

=BriefCam TRANSLATING VIDEO INTO IMPACT

BriefCam Installation Guide

19 May 2025

© 2025 BriefCam





Contents

BriefCam Installation Guide
Prerequisites
Site and Network Topology
Supported GPUs
Supported Hardware Configurations
Installed Software
Antivirus
Firewall Consideration and Ports Availability. 12
RESEARCH Prerequisites
All-in-One Installer
Order of Installation
Installation Components
PostgreSQL Installation
RabbitMQ Installation
BriefCam Server Installation
BriefCam Web Services Installation
BriefCam RESEARCH Installation
Help Center Installation 66
License Activation
Network Security Considerations
Silent Installations
Large Scale Deployments 77
Logging and Monitoring

=BriefCam

Deploying a Graylog Server	7
Load Balancers	2
MongoDB Installation	2
VMS Integrations	6
BriefCam's VMS Integration Levels	7
Supported VMS Table	8
Third Party Integrations 8	8
BriefCam VMS Integration Plugin Installation 8	9
American Dynamics Integration	0
Arcanes Technology Integration	0
Avigilon Integration	18
Axis Integration	0
Bosch Integration	6
CASD Integration	2
Dallmeier Integration	5
Digifort Integration	!4
Exacq Integration	0
FLIR Integration	;1
Genetec Integration	4
GeoVision Integration	51
Geutebruck Integration	62
Hanwha Techwin Integration	62
IndigoVision Integration	7
Intellicence Integration	6

--BriefCam

	IPOrchid Fusion Integration	175
	ISS Integration	176
	LenelS2 Onguard Integration	180
	Lensec Integration	186
	March Networks Integration	189
	Milestone Integration	193
	NX (Network Optix) Integration	219
	Pelco Integration	222
	Qognify Nicevision Integration	225
	Qognify Ocularis and Qognify VMS Integration	228
	Salient Integration	237
	Teleste Integration	239
Pr	oprietary Format Support	241
	Dahua Integration	241
	HIK Integration	242
	Infodraw Integration	242
	Timespace X300 Integration	242
Techn	ical How-tos	242
Cł	nanging Default Ports Configuration	243
Mo	oving the BriefCam Network Share	244
Ru	unning BriefCam in Virtual Environments	244
Co	onfiguring Single Sign-On (SSO)	245
SA	AML – ADFS Relying Party Setup for BriefCam Requirements	245



	Installing and Configuring NGINX	257
	Adding a New Cluster in the RESEARCH Module	269
	Configuring RESEARCH and Web Services Distributed Environment	282
	Adding a New Cluster in the RESEARCH Module	285
	Replicating the BriefCam PostgreSQL Database	297
Ins	tallation and Troubleshooting Tools	305
	Check Prerequisites Tool.	305
	Move Storage Tool	305
	Server Hostname Change Tool	307
	Configure Server Logging Tool	308
	Log Collector Tool	308
	Installation Troubleshooter	309
Dis	stributed Architecture	310
Re	quired Configuration per Machine Type	310
Ins	tallation Guide: Appendix	312
	Installed Prerequisites	312
	Installed Services	313

Copyright, trademarks, and disclaimer

Copyright © 2025 Milestone Systems A/S

Trademarks

This document contains trademarks owned by Milestone Systems A/S such as Milestone, Arcules, BriefCam, and XProtect.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious.

Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.





BriefCam Installation Guide

This guide provides detailed information about installing BriefCam products including prerequisites, the order of installation, technical how-tos, and instructions about VMS-specific BriefCam integration plugins.

For information about installing the Next-Gen engine, see the BriefCam Next-Gen Engine document.

See also:

Prerequisites All-in-one Installer Order of Installation Installation Components Upgrading Instructions Silent Installations Large Scale Deployments VMS Integrations Technical How-tos Installation and Troubleshooting Tools Distributed Architecture Installation Guide: Appendix

Prerequisites

BriefCam offers the Check Prerequisites tool that you can use to check that the hardware and operating system parameters on a machine meet the BriefCam's prerequisites before running the BriefCam installers.

See also: Site and Network Topology Supported GPUs Supported Hardware Installed Software Antivirus Firewall Consideration and Ports Availability RESEARCH Prerequisites

Site and Network Topology

Make sure an adequate site survey was performed and the following requirements are met:



Requirement	Description	
Servers	It is highly recommended to install BriefCam on a machine with the operating system only (no VMS, or any other additional software should be installed on the BriefCam machine). Make sure that the recommended hardware specified in the Bill of Materials (BoM) is being used. For more information, contact your Account Manager.	
Memory	At least 128GB of RAM.	
Storage	 At least 250GB of free space for the application At least 250GB for the database (on SSD drives) At least 500GB drive for data storage (video and metadata) 	
GPUs	At least one supported GPU in the deployment. For a list of the supported GPUs, see the Supported GPUs section in the BriefCam User Guide . Note that the GPU should not be used for any system task (for example: connecting a monitor to the GPU or running applications, such as Chrome, using the GPU).	
CPUs	For each CPU, at least 8 cores at base (non-turbo) frequency of 2.5GHz and above.	
Operating system language	The operating system language must be an English locale for all installations. After installing BriefCam, you can install any required language pack.	
Drivers	For the server with the GPU, make sure to download a supported version of the NVIDIA driver (535 or higher). Make sure to restart the machine after installing the NVIDIA driver.	
Network connectivity between BriefCam and the VMS	Ensure a minimum of 1 Gbps of throughput is available. This is relevant for deployments with less than 300 cameras on site. For larger deployments, consult with your BriefCam Account Manager. The latency should be less than 100 ms with a recommended latency of between 30-40 ms.	
Network connectivity between BriefCam components	Ensure a minimum of 1 Gbps of throughput is available and that all BriefCam server devices are located as topologically close as possible to one another (same switch, same subnet, etc.). This is relevant for deployments with less than 300 cameras on site. For larger deployments, consult with your BriefCam Account Manager.	

Supported GPUs

The GPUs listed below have undergone thorough testing and certification by BriefCam accompanied by throughput benchmarking conducted by our organization. The results are as follows (for 1080p cameras, 15 FPS, and medium activity):

Engine	GPU	Real-time channels	On-demand Hs/H



Windows-based OX5 engine	Ampere A10	30	20
	Ampere RTX A2000	23	25
	Ampere RTX A4000	30	28
	Ada RTX4080 (for laptops only)	28	24
	Ada L4	30	30

Note that:

- Hs/H means the number of hours of video that can be processed in a single hour. For example, 8 Hs/H means that 8 hours of video fetched from a particular camera can be processed in 1 hour.
- Throughput refers to number of concurrent on-demand processing speed multiplier or real-time channels per GPU (pending available GPU RAM).
- Intel, AMD or any other non-NVIDIA GPUs are not supported at this time.
- BriefCam does not support using more than one type of GPU on the same machine.

Supported Hardware Configurations

The following are the supported configurations:

Workstation Grade

- Dell Tower Workstation 3660 equipped with (1) A2000
- Dell 1U Workstation Rack Mount 3930 equipped with (1) A4000
- Dell 2U Workstation Rack Mount 7920 equipped with (4) RTX A4000

Server Grade (during non-HW sales, recommended for spec only)

- L4, featuring the following specifications:
 - RĂM: 128/256ĞB RAM
 - Storage: 2X 512 GB SSD disk for the OS
 - CPU: A minimum of 24 cores at a clock speed of 2.90GHz



These specifications apply to one NVIDIA L4 hosted on the BriefCam processing machine. If the number of cards doubles, increasing the RAM and CPU is advisable. It is recommended not to host more than two L4s on one processing machine.

Laptop Grade (during non-HW sales, recommended for spec only)

- RTX4080 ADA, featuring the following specifications:
 - RAM: 64GB RAM
 - Storage: 2TB SSD disk
 - CPU: A minimum of 24 cores at a clock speed of 2.20GHz

Installed Software

Before installing a BriefCam component, download the installer to the machine where you will be installing that component.

The following software components must be installed prior to the BriefCam product installation:





Supported Operating Systems for OX5

The operating systems that are supported are:

- Windows Server 2022
- Windows Server 2019
- Windows 11 (for laptop environments)
- Windows 10 IoT Enterprise 2021 LTSC

You can check the Windows versions by running winver.exe.



Windows 10 and Windows 11 can be used for development environments. They are not supported for other production environments (with the exception of laptop configurations) and do not support RESEARCH environments.

Windows Updates

Make sure that every server has the latest Windows updates installed.

Supported Browsers

- Google Chrome v. 77.* and above
- Microsoft Edge v. 80 and above

High Security Environment with Customized Policy Settings

If your environment is configured for high security with customized policy settings, note the following:

Many of the installers use PowerShell. To enable PowerShell to run, the Local Computer's **Turn on script execution policy** must be enabled or not configured (and not disabled). In addition, the maximum restriction of the policy that can be used is **RemoteSigned**.

To turn on script execution follow these steps:

1. From the Windows Start menu, type policy and select Edit group policy.



- 2. The Local Group Policy Editor will open.
- 3. Navigate to Computer Configuration -> Administrative Templates -> All Settings.
- 4. Check that the Turn on Script Execution policy is set to Not configured or Enabled.



Local Group Policy Editor				
File Action View Help				
🗢 🔶 🙍 📷 🕞 📓 🖬 🝸				
 Local Computer Policy Computer Configuration Software Settings Windows Settings Administrative Templates Control Panel Network Printers Server 	Setting Turn on protocol recognition Turn on raw volume write notifications Turn on recommended updates via Automatic Updates Turn on removal of items from scan history folder Turn on reparse point scanning Turn on Responder (RSPNDR) driver Turn on root certificate propagation from smart card Turn on second frequential feature updates	State Not configured Not configured Not configured Not configured Not configured Not configured		
 Start Menu and Taskbar System Windows Components All Settings User Configuration Software Settings Windows Settings Mindows Settings Administrative Templates 		Not configured Not configured Not configured Not configured Not configured Not configured Not configured		

To check that the maximum restriction of the execution policy is **RemoteSigned**:

• From PowerShell, run the following command: Get-ExecutionPolicy.

To set the execution policy to RemoteSigned:

· From PowerShell, run the following command: Set-ExecutionPolicy RemoteSigned

Antivirus

It is required to disable antivirus scans from all BriefCam's folders as specified below.

The BriefCam engine extracts many objects from raw video and keeps them in small video files and image files. (In high activity scenes, there may be thousands of files created in each hour and even more.)

When the antivirus is enabled and every created file is automatically scanned, this leads to poor performance and poor hardware utilization.

To disable the antivirus:

In each one of BriefCam's servers, disable the antivirus scan for these paths (if they exist, which depends on the installed components).

Installation Folder	Default Installation Path	
Server	C:\Program Files\BriefCam\BriefCam Server	
Web services	C:\Program Files\BriefCam\BriefCam Web Services	
PostgreSQL	C:\PostgreSQL	
	C:\PostgreSQL_Data	
Redis	C:\Program Files\Redis	
Qlik	C:\Program Files\Qlik	
MongoDB	C:\Program Files\MongoDB	
RabbitMQ	C:\Program Files\RabbitMQ Server	

It is also recommended to add all the executable files located in the installation folders (from the table above) to the Allowed





Programs/Apps.

Allow apps to communicate through Windows Firewall			
To add, change, or remove allowed apps and ports, click Change settings.			
What are the risks of allowing an app to communicate?	- 😌 Ch	ange sett	ngs
Allowed apps and features:			
Name	Private	Public	٨
☑ BriefCamPostgreSQL		R	
BriefCamPostgreSQL	¥	R	
BriefCamRedis			
☑ BriefCamRedis	¥	2	
BriefCamRESEARCH		R	
BriefCamRESEARCH	2	2	
BriefCamRESEARCH	2	R	-
☑ BriefCamServer	2	2	
BriefCamServer	×	R	
BriefCamServer			
BriefCamServer	¥	R	
RiefCamServer	R	R	v

In the storage server, disable the antivirus scan for these paths (if they exist):

Installation Folder	Default Installation Path
ServerData	\\hostname\BriefCam\ServerData
Qlikshare	\\hostname\BriefCam\Qlikshare

Known Issues When the Antivirus Is Active

- Timeouts and errors when writing or reading from the storage occur when the antivirus becomes a bottleneck when trying to access the storage.
- · Slow server response time due to heavy use of memory, CPU, and disk utilized by the antivirus processes.
- Files that include low-level operations (such as HASP DIIs and NVIDIA drivers) may be put in quarantine and disrupt the normal functioning of BriefCam.

