ Refresh
dverview	Authentication method: Access key (Switch to Add directory A
Diagnose and solve problems	\wp Search files by prefix
Access Control (IAM)	Name
Browse	No files found.
Operations	

Create 2 folders (config and content):

🖉 Connect Upload 🕂 Add directory	
Authentication method: Access key (Switch to A	λz
${\cal P}$ Search files by prefix	_
Name	
Config	
Content	

Go to the storage account main menu and click on Access keys:

1	appventixstorag Storage account	eaccount Access keys ★ ··	
۶	Search	≪ (S Set rotation reminder () Refresh 🔗 Give feedback	
	Overview		
-	Activity log	Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure le Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using t	ocation the oth
0	Tags	Remember to update the keys with any Azure resources and apps that use this storage account.	
×	Diagnose and solve problems	Learn more about managing storage account access keys 🗹	
ጽ	Access Control (IAM)	Storage account name	
r	Data migration	appventixstorageaccount	
۶	Events	keyt () Potete key	
-	Storage browser	Last rotated: 10/4/2023 (0 days ago)	
•	Storage Mover	Key	
Da	ta storage	Show	
_	Containers	Connection string	
-	Containers	Show	J
-	File shares	kev2 🖒 Rotate key	
	Queues	Last rotated 10/4/2023 (0 days ago)	
100	Tables	Key	
Se	curity + networking	Show	J
۲	Networking	Connection string	
2	Front Door and CDN	Show	
-	From Door and CDIN		
•	Access keys		

From here copy the storage account name and the access key, now go to the Central View settings page.

Enter the file share you just created in the below format (note the config folder at the end):

\\appventixstorageaccount.file.core.windows.net\appventixshare\config

(Replace the storage account name and share name with the one you just created)

Clear the checkbox and copy the storage account name in the username textbox, make sure to use localhost\storageaccountname.

In the password field paste the access key.

Example:

Please enter the				
\\appventixstora				
Use integrated windows authentication for share access (?)			 Share permissions 	
Username:	localhost\appventixconfig	3		
Password:	•••••			

Save the settings, if the settings are saved successfully it means the share is accessible and configured correctly.

The content folder which you have created in the previous step, can be used in the machine group configuration:

Select machine group:	•	Ξ.	a 🕹	
My Azure AD 🔹	Add new Machine Group ▼	Remove selected Machine Group	Configure Agent for selected Machine Group	e
	Acti	ions	Configuration	
Machine Group: Azure AD Friendly Name: My Azure AD	location in AD when	e the machines in th	ie Hostpool are located)	
Content share(s) used by this group:				
\\appventixconfig.file.core.windows.net\	appventixconfigshare ^v	content	Enable pre-cache	

This is the location where you can store the App-V, MSIX (app attach) and\or FSlogix app masking rules on. In the manage content page you can browse to the share and upload content.

Using Azure file shares that are AD integrated:

Use an existing file share or create an Azure file share just like in the previous steps, then join the share to Active Directory:



(note you can also use Azure AD Kerberos integrated, but the steps to configure the share in AppVentiX will be the same as the stand-alone share configuration).

After you completed the steps to integrate the share with your Active Directory, you have 2 options to authenticate to the share:

1: Create a group and add the machine accounts to the group, give this group read permissions:

Home > saceuwfiles > saceuw-appl01				
Saceuw-appl01 Acc	ess Control (IAM)			
P Search (Ctrl+/) ≪	$+$ Add \downarrow Download role assignments \equiv	🗄 Edit columns 🕐 Refresh 🛛 🗙 Rem	iove 🛛 🛇 Got feedback?	
a Overview	10	2000		
R Access Control (IAM)				
Settings	Search by name or email Type : All	Role : All Scope : All scopes	Group by : Role	
Properties	4 items (1 Users, 2 Groups, 1 Service Principals)			
Operations	Name	Туре	Role	Scope
🖄 Snapshots	Reader and Data Access			
🔗 Backup	Microsoft.StorageSync	App	Reader and Data Access ①	Parent resource (Inherited)
	Storage File Data SMB Share Elevated Contrib	utor		
	LAB_PER_AZUREFILES_saceuwfiles	Group	Storage File Data SMB Share Elevated C	Parent resource (Inherited)
	Storage File Data SMB Share Reader			
	LAB_PER_AZUREFILES_saceuwfiles	Group	Storage File Data SMB Share Reader 🛈	Parent resource (Inherited)

Make sure this group has read\write permissions in the inventory folder on the configuration share or else the remote inventory will not work. You can leave the integrated authentication checkbox enabled.