Firewall Consideration and Ports Availability

BriefCam offers the Check Prerequisites tool that you can use to check that the hardware and operating system parameters on a machine meet the BriefCam's prerequisites before running the BriefCam installers.

Internal (Local) Ports

On each server, the following ports should be opened for internal communication:

- On each server, all outbound ports should be opened, to allow communicating with other servers as needed.
- On each server, the following inbound ports should be opened according to the installed services. The BriefCam
 application listens for incoming traffic from these ports. The installer will create the relevant Windows firewall rules
 for these ports.



Component	Port #
BI Face Recognition Service	TCP 2556, TCP 13004
Face Recognition Matching Service	TCP 2553, TCP 13002
Filtering Service	TCP 2555, TCP 13001
License Service	TCP 1947
Lighthouse Service	TCP 2557
LPR Matching Service	TCP 2554, TCP 13003
MilestoneSSOProvider	TCP 8030
Notification Service	TCP 7080
PostgreSQL	TCP 5432
Rabbit MQ	TCP 5672
Redis	TCP 6379
Storage	TCP 139, TCP 445
Storage Gateway Service	TCP 5012
Video Streaming Gateway Service	TCP 5010
VSServer Service	TCP 1112, TCP 1113
Web Services (BOA, ProWebApi, AdminWebApi)	HTTP (80)
Large scale only	
MongoDB	TCP 27017
Hub	
BI Hub Export Gateway	TCP 5007
Outbound API Gateway	TCP 5005
Hub SSO Gateway (for future versions)	TCP 5008

RESEARCH (BI) Ports

RESEARCH (Qlik)	Port #	
НТТР	TCP 8090	Inbound / Outbound
HTTPS	TCP 443	Inbound / Outbound
API ports	TCP 4242, TCP 4243	Inbound / Outbound
Qlik Sense Engine Service	TCP 4747	Inbound / Outbound
Broker Service	TCP 4900	Inbound / Outbound





External Ports

The following ports should be opened to traffic coming from the end users' browsers.

Component	Port #	Comment
Web Services	HTTP (80)	
RESEARCH	HTTP (8090)	Not needed when using a load balancer
Video Streaming Gateway Service	TCP 5010	
Notification Service	TCP 7080	

To work with HTTPS and port 443, you need to use a load balancer. For more information, see the Installing and Configuring NGINX section.



Some ports can be changed if they are not allowed on the customer's network. For detailed instructions, see the Changing Default Ports Configuration section.

RESEARCH Prerequisites

When installing or upgrading an environment that uses an extended Research license, contact BriefCam's Support team by logging into the BriefCam Portal at https://www.briefcam.com/support/ and opening a ticket.

- .NET 4.8 Framework Runtime is required. The installer will check if this is installed on your machine but will not
 install it for you. Download it and install it on your machine from this link: https://dotnet.microsoft.com/en-us/download/dotnet-framework/net48.
- On the machine where you are installing the RESEARCH component, the **Automatically adjust clock for Daylight Saving Time** option must be selected.

=BriefCam

💣 Date and T	ime			×
Date and Time	Additional Clock	s Internet Time		
💣 Time Zor	ne Settings			×
Set the time	zone:			
Time zone:				
(UTC+02:00)) Jerusalem			\sim
Automat	ically adjust clo	ck for Daylight Sa	aving Time	
Current date	e and time:	Monday, April 5,	2021, 12:06 PM	
New date ar	nd time:	Monday, April 5,	2021, 1:06 PM	
		I	ОК	Cancel
Daylight Sa clock is not	ving Time ends set to adjust fo	on Sunday, Octo r this change.	ber 31, 2021 at 2:0	0 AM. The
🗸 Notify n	ne when the clo	ck changes		
		OK	Cancel	Apply

The following prerequisites are also required. However, if you are installing on a machine with the operating system only, you will not need to check for these prerequisites.

- 1. Make sure that the ports detailed in the RESEARCH Ports section are available before starting the installation.
- 2. Close the Task Manager, Services, Computer Management and MMC Console applications.
- 3. Temporarily disable the User Account Control (UAC).
- 4. Ensure that the current logged in user has full local admin rights and full Registry Read/Write permissions.
- 5. Disable the firewall when possible.
- 6. Stop the Antivirus, AntiMalware and any GPO activity on the server (all can be re-enabled after the installation) when possible. Or, ensure that the following folders are excluded:
 - C:\ProgramData\Qlik
 - C:\Program Files\Qlik
 - C:\Program Files\Common Files\Qlik
 - C:\qlikshare
 - C:\Users\YourId\AppData\Local\Temp
- 7. Reboot the server for changes to take effect.



When installing RESEARCH in an Offline environment, the installation has to be done manually. Contact BriefCam Support for assistance.

RESEARCH and Web Service on Separate Machines

If you are working with a distributed environment where the Web Services component and the RESEARCH component are on separate machines, you either need to:





- Use a load balancer (see: Installing and Configuring NGINX)
- Use an FQDN (preferable) or an alias/CNAME

For additional information, see: Configure RESEARCH and Web Services Distributed Environment.

All-in-One Installation Wizard



The all-in-one installation wizard is available for major releases only. For example, you can install BriefCam 2024 M1 with the wizard, but not BriefCam 2024 R2. In these cases, where the all-in-one installer is not available, use the individual installation components.

Order of Installation

It is important to install the components in the following order, as there are dependencies between the different components. The sections below will describe each of the components.

The links to the installation files are available from the Installation Downloads page.

- 1. Database (BriefCamPostgreSQL.exe) This file installs the PostgreSQL database and Redis cache. If you will be using MongoDB as well (which is only for large-scale deployments), install it after you install PostgreSQL.
- RabbitMQ (BriefCamRabbitMQ.exe)
- 3. BriefCam Server (BriefCamServer.exe)

On the server machines, in addition to the Server component, you also need to install:

NVIDIA driver – For any Server machine with a GPU, use a supported version of the NVIDIA driver (535 or higher). Note that you cannot put NVIDIA graphic cards from different models on the same machine. Make sure to restart the machine after downloading the NVIDIA driver.

- 4. BriefCam RESEARCH (BriefCamRESEARCH.exe) Run this file only if you will be using the RESEARCH solution. • Create Virtual Proxy (optional)
- 5. BriefCam Web Services (BriefCamWebServices.exe)
- 6. BriefCam VMS integration plugins Install the plugin for your VMS on every Server machine.
- 7. Help Center Installation (BriefCamHelpCenter.exe) Run this file only if BriefCam will be run offline.
- 8. Activate the license
- 9. Initial Set Up.
- 10. Launching BriefCam



Note that when installing or upgrading BriefCam or upgrading the NVIDIA GPU driver, it takes up to 30 minutes for the Processing Server service or Alert Processing Server service to start for the first time, because the Deep Neural Networks are being rebuilt.



Changing the server name after installing the BriefCam software will require additional changes. If you need to change the server name, contact BriefCam Support.

For information about installing large scale deployments, see the Large Scale Deployments section.





Installation Components

This section will provide you with details about installing the various components in BriefCam.

- Order of Installation
- PostgreSQL Installation
- **BriefCam Server Installation**
- BriefCam RESEARCH Installation
- BriefCam Web Services Installation
- Help Center Installation
- License Activation
- **Network Security Considerations**
- Large Scale Deployments

PostgreSQL Installation

Prerequisites

- When running the PostgreSQL installer, you are asked to select a data drive. This should be the drive with the most available space. For this drive, in the properties, uncheck the Allow files on this drive to have contents indexed in addition to file properties checkbox (as shown in the image below).
- The following ports are required during the BriefCam installation for PostgreSQL. Make sure that they are available before starting the installation:

Component	Port #
DB	TCP 5432 (or as provided)
Redis	TCP 6379



BriefCam cannot interface with a customer-managed PostgreSQL instance even if such an instance exists.

Installation Steps

1. To run the PostgreSQL Installation wizard, right-click on the BriefCamPostgreSQL_<Version number>.exe file and select Run as administrator.

Note: If you are using the latest Windows Update and a Windows Defender alert appears, click the **More info** link and click **Run anyway**.



Windows protected your PC

Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk. More info

2. The installation checks for prerequisites. If anything is missing, the following screen will appear. Click Next.

Х



3. In this screen, the prerequisites checked are the missing prerequisites. Click Next to install them.





4. In the Welcome screen, click Get Started.





5. Accept the terms of the license agreement and click **Next**.

-BriefCam

	×
BriefCam Install PostgreSQL	
	Ĵ
BRIEFCAM LTD.	^
END USER LICENSE AGREEMENT	
THIS END USER LICENSE AGREEMENT ("EULA") IS AN AGREEMENT BETWEEN YOU ("LICENSEE") AND BRIEFCAM LTD. ("BRIEFCAM") WHICH SETS FORTH THE TERMS OF THE LICENSE GRANTED BY BRIEFCAM TO LICENSEE AS TO THE SOFTWARE, AS DEFINED BELOW. THIS EULA PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS. READ IT CAREFULLY BEFORE USING THE SOFTWARE. BY SELECTING THE "I AGREE / I ACCEPT" BUTTON YOU ARE CONFIRMING YOUR ACCEPTANCE OF THIS LICENSE TO USE THE SOFTWARE AND AGREEING TO BECOME BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS	*
✓ I accept the license agreement	
Back	

The following screen will appear.





- 6. Select the drive where you want to install PostgreSQL.
- 7. Select the drive where you want to install the PostgreSQL data. The path to the PostgreSQL data cannot contain special characters, such as space, ~, and &.
- 8. Select the drive where you want to install the PostgreSQL scripts. It is recommended that both paths be set to a local SSD drive.
- 9. Click Next.

The following screen will appear.



	x
=BriefCam	Install PostgreSQL
Account Settings	
This user will run BriefCam's service	es
Use an existing user O Creat	e a new user
Domain .	
If the user is a local user, enter a period (.)	in the Domain field
Username bcuser	
Password	
Confirm Password	
Deny remote login for the BriefCam user	
Back	Next

- 10. Select whether to use an existing account or create a new account.
- 11. By default, BriefCam will populate the Username field with bcuser. Leave it as is or change it.
- 12. Enter the password. Note that special characters are not supported in the **Password** field.

Use a password that is compliant with your password policy.

It is important that you remember the password since you will be prompted to use this password in the following BriefCam component installations.

A password may fail for a variety of reasons:

- The password does not meet the password policy of the operating system and/or organization.
- Domain accounts cannot be created by this dialog. Contact the relevant IT person if a new domain account is needed.
- If the user is disabled, locked, or otherwise limited.
- 13. If the user is a domain user, enter the domain name and make sure that the domain user has full admin privileges on the server. If the user is a local user, enter a period (.).







- 14. If you selected to use an existing user, you can click **Validate Existing User** to check that the user credentials are valid.
- 15. For new users, you can select the **Deny remote login for the BriefCam user** checkbox to prevent the BriefCam user from remotely logging into the machine. If the checkbox is not checked, it will be possible to give the BriefCam user access to remote login (depending on your organization's policies).
- 16. Click Next.

The following screen will appear.

	×
=BriefCam	Install PostgreSQL
Create required data	base accounts:
Root account (for system	n administration)
Postgres Username	dbadmin
Postgres Password	*
() Keep this password for futur	e database administration
Application User	
Postgres Username	brief
Postgres Password	*
Keep this password and use	it in other BriefCam installers
Database Port	5432
Back	Next

17. Define a PostgreSQL administrator user and password both for the root account (for system administration) and for the application user.

Only English letters and whole numbers are supported for these fields.

18. Confirm the database listening port or select a new one if a non-default one is used. If you use a non-default one,



you will also have to use the same non-default port in the other installers.

19. Click Next.

The following screen will appear.

	×
BriefCam	Install PostgreSQL
BriefCam Shared Data Folde	er
Select a destination for Brie	fCam data folder:
C:\Briefcam	
The data folder will store al as video clips, images, etc. a servers.	I the processing artifacts, such nd share them with BriefCam
It's recommended to select the	drive with the most space available
() This field cannot contain specia	al characters, such as space and %
For remote machines: Select an For example: \\Host\BriefCam	n existing shared network folder,
For local machines: Select the of to create the data folder. For ex	rive where you want BriefCam ample: C:\
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Back	Install

- 20. Select the data drive that will hold the BriefCam data, including longer blobs, database backups, rendered synopsis files, and more.
 - · It's recommended to select the drive with the most available space.
 - The path to the PostgreSQL data cannot contain special characters, such as space, ~, and &.
 - If you select an existing shared network folder, make sure that the user has permissions to the shared network folder.
 - In the properties of the drive you select, make sure you unchecked the Allow files on this drive to have contents indexed in addition to file propertiescheckbox (as described in the prerequisites above).

The set up will automatically create a shared BriefCam folder on the selected drive.

If you want to select a mapped drive, make sure to first map the drive and then select it from the **BriefCam Shared Data folder** screen.

- 21. Click Install.
- 22. Your PostgreSQL installation is now complete. Click Finish.







If you want to move the BriefCam network share to another location, see Moving the BriefCam Network Share.

Uninstalling the PostgreSQL Component



If the PostgreSQL component is uninstalled, the PostgreSQL base directory and data directory, as specified during the installation, must be manually removed.

See also:

Backups

RabbitMQ Installation

BriefCam is built with an extensive task-oriented architecture in which every video analytics request is split into many tasks, such as fetching, processing, and rendering. These tasks run in parallel and they often have dependencies, priorities and error handling procedures. This parallelization is done using RabbitMQ, which is an advanced message queueing platform.

Note that:

- RabbitMQ must be installed before the BriefCam Server.
- BriefCam does not currently support RabbitMQ connections over secure channels.

Installation Steps

- 1. To run the BriefCam RabbitMQ Installation wizard, double-click BriefCamRabbitMQ_<Version number>.exe.
- 2. The installation checks for prerequisites. If anything is missing, the following screen will appear. Click Next.







3. In this screen, the prerequisites checked are the missing prerequisites. Click **Next** to install them.

	×
<i></i> =BriefCam	Install RabbitMQ
The prerequisites checked below a install them	are missing. Click "Next" to
Prerequisites ☑ BriefCam-Utils ☑ Microsoft Visual C++ 2015-	2022 Redistributable (x64)
Back	Next

4. In the Welcome screen, click Get Started.





5. To proceed with the installation, read and accept the License Agreement terms. Click **Next** to continue. 6.

-BriefCam



7. Select the location where you want to install RabbitMQ and click Next.





The following screen opens.





- 8. In the **Database Host** field, enter the hostname or IP address of the PostgreSQL database.
- 9. In the **Database Port** field, enter the port of the PostgreSQL database.
- 10. Enter the application user and password. Note that special characters are not supported for passwords.
- 11. Click the **Test Database Connection** button.
- 12. Click Install.
- 13. Once the installation is complete, click **Finish**.

BriefCam Server Installation

Prerequisites

All BriefCam servers must reside in the same time zone and have the same time zone. When products are configured in one location and moved to another, the time zone configuration may change and cause previous processes to break. For example, the data synchronization between the BriefCam server and RESEARCH dashboards will not work.

Remember that before installing the BriefCam server, the PostgreSQL database needs to be installed.

It is recommended to not turn on IPv6 on the Network connections for the BriefCam servers.

The following ports are required during the BriefCam server installation. Make sure that they are available before starting the installation.





Component	Port #
VSServer Service	TCP 1112, TCP 1113
Notification Service	TCP 7080
Lighthouse Service	TCP 2553, TCP 2554, TCP 2555, TCP 2556, TCP 2557

Installation Steps

1. To run the BriefCam server Installation wizard, right-click on the BriefcamServer_<Version number>.exe file and select Run as administrator.

Note: If you are using the latest Windows Update and a Windows Defender alert appears, click the **More info** link and click **Run anyway**.

	Windows protected your PC	×		
	Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk. <u>More info</u>			
2.	The installation checks for prerequisites. If anything is missing, the following scre	en will a	appear. Cli	ck Next.





3. In this screen, the prerequisites checked are the missing prerequisites. Click **Next** to install them.





4. Click Get Started.





5. Accept the terms of the license agreement and click **Next**.

-BriefCam



6. Select the location where you want to install the BriefCam server and click Next.
-BriefCam







- 7. Select whether to use an existing account or create a new account.
- 8. Enter the user name and the password. The user needs to have administrator rights on the local machine. Note that special characters are not supported in the **Password** field.
- 9. If the user is a domain user, enter the domain name. If the user is a local user, enter a period (.).



- 10. If you selected to use an existing user, you can click **Validate Existing User** to check that the user credentials are valid.
- 11. For new users, you can select the **Deny remote login for the BriefCam user** checkbox to prevent the BriefCam user from remotely logging into the machine. If the checkbox is not checked, it will be possible to give the BriefCam user access to remote login (depending on your organization's policies).
- 12. Click Next.

-BriefCam

	×
<i>≂BriefCam</i>	Install BriefCam Server
Database Settings	
BriefCam Database 💿	product1
BriefCam Database port	5432
Application User	brief
Application Password	****
Test database connection	
Security Configuration	
Passphrase 💿	
If you're now installing the first server, yo you're now installing additional servers: have one; otherwise, leave the field empt	ou can create a custom passphrase. If enter the custom passphrase if you ty.
Back	Next

- 13. In the **Database Settings** section:
 - a. In the **BriefCam Database** field, enter the host name or the IP address of the PostgreSQL database.
 - b. The **BriefCam Database port** field will be automatically populated with 5432. This needs to be the same port that was used when installing PostgreSQL.
 - c. In the **Application User** and **Application Password** fields, make sure to use the same application user and password that you defined in the PostgreSQL installer. Note that special characters are not supported for passwords.
 - d. Click the Test database connection button.
- 14. In the **Passphrase** field, you can optionally create a passphrase when installing the first server and use the same passphrase in all installers. The passphrase can include 5-20 characters. If you are installing an additional server, use the same passphrase that you created when installing the first server. If you did not create a passphrase with the first server, leave the field empty.
- 15. Click Next.





16. In the BriefCam's shared data folder field, select the location where the video files and processing artifacts will be stored. In an all-in-one installation, the automatically generated value is correct. For distributed installations, set it to the BriefCam data shared folder created during the Postgres installation.

17. Set the **Connectivity Settings**.

- 18. Check the **Enable video streaming from this host** checkbox if you want the Video Streaming Gateway service to be enabled on the computer where you are installing the BriefCam server.
 - If you are installing all the components on one machine (an all-in-one installation), this checkbox needs to be checked.
 - If you are installing a distributed environment, the Video Streaming Gateway service should only run on one server this means that you need to decide in advance which machine should run this service.

19. Click Install.

20. Once the installation is complete, click Finish.



It is recommended to always log on with the same OS user to the BriefCam server.

The OS user that installs the BriefCam product has to be an administrator with full privileges. This user should be the only OS user to log on to the BriefCam server post installation.





For a list of the services installed when you install the BriefCam server, see the Installed Services section.

BriefCam Web Services Installation

Prerequisites

If you installed the RESEARCH component on a separate machine, please copy the certificates folder to the Web Services machine.

The following port is required during the BriefCam Server installation. Make sure that it is available before starting the installation.

Component	Port #	
Web Services	TCP 80	

Installation Steps

1. To run the BriefCam Web Services Installation wizard, right-click on the BriefCamWebServices_<Version number>.exe file and select Run as administrator.

Note: If you are using the latest Windows Update and a Windows Defender alert appears, click the **More info** link and click **Run anyway**.



2. The installation checks for prerequisites. If anything is missing, the following screen will appear. Click Next.





3. In this screen, the prerequisites checked are the missing prerequisites. Click **Next** to install them.





4. Click Get Started.





5. To proceed with the installation, read and accept the License Agreement terms.

6. Click **Next** to continue.

-BriefCam



7. Select the location where you want to install the BriefCam Web Services and click Next.





8. Select whether you agree to share anonymous usage data with BriefCam and click **Next**. (The anonymous data will be used for measuring the adoption of different product features. The data is monitored by BriefCam's product team, and helps focus on what matters most to BriefCam customers and to improve the product experience.)







- 9. Select whether to use an existing account or create a new account.
- 10. In the **Endpoint** field, enter the name. Note that the Web Services installer does not work with hostnames that are longer than 15 characters.
- 11. Enter the password. Note that special characters are not supported in the **Password** field.
- 12. If the user is a domain user, enter the domain name. If the user is a local user, enter a period (.).



- 13. If you selected to use an existing user, you can click **Validate Existing User** to check that the user credentials are valid.
- 14. Click **Next** and the following screen will appear.





- 15. Set the Web Services' Web endpoint and port. It is recommended to keep the default port that was populated automatically.
- 16. In the **License Server Host** field, enter the Licensing server host name (BriefCam Server host name) not fully qualified (without the domain name).



In the **License Server Host** field, it is recommended not to use localhost. If localhost is used in the field, the installation re-writes it with the host name of the current machine (this is to enable remote access for the license manager in a distributed deployment). If this occurs, the licensing server host name can be changed back to localhost in the BriefCam Administrator Console's **License.LicenseManager** environment setting. In addition, if you used a fully qualified name (which is currently not supported), you can change it in the **License.LicenseManager** environment setting.

17. Click Next and the following screen will appear.



	×
<i>BriefCam</i> ┌BriefCam's shared data folder	Install BriefCam Web Services
Enter the network path to Brief	Cam's data folder
\\PRODUCT1\BriefCam	
For example: \\ServerName\BriefCam	(~~~ (*** _/)
Database Settings	
BriefCam Database Hostname	PRODUCT1
BriefCam Database Port	5432
Application User	brief
Application Password	*****
Test Database Connection	
Security Configuration	
Passphrase (9)	
If you created a passphrase when inst passphrase. If you did not create a pas	alling the first server, enter the same sphrase, leave this field empty.
Back	Install

- 18. In the **BriefCam's shared data folder** field, enter the BriefCam file share (the BriefCam data shared folder created during the Postgres installation).
- 19. In the BriefCam Database Hostname field, enter the name of the machine where you installed PostgreSQL.
- 20. The **BriefCam Database Port** field will be automatically populated with 5432. This needs to be the same port that was used when installing PostgreSQL.
- 21. In the **Application User** and **Application Password** fields, make sure to use the same application user and password that you defined in the PostgreSQL installer. Note that special characters are not supported for passwords.
- 22. Click the Test Database Connection button.
- 23. In the **Passphrase** field, if you created a passphrase when installing the first server, enter the same passphrase here. If you did not define a passphrase, leave the field empty.
- 24. Click Install.

In certain scenarios, when installing the Web Services offline, a "SmartScreen can't be reached right now" message appears. If this message appears, click the **Run** button.

BriefCam RESEARCH Installation

The RESEARCH component should be installed if you have a Protect/Insights product license.



Do not install the RESEARCH component for Site deployments that are part of a multi-site deployment (comprised of multiple site systems and a central Hub).

Prerequisites

When installing or upgrading an environment that uses an extended Research license, contact BriefCam's Support team by logging into the BriefCam Portal at https://www.briefcam.com/support/ and opening a ticket.

- .NET 4.8 Framework Runtime is required. The installer will check if this is installed on your machine but will not
 install it for you. Download it and install it on your machine from this link: https://dotnet.microsoft.com/en-us/download/dotnet-framework/net48.
- For the RESEARCH installation, the network adapter must be turned on.
- If you are not installing on a clean machine (a machine with an operating system only), please see the RESEARCH Prerequisites section.

Installation Steps

1. To run the BriefCam RESEARCH Installation wizard, right-click on the BriefCamRESEARCH_<Version number>.exe file and select Run as administrator.



2. The installation checks for prerequisites. If anything is missing, the following screen will appear. Click Next.





3. In this screen, the prerequisites checked are the missing prerequisites. Click **Next** to install them.





4. Click Get Started.





5. Accept the terms of the license agreement and click **Next**.

-BriefCam







- 6. In the **RESEARCH Platform Path** field, select the path where you want to install the RESEARCH platform.
- 7. In the RESEARCH Platform's Data Folders section:
 - In the first field, select the path where you want to save the RESEARCH data. For upgrades, this should be the same drive where you previously installed the RESEARCH data.
 - In the second field, select the path where you want to save the RESEARCH backup files.
- 8. Click **Next** and the following will screen will appear.