2: Create a service account and give this user account read\write permissions on the share



Then enter this account in the Central View settings window:

Please enter the central configuration share (UNC):						
\\appventixsharedomainintegrated.file.core.windows.net\appventixshare\config						
🗌 Use integra	ted windows authentication for share access 🛛 😮)	(i) Share permissions			
Username:	domain\svc-appventix	?				
Password:	•••••					

Advanced configurations

AppVentiX should work out of the box with default settings, but every environment has different requirements and characteristics. AppVentiX can be customized to adjust to those requirements.

Share permissions and share configuration

AppVentiX supports **Windows file shares (both direct and DFS), Azure file shares (domain integrated or stand-alone) and shares created on storage vendors like Nutanix and NetApp**. AppVentiX can be configured to use integrated authentication or a (service) account to access the shares. The permission table is visible in the Central View console (share permission button). A screenshot is added at the beginning of this guide. The following share permissions are needed for AppVentiX to operate:

Share	AppVentiX Agent	AppVentiX Central View
Configuration share	Read	Read\Write*
Configuration share (inventory folder)	Read\Write	Read\Write
Content share(s)	Read	Read*

* Central View needs also write permissions if you want to convert MSIX packages to app attach or App-V packages to MSIX, if you want to delete content from the Content Share directly from the console you also need write permissions. For other management activities only read permissions are needed. This means you can provide the console to helpdesk\admins to operate the deployment but not change any configurations.

When creating a share in an active directory environment, you can use integrated authentication or provide a (service) account. When using integrated authentication, provide the domain computers group read permissions on the configuration share and read/write permissions on the inventory folder inside the configuration share. Below a screenshot of the permissions:

Permissions for Config		×	Permissions for Inventory		
ecurity			Security		
Object name: 🗰	Config		Object name:	Config\Inv	entory
Group or user names:			Group or user names:		
🎎 Domain Computers (Domain Computers)		SYSTEM		
SYSTEM			Domain Admins (Control Dom	iain Admins)	
Permissions for Domain Computers	Add	Remove	Permissions for Domain Computers	Add	Remove
Permissions for Domain Computers Full control	Add Allow	Remove Deny	Permissions for Domain Computers Full control	Add Allow	Remove Deny
Permissions for Domain Computers Full control Modify	Add Allow	Remove Deny	Permissions for Domain Computers Full control Modify	Add Allow	Remove Deny
Permissions for Domain Computers Full control Modify Read & execute	Add Allow	Remove Deny	Permissions for Domain Computers Full control Modify Read & execute	Add Allow	Remove
Permissions for Domain Computers Full control Modify Read & execute List folder contents	Add Allow	Remove Deny	Permissions for Domain Computers Full control Modify Read & execute List folder contents	Add Allow	Remove Deny
Permissions for Domain Computers Full control Modify Read & execute List folder contents Read	Add Allow	Remove Deny ^ ^ 	Permissions for Domain Computers Full control Modify Read & execute List folder contents Read	Add Allow	Remove
Permissions for Domain Computers Full control Modify Read & execute List folder contents Read	Add Allow	Remove	Permissions for Domain Computers Full control Modify Read & execute List folder contents Read	Add Allow	Remove

Domain computers: Read permissions on configuration share Domain computers: Read\Write permissions on inventory folder Domain admins (or group that performs management): Read\Write permissions

Share permissions can be set to everybody full control, so NTFS permissions are used for effective permissions to the files.

When the machines are Active Directory integrated, the AppVentiX agent uses the computer account to query AD to retrieve user groups. By default this works out of the box, but sometimes Active Directory is configured with a lot of security related settings. In this case contact support@appventix.com so we can help with the configuration of the AD domain integration.