- 9. Enter the following:
 - Server Hostname The hostname where the RESEARCH component is installed (use the system host name and not localhost).
 - **HTTP port** The RESEARCH module's port. Populated with 8090 by default. To define an alternative port if the default port is occupied, follow the details in section Changing Default Ports Configuration.
 - RESEARCH Endpoint A hostname or the load balancer endpoint when using a load balancer.
 - **RESEARCH Certificates Path** Location where the RESEARCH certificate is saved.
- 10. For first time installations, make sure the **Retain existing database settings** checkbox is not checked. When upgrading BriefCam, check the **Retain existing database settings** checkbox.

When checking the **Retain existing database settings** checkbox, the installer will deploy the updated RESEARCH components but keep all the previous RESEARCH-related environment settings unchanged.

- 11. Click Next.
- 12. If you did **not** select the **Retain existing database settings** checkbox, the following screen will appear. (If you did select the checkbox, skip to step 19).



- 13. In the **Hostname** field, enter the machine name of the server where the PostgreSQL database is installed. For an all-in-one installation, use the hostname (or localhost, as needed).
- 14. The **Port** field will be automatically populated with 5432. This needs to be the same port that was used when installing PostgreSQL.
- 15. In the **Application User** and **Application Password** fields, make sure to use the same application user and password that you defined in the PostgreSQL installer. Note that special characters are not supported for passwords.
- 16. Click the Test Database Connection button to check that the database is connected properly.
- 17. Click Next.

You will now be prompted to install Qlik with the default license or to enter RESEARCH (Qlik) license information.



- 18. To use the default license (in both online and offline installations), make sure that the **Install Qlik with the default license** button is checked.
- 19. If you select **Specify a different Qlik license**, enter the RESEARCH (Qlik) license information:
 - Serial Qlik license key.
 - **Control** Qlik control number.
 - LEF The LEF parameter should only be specified if there is no internet connectivity. You can get a LEF token by using this web page: Manual LEF (qliktech.com). If you need assistance with this, please contact BriefCam's support.
- 20. Click **Next** and the following screen will appear.





21. Select whether to use an existing account or create a new account.

The BriefCam user account should be a local administrator user on the local machine. Use the same password you configured for the BriefCam user account that was created during the database installation. (This needs to be done so that the RESEARCH backup will successfully run.)

You can use local accounts or domain accounts. Make sure the domain account is a member of the local Administrators group.



When upgrading the RESEARCH component, you cannot change the user. You must use the same user that you used in the original installation and the user field will be grayed out.

- 22. For an existing account, enter the password and for a new account, create and confirm the password. Note that special characters are not supported in the **Password** field.
- 23. If you selected to use an existing user, you can click **Validate Existing User** to check that the user credentials are valid.
- 24. If you selected to create a new user, you can select the **Deny remote interactive login for the BriefCam user** account checkbox to prevent the BriefCam user from remotely logging into the machine.

If the checkbox is not checked, it will be possible to give theBriefCam user access to remote





interactive login (depending on your organization's policies).

25. Click Next and the following screen will appear.

				×
BriefC	am		Install Bri	efCam RESEARCH
! Clie	ck the VER	RIFY button b	below	
The veri are free	fication wil	I check if the	e following p	ports
4242	443	4747	4900	9200
4243	4432	4899	7070	8090
Verify th	at the follo	wing proces	ses are clo	sed:
* Task N	lanager			
* Proces	ss Explore	r		
* Any Mi includii	icrosoft Ma ng Service	nagement (s and Comp	Console (Mi outer Manag	MC) application gement
VERIFY Verification may take 1-2 minutes				
Back	:			Install

- 26. Click the **VERIFY** button. The verification may take several minutes.
- 27. If the ports section is marked in red, this means that one or more of the ports is not free. Open the RESEARCH_Install.log file (located at: %APPDATA%\BriefCam), search for the string check_open_ports and see which of the ports are not free. Once you open the failing ports, try the verification again until it passes.
- 28. If the installer indicates that one of the following are open on your machine, close them and retry the verification: Task Manager, Process Explorer and any Microsoft Management Console (MMC) applications, including Services and Computer Management.
- 29. Once the verification is done (and you see two green check marks), click Install.

The RESEARCH installation may take 10 minutes or more to completely install.





If you are using a separate RESEARCH server, it is recommended to run the RESEARCH behind a load balancer. For information about how to do this, see Installing and Configuring NGINX.

Uninstalling RESEARCH

Uninstalling the RESEARCH component is only supported from the installer and not from the Windows Programs and Features.

This does not uninstall Qlik[®]. To uninstall Qlik:

- 1. Go to the **Control Panel > Programs > Programs and Features**.
- 2. On the left side, click View installed updates.
- 3. Uninstall Patch 6.

Installed Updates			
$\leftarrow \rightarrow \ ^{\vee} \uparrow \mathbf{P} \rightarrow \mathbf{Control} P$	anel > Programs > Programs and Features > Installed Up	odates	~
Control Panel Home Uninstall a program Turn Windows features on or off	Uninstall an update To uninstall an update, select it from the list and then of Organize Vininstall	click Uninstall or Change	L.
	Name	Program	Version
	Microsoft Windows (12)		
	Feature Update to Windows 10 21H2 via Enablement	Microsoft Windows	
	Feature Update to Windows 10 22H2 via Enablement	Microsoft Windows	
	Security Update for Microsoft Windows (KB5012170)	Microsoft Windows	
	Security Update for Microsoft Windows (KB5027215)	Microsoft Windows	
	E Servicing Stack 10.0.19041.1704	Microsoft Windows	
	E Servicing Stack 10.0.19041.1737	Microsoft Windows	
	E Servicing Stack 10.0.19041.2300	Microsoft Windows	
	E Servicing Stack 10.0.19041.2664	Microsoft Windows	
	E Servicing Stack 10.0.19041.2780	Microsoft Windows	
	E Servicing Stack 10.0.19041.2905	Microsoft Windows	
	E Servicing Stack 10.0.19041.3025	Microsoft Windows	
	Update for Microsoft Windows (KB5027122)	Microsoft Windows	
	Qlik Sense May 2022 (1)		
	Qlik Sense May 2022 Patch 6	Qlik Sense May 2022	14.67.17

4. Go back to Uninstall a program and uninstall Qlik Sense May 2022.









Restarting the RESEARCH Machine

Before rebooting or shutting down a machine with RESEARCH installed on it, check the status of the tasks in QMC and wait until the tasks marked in the image below in grey have finished running (when the **Status** column is set to **Success**).

🖷 Start 🔻						
Tasks						
Tasks Showing: 10 Select	ted: 6					
Name 🔺 🕞	Associated resource	Type 📑	Enabled	G	Status	G
Delete_Research_Data Application	Delete_Research_Data	Reload	Yes		 Success 	0
Manually triggered reload of Resear	Research	Reload	Yes		Success	0
Manually triggered reload of Resear	Research_Agg	Reload	Yes		Success	0
Reload License Monitor	License Monitor	Reload	Yes		 Success 	0
Reload Operations Monitor	Operations Monitor	Reload	Yes		 Success 	0
Research Application Reload Task 🥜	Research	Reload	Yes		Success	0
Research_Agg Application Reloa 🥜	Research_Agg	Reload	Yes		Success	0
Research_DB Application Periodi	Research_DB	Reload	No		Skipped	0
Research_DB_Agg Application P 🥜	Research_DB_Agg	Reload	Yes		Success	0
RESEARCH_USERS_usersynctask	RESEARCH_USERS	User synchronization	Yes		✓ Success	0

RESEARCH Installation – Known Issues

• When installing the RESEARCH component on a machine where the **Automatically adjust clock for Daylight Saving Time** option is not selected, the installation fails.

📸 Date and Time	\times
Date and Time Additional Clocks Internet Time	
Time Zone Settings	
Set the time zone:	
Time zone:	
(UTC+02:00) Jerusalem V	
Automatically adjust clock for Daylight Saving Time	
Current date and time: Monday, April 5, 2021, 12:06 PM	
New date and time: Monday, April 5, 2021, 1:06 PM	
OK Cancel	
Daylight Saving Time ends on Sunday, October 31, 2021 at 2:00 AM. The clock is not set to adjust for this change.	
☑ Notify me when the clock changes	
OK Cancel Apply	

In certain scenarios, the Research installation fails during the installation. If this happens and all eight Qlik services
are running, uninstall the Research component and then reinstall it. If any of the services are not running, contact
the Support team.



RESEARCH Installation – Creating a Virtual Proxy

A virtual proxy might be needed in the following conditions:

- · When the RESEARCH machine is in a domain
- · Other cases in which the RESEARCH machine has multiple host names

Note that a Qlik virtual proxy named bc is always created.

A virtual proxy can be used to handle different settings for the same physical server.

To define a virtual proxy, follow these steps:

- 1. In the Qlik Management Console (open a browser and use the following URL: https:// RESEARCH_Host_Name/ qmc), select **Virtual proxies** on the QMC start page or from the **Start** drop-down menu to display the overview.
- 2. In the Virtual Proxy window, select the pre-configured Central Proxy and click Edit.
- 3. Click Advanced, and in the Host white list section, click Add new value.
- 4. Add any names (not IPs) by which this server will be accessed. For example: localhost, myhostname.mylocaldomain.

All values added here are validated starting from the bottom level. If, for example, domain.com is added, this means that all values ending with domain.com will be approved. If subdomain.domain.com is added, this means that all values ending with subdomain.domain.com will be approved.

# Ref. +			G Help - Annuar -
Virtual process Edit on fault process			
 Virtual provins 	X Edit virtual prosp		
Cerra Pay Delat	IRANTIPICATION Description Prafix Is default virtual prory Season reactivity times d forunted	Exercise Procey (Collarity) The profits must be unspect for all virtual process used by the same proces service, as this differentiates the virtual profits must be unspect for all virtual (bend (previde)) valid characters for prefits are "s-r", "4-dr", "11, "11, "11, "11, "11, "11, "11, "	Proportion Sterification Autoritication Load beaming Advanced Taggetion
	Session 100kie header name	The sector costs header name must be unique for all virtual provise used by the same proxy service.	Ciert suffertication link Teps Custom properties
	Extended security environment Session-cookie domain	Calculate the checkbox to enclosed extended information about the client environment to the engine CS, decise, towards, and IP comp entended client information will prevent shared app usage between devices and attractive towards toward towards toward prevent towards appendix.	Associated Rens
	Additional response headers Meast white list		
	Apply Canod	Q Add new-ration	



A Blart +			😡 Help 👻 bevær 👻
Virtual proxies Edit Virtual proxy			
▲ Wrtual proxies	🗙 Edit virtual prany		
Central Prony (Defeur()	DENTIFICATION Description Prefix Is default virtual prony Session inactivity timeout (ninutes) Bession cookie header name Description cookie header name Edended security environment Session cookie domain Additional response headers		Properties Sentification Authenticution Load telanoling Advanced Integration Client authentication link Tags Custom properties Associated literes Process
	Host white list		
		Add new value	<u>v</u>
	Apply Cancel		

5. Click **Apply**. Wait for the service to restart; then, log in again, navigate back to the **Virtual Proxies** page, and repeat the steps above for the bc virtual proxy.

Description T 🕞	Prefa D	Session coulde header name	Is default virtual proxy	Linked to prazy service
	be	X-Qik-Session-bc	No	Yes
Central Proxy (Default)		X-Q/ik-Session	Yes	Yes

Help Center Installation (Optional)

BriefCam includes a Help Center that is accessible directly from the BriefCam product. If your organization allows access to BriefCam's online Help Center, this installation is not required. You only need to run the Help Center installer if you are installing BriefCam for an offline deployment.

Installation Steps

1. To install the offline help files, right-click on the BriefCamHelpCenter_<Version number>.exe file and select Run as administrator.

Note: If you are using the latest Windows Update and a Windows Defender alert appears, click the **More info** link and click **Run anyway**.







- 3. Select the location where you want to install the help files.
- 4. In the Endpoint field, enter the machine name or domain name where the help center will be accessible from.
- 5. Enter the database information.
- 6. Click Install.



	×
=BriefCam	BriefCam Help Center
Where do you want to instal	I the BriefCam Help Center?
C:\Program Files\BriefCam\WebService	es\Help Center\
① Setup requires 77 MB	
- Help Center Configuration	
Endpoint *	
PostgresSOL Database	
Databasa Host * @	
	A COLUMN AND A COLUMN A COLUMN A COLUMN
Database Port	5432
Back	Install

License Activation

BriefCam products should be activated and registered prior to first use. Use the supplied BriefCam License Activation tool and the provided product key to activate the software. Both online (Internet-connected) and offline activation modes are supported.



If a physical software protection dongle is used, no activation is required, and this section can be skipped entirely.

To extend or renew your software license, please contact your sales channel orBriefCam presales representative. In some cases, such as license extension or product renewal, product keys may be delivered by e-mail.

Online Activation

Online activation requires an active Internet connection.

To perform online activation:



1. Launch the BriefCam License Activation Tool from the VSServer machine's Start menu.



2. Enter your product key and click Activate.

BriefCam License Activation	×
Online Offline	
Product key:	
Settings	
Activate Close	

Upon successful activation, the following dialog will appear.

-B Activation completed successfully	×
Activation completed successfully!	
Tag ID:	
OK	

3. Click OK to close the dialog, then click Close in the main tool's window to close the License Activation tool.

Offline Activation

Offline activation is useful in cases where Internet connectivity is not readily available on the computer being used to install BriefCam products.

Two offline activation flows are supported – one intended primarily for use with a stand-alone PC lacking an Internet connection, and the other involving the use of an intermediary, Internet-connected PC.

To perform offline activation on a stand-alone PC lacking an Internet connection:

- 1. Launch the BriefCam License Activation tool.
- 2. Click the **Offline** tab to access offline activation.





3. Click **1.** Collect Information to generate a c2v (client to vendor) file, select or approve the destination in which it is to be stored, and click **Save**.

Save As		×
Libraries	Documents	Search Documents
Organize 👻 New fold	er)II 🔹 🔞
★ Favorites ■ Desktop	Documents library Includes: 2 locations	Arrange by: Folder 🔻
Downloads	Name	Date modified Type
Recent Places	Customer_activation.c2v	1/2/2014 4:50 PM C2V File
🥽 Libraries 🗮		
Documents		
J Music		
Pictures		
Videos		
I톺 Computer 실 Local Disk (C:)	٠ [[]]	
File name:		•
Save as type: Inform	mation file	
Hide Folders		Save Cancel

- 4. Send the c2v file to the Support team by logging into the BriefCam Portal at https://www.briefcam.com/support/ and opening a ticket where you can attach the c2v file. The BriefCam support group will then respond by e-mailing you the appropriate v2c (vendor to client) file required for activation.
- 5. Click **3.** Apply license in the main License Activation tool window, select the v2c file provided by the BriefCam support group when prompted to do so, and click **Open**.





6. The BriefCam product will now be activated. Once informed of successful product activation, click **OK** and close the License Activation tool.

To perform offline activation via an intermediary PC with an Internet connection:

1. Launch the BriefCam License Activation tool.

BriefCam License Activation	\times
Online Offline	
Product key:	
Settings	
Activate Close	

2. Click the **Offline** tab to access offline activation.





3. Click **1.** Collect Information to generate a c2v (client to vendor) file, select or approve the destination in which it is to be stored, and click **Save**.

Organize 👻 New f	older		8	• 0
ጵ Favorites 📃 Desktop	Documents li Includes: 2 location	brary	Arrange by:	older 🔻
Downloads	Name	*	Date modified	Туре
Recent Places	Customer_activa	tion.c2v	1/2/2014 4:50 PM	C2V File
🧊 Libraries	E			
Documents				
J Music				
Pictures				
📑 Videos				
📜 Computer				
🏭 Local Disk (C:)	v (111		
File name:				
Save as type: In	ormation file			

- 4. Transfer the c2v file (via a USB stick, for example) to an intermediary PC on which the License Activation tool is also installed and on which an Internet connection is available. Launch the License Activation tool on this PC, click the **Offline** tab for offline activation, and click **2. Retrieve license**.
- 5. Enter your product key in the appropriate field on the dialog that appears, then click the browse button (..) next to Information file: (input) to locate and load the c2v file generated on the offline PC.
| Retrieve License | | × |
|---------------------------|------------------------|---|
| Product key: | 123-456-789654654-6541 | |
| Information file: (input) | | |
| License file: (output) | | |
| OK Cancel | | |

- Click the browse button (..) next to License file: (output), select a desired destination in the browse dialog that pops up, and click Save. The License Activation tool will then generate and save an appropriate v2c (vendor to client) activation file.
- 7. Transfer the v2c file back to the offline PC and click **3. Apply license** in the main License Activation tool's window.

BriefCam License Activation X								
Online Offline								
✓ ✓ I. Collect information								
🕑 🥖 2. Retrieve license								
✓ ✓ 3. Apply license								

8. Select the v2c file generated via the intermediary PC when prompted to do so and click **Open**.

🖲 Open		×
↓ Libraries	► Documents ► 🗸 🗸	Search Documents
Organize 🔻 New folde	er	iii 🔹 🔟 🔞
☆ Favorites ■ Desktop	Documents library Includes: 2 locations	Arrange by: Folder 🔻
Downloads	Name	Date modified Type
E Recent Places	Customer_activation.v2c	1/2/2014 4:50 PM V2C File
Computer		
🗣 Network 🖉	•	•
File n.	ame:	License file Open Cancel

- 9. The BriefCam product will now be activated. Once informed of successful product activation, click **OK** and close the License Activation tool.
- 10. For details about how to launch BriefCam, see the BriefCam User Guide.

Network Security Considerations



- 1. The network segment hosting the BriefCam servers / virtual machines should be separated from other networks by a firewall and access should be granted only via ports configured in NGINX. For additional information, see the Installing and Configuring NGINX section.
- Administrative access to the servers, such as RDP, should be allowed either over VPN or from administration bastion hosts. A bastion host is a server that allows access to a private network from a public network, such as the internet. Bastion hosts are vulnerable to potential attacks and should be kept as secure as possible.
- 3. If DPI / WAF/ URL protection are required they should be implemented on the firewall when pointing to the operational BriefCam NGINX host.

Silent Installations

Silent installations are available for several installers: PostgreSQL, Server, Web Services, RESEARCH, MongoDB and RabbitMQ.

To use the silent installations:

- 1. Sign into the machine using an administrator account.
- 2. Open PowerShell.
- 3. Run the silent install commands listed below for each one of the components.
 - a. Select the relevant PowerShell command according to the type of user you want to run BriefCam's services (local user or domain user)
 - b. Fill out all the relevant parameters and pay special attention to SERVER_DOMAIN and SERVER_USER These parameters must be case sensitive.

Note that:

- In the commands below, you can change the APPDIR parameter to: "C:\Program Files\Briefcam" instead of using the env variable.
- Special characters are not supported for passwords.



PostgreSQL Installer

{ PostgresInstaller file name} /qn BC_DOMAIN="." BC_USER="{user to run BriefCam services}" BC_PWD="{BriefCam's user password}" DENY_USER_REMOTE_LOGIN="{true/false}" CREATE_BC_USER="NO" APPDIR="\$env:ProgramFiles\briefcam\ Briefcam PostgreSQL " DB_INSTALLDIR=C:\PostgreSQL POSTGRESQL_DATA_DIR="C:\PostgreSQL_Data" BRIEFCAM_S HARED_FOLDER="{BriefCam required shared folder}" POSTGRES_PORT=5432 POSTGRES_ADMIN_USER="dbadmin" P OSTGRES_ADMIN_PASSWORD="{db admin password}" POSTGRES_BC_USER="{DB user for BriefCam user}" POSTGRES_SC_USER="{DB user

Server Installer

Local User

{ ServerInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefCam\BriefCam Server" NOTIFICATION_PORT=7080 VIDEO GATEWAY_PORT=5010 POSTGRES_ADDRESS="{BriefCam DB hostname}" POSTGRES_PORT=5432 POSTGRES_BC_U SER="{DB user for BriefCam user}" POSTGRES_BC_PASSWORD="{DB password for BriefCam user}" SERVER_DOMAI N="." SERVER_USER="{user to run BriefCam services}" SERVER_PWD="{BriefCam's user password}" CREATE_SERVE R_USER="NO" BC_SHARED_DATA_FOLDER="\\{server hostname}\BriefCam" PASSPHRASE="{optional passphrase}" IS_VI DEO_STREAMING="YES" /!*v "{logfolder}\log.log"

Domain User

{ ServerInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefCam\BriefCam Server" NOTIFICATION_PORT=7080 VIDEO GATEWAY_PORT=5010 POSTGRES_ADDRESS="{BriefCam DB hostname}" POSTGRES_PORT=5432 POSTGRES_BC_U SER="{DB user for BriefCam user}" POSTGRES_BC_PASSWORD="{DB password for BriefCam user}" SERVER_DOMAI N="{domain name}" SERVER_USER="{user to run BriefCam services}" SERVER_PWD="{BriefCam's user password}" CREA TE_SERVER_USER="NO" BC_SHARED_DATA_FOLDER="\\{server hostname}\BriefCam" PASSPHRASE="{optional passph rase}" IS_VIDEO_STREAMING="YES" /I*v "{logfolder}\\og.log"

Processing Servers for Distributed Environments

In distributed environments, you run either the Local User or Domain User command given above. For all other server machines when only the processing server will run, use the command below. The difference here is that the IS_VIDEO_STREAMING parameter is set here to NO.

{ ServerInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefcam" NOTIFICATION_PORT=7080 VIDEOGATEWAY_PO RT=5010 POSTGRES_ADDRESS="{BriefCam DB hostname}" POSTGRES_PORT=5432 SERVER_DOMAIN="." SERVER_U SER="{local user to run BriefCam services}" SERVER_PWD="{BriefCam's user password}" CREATE_SERVER_USER="NO" BC_SHARED_DATA_FOLDER="\\{server hostname}\BriefCam" IS_VIDEO_STREAMING="NO" /I*v "{logfolder}\log.log"

Web Services Installer

Local User

{ WebInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefcam" WS_HOST="\$env:computername" WS_PORT=80 CREA TE_SERVER_USER="NO" SERVER_DOMAIN="." WS_USER="{user to run BriefCam web services}" WS_PWD="BriefCam's user password}" POSTGRES_ADDRESS="{BriefCam DB hostname}" POSTGRES_PORT=5432 POSTGRES_BC_USER="{D B user for BriefCam user}" POSTGRES_BC_PASSWORD="{DB password for BriefCam user}" BRIEFCAM_SHARE="\\{server hostname}\BriefCam" LICENSE_SERVER_ADDR="{server hostname}" PASSPHRASE="{optional passphrase}" USAGE_DAT A_SETTINGS="{true/false}" /I*v "{logfolder}\log.log"

Domain User

{ WebInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefcam" WS_HOST="\$env:computername" WS_PORT=80 CREA TE_SERVER_USER="NO" SERVER_DOMAIN="{domain name}" WS_USER="{user to run BriefCam web services}" WS_PW



D="BriefCam's user password}" POSTGRES_ADDRESS="{BriefCam DB hostname}" POSTGRES_PORT=5432 POSTGRE S_BC_USER="{DB user for BriefCam user}" POSTGRES_BC_PASSWORD="{DB password for BriefCam user}" BRIEFCA M_SHARE="\\{server hostname}\BriefCam" LICENSE_SERVER_ADDR="{server hostname}" PASSPHRASE="{optional passp hrase}" USAGE_DATA_SETTINGS="{true/false}" //*v "{logfolder}\log.log"

RESEARCH Installer

Silent Installation with Default Parameters

{ ResearchInstaller file name}

Silent Installation with Non-Default Parameters

{ ResearchInstaller file name} --SERVER_PORT "8090" --RESEARCH_ENDPOINT "{RESEARCH hostname or load balancer endpoint}" --POSTGRES_ADDRESS "{BriefCam DB hostname}" --POSTGRES_PORT "5432" --POSTGRES_BC_USER "{DB user for BriefCam user}" --POSTGRES_BC_PASSWORD "{DB password for BriefCam user}" --DOMAIN_NAME "." --BRIEFC AM_USER "{user to run BriefCam services}" --BRIEFCAM_USER_PWD "{BriefCam's user password} --QLIK_DATA_FOLDER "C:\QlikShare" --QLIK_BACKUP_FOLDER "C:\Program Files\BriefCam\qlikbackup"