The agent also uses integrated authenticated by default, integrated authentication uses the machine account to read the shares. You can configure the agent with a user account, just like in the Central View console:



You can also install\update the agent silently to use the same account as configured in the Central View console (click on the silent install button in the Central View console):

Close	The AppVentiX agent is a small and light weight installation, it can be pushed remotely or installed using the below silent installation parameter. When an older version is detected it will be upgraded automatically. The agent installation or upgrade can be done while users are logged in.
Silent inst	all parameter
Silent ins	tallation with the configuration share as parameter: f "AppVentiX Agent.msi" /quiet CONFIGURATIONSHARE=\\appventixstorageaccount.file.core.windows.net\appventixshare
Silent ins	tallation with the configuration share and configure the agent with the same account as Central View to access shares:
msiexec , \config S	i "AppVentiX Agent.msi" /quiet CONFIGURATIONSHARE=\\appventixstorageaccount.file.core.windows.net\appventixshare HAREACCOUNT=UxKgSkdt/VcjPrQNeBPuj/jj920E4ZY/PeC0kENm2ZAikqNiqpmKC1Asaoez7ckJaE6te2taJBD

This makes it easy to deploy the solution with minimal effort and get up and running quickly.

Central View inventory

By default the machine, user, process and event inventory data is stored on the configuration share in the inventory folder. When an inventory is triggered the agent will receive a command (also through the configuration share) to perform the inventory. The inventory data is displayed (together with the inventory time) in the console.

Optionally it's possible to enable direct inventory to the agent using WinRM (in the advanced agent settings turn the inventory slider to disabled). The performance and scalability of the inventory through the configuration share is much better then the direct connection, so recommended is to leave the inventory through configuration share option enabled.

Central View advanced settings

In the Central View advanced settings you can configure global settings which will apply to the whole deployment (both console and agents), the following advanced settings can be configured:



- Enable multi domain and nested group support: This setting is enabled by default for new installations. It will provide support when users are located in different domains and when using nested groups (groups inside groups).
- Enable LDAPS: When enabled, both Central View and agents will use LDAPS to communicate to the domain, please note you need certificates installed on your domain controllers
- Use SSL for remote machine inventory: This setting will enable WinRM communication over SSL. Please note you have to deploy a machine certificate to the agent machines in order to use WinRM over SSL. On the next page you will find more information how to enable WinRM over SSL. This setting is not used when inventory is done through configuration share (new default)
- Inventory machines on FQDN, when enabled the FQDN (for example machinename.mydomain.local) name will be used to contact the machines for management
- Remote connection (WinRM) time-out value this is the maximum time to wait before timing out a connection to an agent, increase this value when running inventory over WAN connections. This setting is not used when inventory is done through configuration share (new default)
- Manually configure the domain context: By default AppVentiX will use the default domain configuration, but when your Active Directory is complex or when it has delegation

configured you might want to manually configure the domain context. When you enable this option you can configure the domain name and domain container:

Domain name (contoso.local or contoso):	
Domain container (OU=company,DC=contoso,DC=local)):
	3

For example the domain name you want to use is: contoso And the domain container is OU=Myorganization,DC=contoso,DC=local AppVentiX will look for machines and user\groups in this OU only, it's also possible to provide multiple domain containers, for example when your machines and user groups are in different OU's, you can configure the domain context as follows:

OU=Mymachines,OU=Myorganization,DC=contoso,DC=local;OU=Myusers, OU=Myorganization,DC=contoso,DC=local

(note the separating semicolon)

Please contact <u>support@appventix.com</u> if you need any help with this configuration.

 Inventory machines on FQDN instead of netbios name, enable this setting when your machines cannot be reached on machine name only, when enabled Central View will retrieve the FQDN name of the machine from AD and will show this in the inventory instead of only the machine name, it will use the FQDN when contacting the machine

Supported operating systems

The following operating systems are supported by the AppVentiX agent:

- Windows server 2016 (64Bit)
- Windows server 2019 (64Bit) (App-V and MSIX client are embedded in Server 2019)
- Windows server 2022 (64Bit) (App-V and MSIX client are embedded in Server 2022)
- Windows server 2025 (64Bit) (App-V and MSIX client are embedded in Server 2022)
- Windows 7, 10 and 11 (64Bit) (App-V and MSIX client are embedded in Win10\11)

The following operating systems are supported by the AppVentiX Central View console:

- Windows server 2019 (64Bit)
- Windows server 2022 (64Bit)
- Windows server 2025 (64Bit)
- Windows 10 (64Bit)
- Windows 11 (64Bit)

For all AppVentiX components you need at least .NET 4.8.

Please check the MSIX and MSIX app attach compatibility with the OS you are using, app attach is currently only supported in Windows 10 Build 2004 and up. And MSIX shared containers are only supported on Windows 10 Build 21X and up.

Upgrade from App-V Scheduler

It is possible to upgrade from App-V Scheduler 2.5 and 2.6 to AppVentiX 3.X The recommended upgrade path is as follows:

- Create a backup copy of the configuration share (just in case)
- Install the new Central View console and point it to the same configuration share. When the console is started for the first time the configuration files are upgraded and renamed. You will see the following message:

AppVenti	Central View	×
1	The previous App-V Scheduler configuration has been successfully upgraded to AppVentiX 3.0. The old configuration files are still on the configuration share to make sure older agents can still use them. Please remove the App-V Scheduler configuration files from the configuration share after all agents are upgraded.	
	OK	

- The old configuration files are kept intact so older agents can still use them. You can also still use the old Central View console to update the configuration
- The new Central View console and updated agents will use the updated configuration files
- When all agents are upgraded you can delete the old configuration files

Upgrade from earlier version of AppVentiX

The upgrade from an earlier AppVentiX version to the latest version is straight forward, the components are upgraded in place (no need to uninstall first). Before upgrading create a copy\backup of the configuration share.

Upgrade the Central View console first, then the agents. The version of the agent is always 1 major version backward compatible with the Central View console, this means you don't have to upgrade all agents at once, but it's recommended to keep this period as short as possible.

FSLogix and roaming profile settings

AppVentiX has been verified to work very well with FSlogix and other profile management solutions like Citrix UPM and Windows roaming profiles, contact support@appventix.com if you have any questions. If you encounter any issues, please check the following:

FSlogix in combination with App-V

When using FSLogix in combination with App-V you might encounter some packages that do not work anymore after the second logon. To fix this, enable the "Always publish this package" option in the publishing task. This will make sure the package integrations for the affected package is

configured correctly after each login. Another work around is to add the following path to the FSlogix exclusions xml file: AppData\Local\Microsoft\AppV\Client. Also make sure to use the latest FSLogix build.

FSlogix in combination with MSIX

MSIX data roaming is enabled by default for FSlogix (see below screenshot). No additional configuration is needed. MSIX data is roamed for normal deployed MSIX packages and MSIX packages delivered by app attach.

MSIX data roaming configuration: 🤇		
Profile container (FSlogix) O Ro	paming profile (Windows \ Citrix UPM etc)	O Local profile (No roaming)

The log file for the roam MSIX app data can be found in: %appdata%\AppVentiX The log file will be cleared every 7 days.

There is only one exclusion needed when you encounter stale Windows Startmenu shortcuts, then create or modify your existing FSlogix exclusions xml file with the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<FrxProfileFolderRedirection ExcludeCommonFolders="0">
<Excludes>
<Exclude
Copy="0">AppData\Local\Packages\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\TempState</Exclude>
</Excludes>
</FrxProfileFolderRedirection>
```

Windows roaming profiles with MSIX

For Windows roaming profiles the following setting needs to be enabled:

```
MSIX data roaming configuration: 😮
```

```
○ Profile container (FSlogix) ● Roaming profile (Windows \ Citrix UPM etc) ○ Local profile (No roaming)
```

When you configured the roaming profile settings to delete cached copies of the profile, you need to enable the below GPO setting as well:

Allow deployment operations in special profiles

🗊 Group Policy Management Editor				-		٥	\times
File Action View Help							
🗢 🤿 🙍 💼 🗟 🛛 🖓 🤝							
> 🛅 System	^	📋 App Package Deployment					
 Windows Components ActiveX Installer Service 		Allow deployment operations in		Setting		State	
Add features to Windows 10	c	special profiles		Allow deployment operations in special profiles		Enable	d
📔 App Package Deployment		Edit policy setting	~	E Allows development of Windows Store apps and installing t	No	t config	jured

Other profile solutions that capture the roaming data of the user (Like Citrix UPM) with MSIX

Enable the following agent setting:

MSIX data roaming configuration: ?