Custom LEF License

{ ResearchInstaller file name} --SERVER_PORT "8090" --RESEARCH_ENDPOINT "{RESEARCH hostname or load balancer endpoint} --POSTGRES_ADDRESS "{BriefCam DB hostname}" --POSTGRES_PORT "5432" --POSTGRES_BC_USER "{DB user for BriefCam user}" --POSTGRES_BC_PASSWORD "{DB password for BriefCam user}" --QLIK_LICENSE_SERIAL "972 1750115078957" --QLIK_LICENSE_CONTROL "10565" --QLIK_LICENSE_LEF "{Qlik license lef}`n`ANALYZER`;'20`;`;`n`GE OANALYTICS`;'YES`;`;`n`GEOPLUS`;`YES`;`;`n`IGNORE_TOKENS`;'YES`;`;`n`OVERAGE`;`NO`;`;`n`PRODUCTLEVEL`;'5 0`;`;'2023`-01`-20`n`PROFESSIONAL`;'4`;`;`n`SPECIAL_EDITION`;`NFR`;`;`n`SPECIAL_EDITION`;`OEM`;`;`n`TIMELIMI T`;'VALUE`;`;'2023`-01`-'21`n`WEBCONNECTORS`;'YES`;`;`n`4YK2`-PAQN`-NDSB`-7YN6`-L2JX" --DOMAIN_NAME "." --B RIEFCAM_USER "{user to run BriefCam services}" --BRIEFCAM_USER_PWD "{BriefCam's user password} --QLIK_DATA_F OLDER "C:\QlikShare" --QLIK_BACKUP_FOLDER "C:\Program Files\BriefCam\qlikbackup"

Distributed Installation

{ ResearchInstaller file name} --SERVER_PORT "8090" --RESEARCH_ENDPOINT "{RESEARCH hostname or load balancer endpoint} --POSTGRES_ADDRESS "{BriefCam DB hostname}" --POSTGRES_PORT "5432" --POSTGRES_BC_USER "{DB user for BriefCam user}" --POSTGRES_BC_PASSWORD "{DB password for BriefCam user}" --DOMAIN_NAME "." --BRIEFC AM_USER "{user to run BriefCam services}" --BRIEFCAM_USER_PWD "{BriefCam's user password} --QLIK_DATA_FOLDER "C:\QlikShare" --QLIK_BACKUP_FOLDER "C:\Program Files\BriefCam\qlikbackup"

MongoDB

{ MongoDBInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefcam" MONGODB_PORT=27017 POSTGRES_ADDRES S="{BriefCam DB hostname}" POSTGRES_PORT=5432

RabbitMQ

{ RabbitMQInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefcam" POSTGRES_ADDRESS="{BriefCam DB hostnam e}" POSTGRES_PORT=5432 POSTGRES_BC_USER="{DB user for BriefCam user}" POSTGRES_BC_USER_PASSWOR D="{DB password for BriefCam user}"

VMS Plugins

Silent installations are also available for the Genetec, Milestone, NiceVision and VisionHub plugins.





Upgrading

Ø

Silent installations for upgrading are not supported for BriefCam version 2024 R2.

Run the following commands to upgrade the PostgreSQL, Server and Web Services to a later version:

PostgreSQL

{PostgreSQLInstaller file name} exe /qn /l*v "{logfolder}\log.log"

Server

{ServerInstaller file name} /qn SERVER_PWD_UPGRADE="{bc_user_password}" /l*v "{logfolder}\log.log"

Web Services

{WebInstaller file name} /qn WS_PWD="{bc_user_password}" /l*v "{logfolder}\log.log"

Large Scale Deployments

Large scale deployments are deployments that handle thousands of video hours per day and usually include 10 servers or more.

This section describes recommended components that can be used to configure a large scale deployment.

Logging and Monitoring

Deploying a Graylog Server

Load Balancers

MongoDB Installation

Logging and Monitoring

When deploying a large scale system, there is a need to monitor the system and the logs from a single place. For this purpose, BriefCam recommends working with the following:

- Prometheus[®] and Grafana technology for large scale monitoring and monitoring dashboards.
- GrayLog for large scale centralized logging

The above components are deployed separately on a dedicated Linux instance.

For additional information about running the Prometheus and Grafana scripts, contact BriefCam Support.

Deploying a Graylog Server

For large scale deployments, BriefCam recommends using the Graylog log management platform to collect the various logs into a single place to help debug the system.

To deploy a Graylog server you need a dedicated Linux server.

When you carry out all the steps below, the following internal components that are needed for Graylog to run will be installed:





- MongoDB A separate database instance for this purpose.
- ElasticSearch This is a middle layer through which the database and Graylog communicate.
- Graylog

In addition, as part of the installation, an agent is deployed on each one of the BriefCam servers. The agent will be responsible for sending logs to the Graylog server.



Prerequisites

- · BriefCam is already deployed on your site.
- The Linux server must be reachable from all BriefCam machines via HTTP/TCP.

Platform Requirements

The Linux server must be ubuntu 18.04.* LTS with the following specifications:

- 1 x i7-10700K CPU
- 64GB RAM
- 256GB SSD

Other Requirements

• All operations need to be performed by a user with sudo permissions.

Installing Graylog on the Linux Server

Installing Graylog on the Linux server consists of the following steps:

- 1. Check that SSH is installed and enabled
- 2. Install Docker Runtime
- 3. Copy the installation files
- 4. Configure and activate the Graylog server engine
- 5. Configure the Graylog collectors
- 6. Configure BriefCam Servers to Send Logs to the Graylog Server



Step 1: Check that SSH is installed and Enabled

- 1. Log into the Linux server.
- 2. Open a terminal window.
- 3. Issue the following commands:

sudo apt update

sudo apt install openssh-server

4. Check that the ssh daemon (service) is up and running:

sudo systemctl status ssh

- 5. You should see text similar to this: Active: active (running) :
- 6. Type q to return to the console.
- 7. Allow ssh in the firewall:

sudo ufw allow ssh

8. Terminate the shell session:

sudo ufw allow ssh

Step 2: Install Docker Runtime

To install Docker Runtime:

1. Open the SSH session to the server machine:

ssh jjcale@tulsa-sound or jjcale@{Server IP address}

- 2. Enter your password to connect to the SSH session.
- 3. Update the apt package manager:

sudo apt-get update

4. Install docker general dependencies:

sudo apt-get install apt-transport-https ca-certificates curl gnupg-agent software-properties-common

5. Install a docker runtime PGP key:

curl -fsSLhttps://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

6. Add a docker runtime repository:

sudo add-apt-repository \ "deb [arch=amd64] https://download.docker.com/linux/ubuntu \$(lsb_release -cs) stable"

7. Install the docker run time itself and direct dependencies:

sudo apt-get update sudo apt-get install docker-ce docker-ce-cli containerd.io



8. Test the docker installation. This should produce a short hello message to the console without errors:

sudo docker run hello-world

The output will look similar to the following:

Unable to find image 'hello-world:latest' locally latest: Pulling from library/hello-world 0e03bdcc26d7: Pull complete Digest: sha256:e7c70bb24b462baa86c102610182e3efcb12a04854e8c582838d92970a09f323 Status: Downloaded newer image for hello-world:latestHello from Docker! This message shows that your installation appears to be working correctly.

9. Add the 'docker' user to the group of the user you are logged in with:

sudo usermod -aG docker jjcale

- 10. Make sure to log out or exit the current session in order for the usermod command to take effect.
- 11. Install docker-compose runtime:

sudo curl -L "https://github.com/docker/compose/releases/download/1.27.4/docker-compose-\$(uname -s)-\$(uname-m)" -o /usr/local/bin/docker-compose

12. Give docker-compose execution permissions:



Step 3: Copy and Extract the Installation Files

- 1. Copy the files from the machine that hosts the installation file (usually a Windows machine) to the Linux server.
- 2. Use openssh for Windows or winscp: https://winscp.net/download/WinSCP-5.17.9-Setup.exe
- 3. Run: scp path\to\package\server.zip jjcale@192.168.0.3:/home/jjcale/
- 4. ssh to the server machine and extract the package files:

cd ~

unzip server.zip

cd server

Step 4: Configure and Activate the Graylog Server Engine

- 1. Open the docker-compose-graylog.yml file with a text editor and set: GRAYLOG HTTP EXTERNAL URI=server ip
- Leave the port as is. For example: GRAYLOG_HTTP_EXTERNAL_URI=http ://{Server IP address}:9000/
- 3. Create a directory for the Graylog files:

sudo mkdir-p /opt/briefcam/graylog

4. Copy the Graylog compose file to the newly created directory:

sudo cp docker-compose-graylog.yml /opt/briefcam/graylog/

5. Create a Graylog service by copying graylog-docker.service to /etc/systemd/system:

sudo cp graylog-docker.service /etc/systemd/system/

6. Enable the new service for when the machine is restarted:

sudo systemctl daemon-reload sudo systemctl enable graylog-docker





7. Start the Graylog service:

sudo systemctl start graylog-docker



The first start may take a couple of minutes since the pulling and starting of new docker containers takes some time.

Step 5: Configure Graylog Collectors

- 1. Log into the Graylog web interface.
- 2. Open a browser and go to the following address: http://{Server IP address}:9000
- 3. The credentials are:

user: admin

password: admin

- 4. Go to system/inputs.
- 5. Create GELF TCP input:
 - a. Check the **Global** checkbox.
 - b. Add a title, such as: "Win TCP".
 - c. Set the port to 12201 (the default).
- 6. Create GELF UDP input:
 - a. Check the Global checkbox.
 - b. Add a title, such as: "Win UDP".
 - c. Set the port to 12201 (the default).
- 7. Go to system/sidecars.
- 8. Create an API token.
 - a. Click Create or reuse a token for the graylog-sidecar user.
 - b. Add a token name, such as: "Win token".
 - c. Click Create Token.
- 9. Save the token or copy it to the clipboard.

Step 6: Configure BriefCam Servers to Send Logs to the Graylog Server

The following steps should be carried out on every BriefCam server.

Step a: Copy the Installation Package Files

Log into the machine remotely (RDP) and copy the following files from the installation links to each of the BriefCam servers:

graylog sidecar installer 1.0.2-1.exe

nxlog-ce-2.10.2150.msi

windows_exporter-0.14.0-amd64.msi

Step b: Install the Logs Collector

1. Install the nxlog collector by running the following in PowerShell with elevated administrative permissions:

..\nxlog-ce-2.10.2150.msi/qn

2. The first step creates services on your machine. In this step, you need to deactivate the system services (Graylog only needs the binaries) by running the following in PowerShell:





cd 'C:\Program Files (x86)\nxlog\'.\nxlog.exe-u

3. Install the Graylog sidecar as a service with the Graylog server IP and the saved API token by running the following in PowerShell:

.\graylog_sidecar_installer_1.0.0-1.exe/S-SERVERURL="http://{Server IP address }:9000/api"-APITOKEN="<apitoken>"

Step c: Configure the Sidecar

- 1. Edit the C:\Program Files\Graylog\sidecar\sidecar.yml file and uncomment the following entries:
 - cache_path
 - log_path
 - collector_configuration_directory
 - collector_binaries_whitelist and the accompanying'- "C:\\Program Files
 (x86) \\nxlog\\nxlog.exe"' entry
- 2. Save the file.
- 3. Register the sidecar as a service and start it by issuing the following commands from the C:\Program Files\ Graylog\sidecar directory:

C:\Program Files\Graylog\sidecar> .\graylog-sidecar.exe -service install

C:\Program Files\Graylog\sidecar> .\graylog-sidecar.exe -service start

Step d: Create the Graylog Configuration

- 1. Open the Graylog UI and navigate to system/sidecars.
- 2. Find your connected machine and click manage sidecar.
- 3. Select the nxlog checkbox.
- 4. Click Configuration.
- 5. Under log collectors, click edit in the nxlog Windows version.
- 6. Give a name, such as "win-nxlog".
- 7. In the default template section, update File entry in the <Input file> section to the desired log directory.
- 8. In the <Output gelf> section, set the Host IP to the correct connected machine address (Server IP address)
- 9. Click Update.