```
○ Profile container (FSlogix) ● Roaming profile (Windows \ Citrix UPM etc) ○ Local profile (No roaming)
```

Make sure the %appdata%\AppVentiX folder is captured\roamed in the roaming profile solution.

Optionally the show save package data progress at logoff can be enabled. This will show a brief notification of the MSIX data being saved at logoff.



Automated image building and deployment actions

Image build events

AppVentiX is often used as part of automated image building procedures. To check if AppVentiX has finished pre-caching packages in the image, the below PowerShell script can be used. The script will check the AppVentiX finished event and then continue.

For App-V, the check can be performed on the pre-cached all App-V packages event (122):

```
$eventlogname = "AppVentiX Agent"
# Check for all packages pre-cached event
Do {
$allpackagesloadedevent = Get-EventLog -LogName $eventlogname -Source "APPV" -Newest 5 |
where {$_.InstanceId -eq 122}
if($allpackagesloadedevent)
{Write-Host "Finished, all App-V packages are pre-cached"}
else{
Write-Host "Not finished, sleep 30 seconds"
Start-Sleep -Seconds 30
}
# End of 'Do'
While (!$allpackagesloadedevent)
```

For MSIX, the check can be performed on the refresh cycle finished event (2000):

```
$eventlogname = "AppVentiX Agent"
# Check for refresh cycle finished event
Do {
    $allpackagesloadedevent = Get-EventLog -LogName $eventlogname -Source " Service" -Newest 5 |
    where {$_.InstanceId -eq 2000}
    if($allpackagesloadedevent)
    {Write-Host "Refresh cycle finished, all MSIX packages are pre-cached"}
else{
    Write-Host "Not finished, sleep 30 seconds"
    Start-Sleep -Seconds 30
    }
    # End of 'Do'
While (!$allpackagesloadedevent)
```

Note for MSIX app attach: It's not recommended to place app attach packages on a content share configured for a machine group where the build VM is member of. App attach packages are not needed to pre-cache in the image because they are virtual disks attached to the VM in runtime.

Run the refresh cycle from the command line

The refresh cycle automatically runs when the machine boots, the refresh cycle can also be invoked from the Agent GUI, based on a timer or remotely through the Central View console (recommended). It's also possible to invoke the refresh cycle with PowerShell. This can be done using the following PowerShell one liner:

(Get-Service 'AppVentiXService').ExecuteCommand(254)

When Central View console takes longer to start

When the machine running the Central View console doesn't have internet access, the console can be slow to start. This is default behaviour for .NET applications that are signed with a certificate, because there is no internet connection the Microsoft CRL checking process can't check the certificate used to sign the AppVentiX executables. To work around the issue you can manually update the CRL, enable internet access or disable CRL checking:

Disable CRL Checking Machine-Wide Control Panel -> Internet Options -> Advanced -> Under security, uncheck the Check for publisher's certificate revocation option

Please note that AppVentiX doesn't make any internet (outbound) connections at all, so internet access is not needed for AppVentiX to work.

Also please make sure to check the connection to the central configuration share. How further away the Central View console is placed from the central configuration share it can take longer to retrieve the configuration.

Example configurations of the AppVentiX Agent

The following examples can give you some insight into how AppVentiX can be configured. This configurations are validated to work, but they are only intended to give you an idea of the possibilities. They can be used as guide line but are not written down here to serve as best practice or recommended configuration. Feel free to contact support@appventix.com we are always happy to discuss which approach is the best for your environment.

Example of AppVentiX deployment in combination with non-persistent machines and App-V

- Move the Cache to a persistent drive (for example the same one as the write-cache)
- Configure in the AppVentiX agent settings to detect the image state (don't deploy packages when in read\write mode)
- Configure the agent to clean the cache after reboot (needed because drive is persistent)
- Use SCS mode in combination with the mount specific packages option (mount packages that either perform better when fully cached or if you want them to be higher available) this combination gives you the best of both worlds

Example of AppVentiX deployment in large scale non-persistent VDI environment in combination with App-V

- Keep the cache on the default location
- Enable the detect image state option and configure to mount all packages in the cache in private mode and use SCS mode when in read-only mode
- The rest of the configuration will be configured automatically according to above setting

In this deployment mode, when the image is booted in private mode (during Windows update or build update), all the latest packages will be mounted in the cache automatically. An event will be logged when the pre-cache operation is done (you can configure your automatic build method to check for this event, contact support for an example).

When the image is in read-only mode new packages can be deployed to the machines, in read-only mode new packages will be added automatically by using SCS mode (reading package content directly from the share). In this way the write-cache isn't polluted.

This deployment mode gives you the best of both worlds in large VDI deployments: lower IO during boot and be able to deploy packages and application updates during runtime of the machine.

Example of AppVentiX deployment in combination with persistent machines and App-V (like RDS\AVD and physical machines)

- Keep the cache on the default location
- Don't clean the cache at machine reboot
- Configure the AppVentiX agent to remove packages that are no longer on source share (keep cache in balance with source)
- Use SCS mode in combination with the mount specific packages option (mount packages that either perform better when fully cached or if you want them to be higher available) this combination gives you the best of both worlds. Or mount all packages by default if disk space is not an issue

Example of AppVentiX deployment in combination with non-persistent machines and MSIX

- Leave the MSIX cache location default or redirect to persistent drive in the agent settings
- Configure the AppVentiX agent to detect the image state (agent setting) (don't deploy packages when in read\write mode). In this scenario we only deploy packages when the image is readonly.
- You can use both MSIX app attach and normal MSIX package delivery, normal packages will be cached on the persistent drive or temporary write cache location (depending if you redirected the cache in the agent settings)
- Clean the MSIX cache after reboot (agent setting) when redirected to persistent drive
- Using above combination gives you the best of both worlds in terms of space utilization and performance

Example of AppVentiX deployment in large scale non-persistent VDI environment in combination with MSIX

- Keep the cache on the default location
- Enable the detect image state option and configure to load all packages in the cache in private mode
- Place all MSIX packages on a content share with the pre-cache option enabled
- Place MSIX app attach packages on a content share with pre-cache disabled

In this deployment mode, when the image is booted in private mode (during Windows update or build update), all the latest MSIX packages will be loaded in the cache automatically. An event will be logged when the pre-cache operation is done (you can configure your automatic build method to check for this event, contact support for an example).

When the image is in read-only mode you can delivery MSIX packages through app attach to users, this will not consume any disk space. You can also decide to deliver all packages through app attach (like previous example) but this example will give you an indication about the possibilities with AppVentiX to achieve the best possible combination.

This deployment mode gives you the best of both worlds in large VDI deployments: lower IO during boot (MSIX packages already exists in image) and you will be able to deploy packages and apply application updates during runtime of the machine.

Example of AppVentiX deployment in combination with persistent machines and MSIX (like RDS\AVD and physical machines)

- Keep the cache on the default location
- Don't clean the cache at machine reboot

- Configure the AppVentiX agent to remove packages that are no longer on source share (keep cache in balance with source). This is enabled by default.
- You can use a combination of normal MSIX deployment and MSIX app attach:
- Use normal MSIX delivery to have less pressure on the content share (packages are loaded in the cache and published from there to users). Also when the share goes down there is less downtime (app attach needs constant availability to the content share). Because packages are published from the local cache of the machine, the application might work faster.
- Use app attach to save disk space on the machines and speed up the registration of bigger packages (the package doesn't have to be loaded on the machine, package data will be accessed over the network through the attached disk

With AppVentiX you are in complete control over the deployment there is always a combination available that suites your uses case the best. Feel free to contact support@appventix.com we are always happy to discuss which approach is the best for your environment.

Website : <u>www.appventix.com</u> Sales : <u>sales@appventix.com</u> Support : <u>support@appventix.com</u>