Load Balancers

To serve a large number of users or real-time channels simultaneously, you can deploy multiple instances of web services behind a load balancer. The load balancer will distribute the traffic efficiently and will enable both scaling and high availability. For this purpose, BriefCam recommends working with the NGINX load balancer.

For additional information, see Working with SSL: Using Load Balancer (NGINX) as an SSL Terminator.

MongoDB Installation

MongoDB is a document-oriented database that stores data in JSON-like documents with a dynamic schema. BriefCam's metadata (BLOBs) are usually stored in a relational database (PostgreSQL). In large scale deployments, where the amount of data used for these blobs becomes very high, it is recommended deploying a MongoDB database, which has native support for horizontal scaling, adding more instances and distributing the data efficiently among them.

It is recommended to install MongoDB before installing the BriefCam Server. If you installed the BriefCam Server before MongoDB, restart VSService on all BriefCam Servers.



Installing MongoDB on an existing BriefCam environment is not supported.

=BriefCam



It is recommended to install MongoDB before installing the BriefCam Server. If you installed the BriefCam Server before MongoDB, restart VSService on all BriefCam Servers.

Installation Steps

- 1. To run the BriefCam MongoDB Installation wizard, double-click BriefCamMongoDB_<Version number>.exe.
- 2. In the Welcome screen, click Get Started.



3. To proceed with the installation, read and accept the License Agreement terms.

4. Click **Next** to continue.



The following screen will appear.



BriefCam	Install BriefCam MongoDE
Account Settings -	
This user will run	BriefCam's services
O Use an existin	ng user 🛛 Create a new user
Domain	
If the user is a loca	al user, enter a period (.) in the Domain field
Username	BCuser
Password	******
Validate Existing User	
Back	Next

- 5. Select whether to use an existing account or create a new account.
- 6. Enter the username and the password. The user needs to have administrator rights on the local machine.



Note that special characters are not supported in the **Password** field.

7. If the user is a domain user, enter the domain name. If the user is a local user, enter a period (.).



- 8. If you selected to use an existing user, you can click **Validate Existing User** to check that the user credentials are valid.
- For new users, you can select the Deny remote login for the BriefCam user checkbox to prevent the BriefCam user from remotely logging into the machine. If the checkbox is not checked, it will be possible to give the BriefCam user access to remote login (depending on your organization's policies).
- 10. Click Next.



The following screen will appear.

BriefCam	Install BriefCam MongoDB
Where do you want to install	MongoDB?
:\Program Files\BriefCam\MongoDB\	
Space required: 178 MB	
MongoDB Database	
Port	27017
PostgreSQL Database	
Database Host 🛛 💿	Product1
Database Port	5432
Application User	brief
Application Password	****
Test Database Connection	
Dask	Install

- 11. Select the location where you want to install MongoDB.
- 12. Enter the path for MongoDB.
- 13. Enter the server address and path where the PostgreSQL database was installed and the application user and password. Note that special characters are not supported for passwords.
- 14. Click the Test Database Connection button.
- 15. Click Install.

VMS Integrations

BriefCam's VMS Integration Levels

Supported VMS Table

American Dynamics Integration

Arcanes Technology Integration





- Avigilon Integration
- Axis Integration
- **Bosch Integration**
- CASD Integration
- **Dallmeier Integration**
- **Digifort Integration**
- **Exacq Integration**
- **FLIR Integration**
- Genetec Integration
- **GeoVision Integration**
- **Geutebruck Integration**
- IndigoVision Integration
- IPOrchid Fusion Integration
- **ISS Integration**
- LenelS2 OnGuard Integration
- **Milestone Integration**
- NX (Network Optix) Integration
- Qognify Nicevision Integration
- Qognify Ocularis and Qognify VMS Integration
- Salient Integration
- Teleste Integration
- Verint Integration

General VMS Known Issue

RTSP-based integrations do not work when user's credentials include the @ sign.

BriefCam's VMS Integration Levels

There are various levels of integration with BriefCam and the various requirements needed for these integrations are referenced below.

Leve	Name	Description	Applicable BriefCam Modules	Applicable BriefCam Products	Integration Scope
L1	Forensics	Integration for on-demand search, for post event	REVIEW	Rapid	Backend



	only integration	investigations		Review	only
L2	Cross modules integration	Level 1 integration and real time integration, for continuous video streaming and processing	REVIEW, RESPOND, RESEARCH	Insights, Protect	Backend only
2a	Real time alerts integration	Level 2 integration with real time alerts sent to the VMS client	REVIEW, RESPOND, RESEARCH	Insights, Protect	Backend only
3	Client integration	Level 1 or 2 integration extended by the BriefCam client incorporated in the VMS UI, ideally with SSO integration	REVIEW, RESPOND, RESEARCH		Frontend and if SSO is used backend
4	Workflow integration	Level 3 integration enhanced with BriefCam functions added to the VMS player (e.g. launch a Synopsis request, add videos to a case from VMS live or playback streams)	REVIEW, RESPOND, RESEARCH		Frontend only

See also:

Supported VMS Matrix

Supported VMS Table

The most up-to-date list of supported VMSs (including changes made after the release date) can be found here: https://www.briefcam.com/partners/supported-vms/.

To obtain integrations created by a VMS partner and for support using these integrations, contact the VMS partner.

Third Party Integrations

There are third parties who have integrated their VMS with BriefCam including the VMSs listed below.

For information about licenses, installing, configuring, and working with these integrations, contact the third party. For the most up-to-date information about all VMS integrations, see: https://www.briefcam.com/partners/supported-vms/.

Note that to use any third party integration with BriefCam, you need to also install BriefCam's VIA plugin: BriefCamVMSIntegrationAPI_VIA_[version number].exe.

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	Support
i-PRO Americas	Video Insight	7.6	5.4.1	L2a	1-800-513-5417 (USA and Canada) or +1-713-621-9779 (international)



VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	Support
ISS	SecurOS	11.8	2024 R2 HF4	L3	https://support.issivs.com/
Qognify	Ocularis	6.1	2023 M1	L2a + L3	
Surveillus	Commander	6.3	6.4	L2a	
Synectics	Synergy 3	24.1.6	2023 M1	L2a + L3	technical@synx.com

BriefCam VMS Integration Plugin Installation

VMS plugin installations are available for BriefCam Protect, Insights, and Rapid Review.

You can install one or more VMS-specific BriefCam integration plugins to subsequently enable the BriefCam Server to connect to one more VMS environment (multiple simultaneous integrations are supported). The VMS integration Plugin Installation, as well as the VMS SDK (for relevant VMSs) is required to be installed on every machine on which the BriefCam Server/ Processing Server/Alert Processing Server is installed.

Plugins are available for selected VMS systems (refer to the BriefCam's Supported VMS table). Each installed plug-in will be embedded on the BriefCam Server for subsequent selection within the BriefCam Server Admin application. For more information, see Camera and VMS Configuration in the BriefCam Administrator Guide.

The VMS plug-in installations will deploy the required prerequisites as needed per plug-in.

To install the plug-ins:

1. Run the VMS Integration Plugin Installation on the BriefCam Server by right-clicking on the BriefCam<VMS name>Plugin <Version number>.exe file and selecting Run as administrator.

Note: If you are using the latest Windows Update and a Windows Defender alert appears, click the **More info** link and click **Run anyway**.



- 2. The VMS integration Plugin Installation is required to be installed on every machine on which the BriefCam Server/ Processing Server is installed.
- 3. Read and accept the License Agreement terms.
- 4. Select the path to the plugin installation directory. The path should be the same directory as the BriefCam Server directory.
- 5. By default, it is set to C:\Program Files\BriefCam\BriefCam Server\.
- 6. Click **Install** and continue as instructed by following the installation procedure.



General VMS Known Issue

RTSP-based integrations do not work when user's credentials include special characters, such as @ and #.

American Dynamics Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support	Additional License Required	
American Dynamics	VideoEdge	6.3	2024 R2 HF4	Integration for on-demand and real-time (L2)	Yes	A floating license is required for each recorder.	

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

VMS SDK

Prior to the plugin installation, install American Dynamics SDK 5.3.3.

Known Limitations

- Bounding boxes when playing the original video are not supported.
- Support for the H.265 format is done per request. If you want to use the H.265 format with this VMS, please contact BriefCam's support.
- In American Dynamics integrations, when fetching fails due to a corrupted file in on-demand requests, the decoding
 partially fails.

Arcanes Technology Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Arcanes Technology	VXCore	6.5.4	6.4 Hot Fix 1	Integration for on-demand and real- time (L2)	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

=BriefCam

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Installation and Configuration

- 1. Run the plugin.
- 2. Generate and set up the VXCore API Access token.
 - a. In VXCore, navigate to Extensions > API access and click the ADD button.



- b. Copy the Connection key. You will need this key when configuring the connection on BriefCam.
- c. Enter the name of the API access token and check the Access to system informations checkbox.



d. From the CAMERAS tab, select all cameras that will be used by BriefCam and click APPLY.



1. In the BriefCam Administrator Console, open the Settings section and click Camera Management.





2. Click the Add Directory button.

BriefCam ADMIN	CAMERA MANAGEMENT								₽ ⊙	() Spi Ox
🗊 Denta	Licenses 1000 Remaining 925 Activated 45									
2. User Management A										
🕀 Deployment 👻	Search Directories. Q		Search/Carr	Q					Dista	y only analytic cameras
Horto	Doe store entrance camera (Disabled)	1		Name	Activation	Enabled	Overhead	Counting	Path	
GPUN	Office entrance (0)	1	0	Serv SNC VB6m/VM6m	2021/07/011-		0	0	MIL2083/-	a 0
Services	 Office conidor (10) 	1	0	ANS Q5125 Mic III Netw	2021/07/011-	•		0	/ML20R3/	a 0
🖓 Settas 🔍 👻				AKSP2255-C/ENetwor	2021-07-011				/ML2083/_	4
Carrier's Management										
Environment Settings										
Localization										
Events Threshold										
<u>⊴i</u> Athlin ∧										
	Add Directory								0 · · · here he ha	pr. 200 Andr

- In the Add Directory dialog, fill in the details of VXCore.
 In the User Name field you need to enter a single space only. A user name is not needed for the connection.
 In the Password field, enter the API access token generated in the VXCore VMS.



6. Ensure that the firewall is accepting connections for RTSP.

Configuration File

After running the plugin, you can customize the BriefCam.VXCore.ini file, which by default is located at: C:\Program Files\BriefCam\BriefCam\BriefCam Server\plugins.

*C:\Program Files\BriefCam\BriefCam Server\plugins\BriefCam.VXCore.ini	\times
File Edit Search View Encoding Language Settings Tools Macro Run Plugins	
Window ?	х
🕞 🚔 🖷 👒 🕞 🙏 🖌 🐚 🏠 ⊃ 🗲 📾 🦕 🔍 🛸 🔚 📰 🎩	>>
BriefCam.VXCore.ini 🔀	
<pre>l ;don't remove this string</pre>	^
2 [Live]	
3 ;LiveDelayMSec = 0	
4 ;UseHTTPSLiveURL = false	
5 L	
6 [Fetching]	
7 ; FFmpegPath = "FFMPEG.EXE"	
	~
lengt Ln : 1 Col : 2 Pos : 2 Unix (LF) UTF-8-BOM IN	S

The settings in the file are:

· LiveDelayMSec – Sets up a time delay when the VMS and RSTP have mismatched times.

When a live image is received from the recorder/camera, the time of the frame is also received. If this time is invalid, BriefCam will set the frame time to the current time minus the value set in the LiveDelayMSec parameter.

For example, if a frame is received with time 01/01/1900 00:00:00, BriefCam will override this time to the current time of the machine and will subtract the configured delay, which by default is 0.

- UseHTTPSLiveURL Uses HTTPS for the live streaming connection.
- FFmpegPath Sets up the location of the FFMPEG, if it's not installed in the default location.



Archiving the Exported File from VXCore

The archive is done because the export consists of multiple files that need to be handled together by the decoder. If they are uploaded separately, the decoder does not know that these files are part of the same export.

For example, a 10-minute export will contain 10 pairs of VXSEEK and VXVIDEO files, one pair for each minute of the export. The VXSEEK file contains the metadata needed to read the VXVIDEO file.

Generating the Archive

To generate the archive that needs to be uploaded to BriefCam:

- 1. Generate the video export from VXCORE ACCESS.
 - a. In VXCORE ACCESS, in the left toolbar, navigate to the Video tab.



b. In the right pane, click the **Raw video dump** button.



c. Set the export start and end time and click the Telecharger les donnees button to initiate the export.





- d. Select the folder on the disk where the export should be saved and confirm. The resulting folder name should be similar to "vxcore_b3c1-9d25-53ca-4d51".
- 2. Copy both scripts (.ps1 and .bat), which are located in the BriefCam installation directory's plugins folder, into the same folder where the VXCore export folder is located. The folder should look like this:

vx.core_b3c1-9d25-53ca-4d51	20/03/2023 14:10	File folder	
vxcore_archiver.bat	20/03/2023 14:08	Windows Batch File	1 KB
xcore_archiver.ps1	20/03/2023 14:10	Windows PowerS	3 KB

- 3. Double-click the vxcore_archiver.bat file. The scripts will look for a VXCore export folder in the same directory where the two scripts are located.
- 4. Once the archive is ready, a new File Explorer window will open to the path where the .vxcorezip archive file is located. (The .vxcorezip file was created by the script.) This file can then be uploaded to BriefCam for decoding.
- 5. In order for BriefCam to decode the export correctly, the following line needs to be uncommented in the RenderingService.ini configuration file:



The vxcore_archiver.ps1 file can be called as a standalone from a PowerShell terminal. For more information, run the help command: vxcore_archiver.ps1 -help.

VXCore Configuration Settings

In the BriefCam installation directory's plugins folder, you'll find the BriefCam.VXCore.ini file's Decoding section. You can use these settings to further configure your system.

9	[Decoding]
10	;StreamID = "video1"
11	;FileReaderQueue = 100
12	;FileReaderQueueMax = 300
13	;FileReaderDelayMS = 20
14	;InitExtractorFrameLimit = 100
15	;InitDecoderBufferSizeKB = 512
16	;DecoderBufferSizeMB = 2

- StreamID The video stream that should be decoded from the VXCore export. This is used in cases where the camera, from which the native video is exported, records multiple streams (e.g., with multiple resolutions). The first stream is always named "video1" (as is the default value of this setting) and additional streams will be named "video2", "video3", etc.
- FileReaderQueue The number of frames that should be buffered from the native export before waiting for pending frames to be decoded. Increase this setting if the ffmpeg decoder (used by the VXCore decoder for decoding single frames) reports increasing its buffer in the logs. Look for the following warning:
 "FFMpegDecoder::AppendChunkToBuffer. increased buffer size from <x> to <y>".
- FileReaderQueueMax The maximum value the file reader queue will be increased to during decoding. This value should be set higher than FileReaderQueue.
- FileReaderDelayMS How long the decoder should wait before trying to extract more frames from the native export once the buffer limit is reached.
- InitExtractorFrameLimit How many frames the decoder should check for a valid first frame before discarding the native export as invalid. Increase this setting if there is a large number of reported invalid decodings. Look for the following error: "[VXCore Decoder] Initialization failed.".
- InitDecoderBufferSizeKB How many KB of frame data the decoder should use for a valid initialization before discarding the native export as invalid. Increase this setting if there is a large number of reported invalid decodings. Look for the following error: "[VXCore Decoder] Could not decode <uploaded native export path>".
- DecoderBufferSizeMB The initial size of the FFMPEG decoder buffer. Increase this setting if the ffmpeg decoder reports increasing its buffer in the logs. Look for the following warning: "FFMpegDecoder::AppendChunkToBuffer. increased buffer size from <x> to <y>".

Avigilon Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Avigilon	Avigilon Control Center	7.14	2024 R2 HF4	Integration for on-demand and real- time (L2)	No
Avigilon	Avigilon Control Center	7.12	2023 M1	Integration for on-demand and real- time (L2)	No

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

VMS SDK

- 1. Prior to the plugin installation, install the relevant Avigilon SDK.
 - For Avigilon 7.12 and 7.14, you need SDK version 6.14.22.6.
- 2. Install the Avigilon SDK on the BriefCam server.
- 3. If the Processing Sever and/or Alert Processing Server is installed on a dedicated machine, also install the Avigilon SDK on the BriefCam Processing Server and/or Alert Processing Server.

Recommended Configuration for Avigilon Cameras

To improve the Avigilon plugin's performance with Avigilon cameras, it is recommended to:

- 1. In Avigilon Control Center:
 - a. Set the Format field to AVE.
 - b. Set the Stream Mode field to Dual Mode.
- 2. In the BriefCam Administrator Console:
 - a. Change the maxProcessingTaskLengthInMinutes environment setting to 30.
 - b. Restart the **Processing Service**.

This change breaks the on-demand videos into smaller chunks (of 30 minutes instead of 4 hours by default), improving the amount of processing that is done in parallel, which leads to better resource utilization and improved performance. However, this change has several side effects:

- There will be a warmup at the beginning of every chunk. The warmup is a short processing period that learns the video characteristics and calibrates BriefCam's Machine Learning engine. The warmup consists of the learning of the background, size, speed, and proximity geometry, which need to be learnt in each video chunk. The warmup period usually lasts for the first few minutes of the processed chunk.
- Persons in the beginning of a chunk will not have the geometry information that accurately places them in the scene. Therefore, they cannot be used in the **Proximity** filter.
- Size and speed filters applied on objects appearing in the beginning of a chunk may show incorrect measurements.
- · Objects that appear in two consecutive chunks, could be identified as two separate objects.

Known Limitations

- In Avigilon integrations, slow processing was observed when working with 4K cameras. This is because of slow
 decoding due to proprietary format.
- In on-demand scenarios:
 - Although the processing is reported to be completed successfully, occasional frames may be dropped and indicated in the logs.
 - In certain scenarios, the fetching of videos is slow. To solve this issue, define additional parallel workers or reduce the camera resolution. For additional information, see the Recommended Configuration for Avigilon Cameras section above.
- Support for the H.265 format is done per request. If you want to use the H.265 format with this VMS, please contact BriefCam's support.

See also: VMS Integration Issues





Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Axis	Axis ACS	5.33	6.4 Hot Fix 1	Real time alerts integration (L2a)	No

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Note that the name of the plugin is: BriefcamACSPlugin_[version number].exe.

Ports Required

The following port should be available when installing the plugin.

Axis Version	Port #
Axis ACS v5.X	55756
Axis ACS v6.X	29204

For Axis ACS v6.X:

- 1. Open the BriefCam.ACSIntegration.ini file, which is located by default at: C:\Program Files\ BriefCam\BriefCam Server\plugins.
- Change the DefaultPort parameter to 29204 and uncomment the row.





Sending Alerts to Axis

Alerts can be sent to Axis ACS. To enable this functionality, carry out the steps below.

BriefCam Configuration

In the **Environment Settings** section, there are three settings relevant for sending alerts outside of BriefCam (see the image below):

- 1. To send alerts outside of BriefCam, set the Respond.AlertsPublishingEnabled setting to true.
- 2. To send alerts to a VMS, check that the Respond.AlertsPublishingToVMSEnabled setting is set to true.
- 3. To change the polling interval, use the Respond.AlertsPublishingIntervalInMilliseconds setting.

B	rief Cam ADMIN	6	enviro	NMENT S	ETT	INGS			
Ħ	Events						_		
2,	User Management	^	publish		×	Type Y		Show settings that have be	en changed
\$	Deployment	^	Scope	Туре		Key		Value	Default Value
G	Settings	*	GLO	Common	[Respond.AlertsPublishingEnabled		false	faise
	Camera Management		GLO	VS-Server		Respond.AlertPublisherAcceptUnsafeC		true	true
	Environment Settings		GLO	VS-Server	ſ	Respond.AlertsPublishingToVMSEnabled		true	true
	Localization		<i>C</i> 10	100.0		0		****	1000
	Events Threshold		GLO	VS-Server	_	Respond.AlertsPublishingIntervalInMilL.		1000	1000
sí	Activities	^	GLO	Common		AkkaHostConfig		akka : { loggers : ["Br	
88	Dashboards	^	GLO	Common		Administration.SystemEventsPublishin		false	false
			GLO	Common		Administration.SystemEventsPublishin		Critical	Critical

4. If you make changes to the settings, you need to restart or start the VSServer service.

Axis Configuration

On the Axis side you need a full admin user.

1. On the ACS server (incoming):



- a. For Axis ACS v5.X, open UDP port 55756.
- b. For Axis ACS v6.X, open UDP port 29204.
 2. To configure the VMS side's trigger, go to the Axis Camera System's Configuration tab, open the Recording and events folder and then the Action rules option.
- 3. Click New.

Configuration × 🖵 AXIS P1468-LE	+ (serr.sm)	::≡
Type to filter	Action rules	
🗣 Devices	Create and edit action rules by selecting triggers, actions, and schedules. Type to filter	
Storage	Rule Trippers: External HTTPS tripper 'TeatTripper'	
Recording and events	Schedule Alvays on Actions: Raise alarm 'BrielCam Alarm'	
Schedules		
Recording method		
I/O ports		
Action rules		
堂 Client		
 Connected services 		
Server		
Licenses		
Security	New Edit Copy	Remove

4. Add a new trigger by clicking **Add**.

Тург	e to filter		Action	rules		
9 g	Devices	I.	Create and ed	it action rules by selecting triggers, actions, and schedules.		
000	Storage	L		New Rule	? X	
€.	Recording and events	L	<u>Steps</u> Triggers Actions	Triggers Triggers describe when a rule should become active.		
	Schedules	L	Schedule	All triggers must be active simultaneously to trigger the actions	Add	
	Recording method		Details			
	I/O ports				Edit	
	Action rules				Remove	
Ŷ	Client			Help Cancel < Back Next >	Finish	
\bigcirc	Connected services					
Ŧ	Server	I.				
	Licenses					
⋳	Security				Net	W

5. Select External HTTPS and click OK.





6. Enter a trigger name. This name will be used in the json mapping file, described below.

	Cre	ate Extern	al HTTPS T	rigger	?	×
Trigger	name:	TestTrigg	er			
Copy th trigger	iis URL in works on	to your l ce it has	orowser t been co	o verify nfigure	y that th d	ne
https:/ Activa {"trigg onds":	//localhos teDeactiv erName" "5"}	st:29204, /ateTrigg :"TestTrig	/Acs/Api/ er? gger","de	Triggei activat	rFacade eAfterS	/ ec
	Н	elp	ОК		Cance	el

- 7. Click **OK** and then click **Next**.
- 8. Add an action.





Create and edit action rules by selecting triggers, actions, and schedules.

<u>Steps</u> Triggers	Actions	
Actions	All the actions you specify here will be carried out when this rule is active.	
Schedule		Add
Details		Edit
		Remove

9. Select the required action (usually Raise Alarm) and click OK.

	Add Action ? X
Action	Description
Record	Raise an alarm on the Server that is sent to all connected Clients.
Raise Alarm	Instructions can be given to operators
Set Output	to initiate appropriate actions.
Send E-mail	
Live view	
Send HTTP Notification	
Send mobile app notification	
Turn rules on or off	
Access Control	
	Help OK Cancel

10. Fill in the alarm's **Title** and **Description**fields. This information will be shown to the operator once the alert is triggered.



	Create	Alarm A	ction		?	×
Alarm me	essage					
Title:						
Description:						
Duration (s):	10				^]·	~
Alarm pro	ocedure show alarn	n proce	dure:			
File name:						
		Prev	iew	Upl	oad	
	Help		ОК		Cance	el

- 11. Open the AxisCamerasMap.json file, located at: C:\Program Files\BriefCam\BriefCam\BriefCam Server\ plugins. This file maps between the cameras and the alarms. Note that this file must always be in the same folder as the plugin's dll file.
- 12. In the AxisCameraMap.json file, enter the Trigger Name from step 6.
- 13. Raise the trigger by filling in either the Camerald with the **External ID** from ACS or by entering the **Respond Rule Name**.

*C:\Repoi\Untegration	ons\BriefCam,ACSIn	tegration\AxisCamerasMa	pjison - Note	-							
7	ew Encoding La	nguage settings loois	Macro Kun	Plugins	window	x	Cameras on source	De:			
ia 🚽 🖬 🗞 👒 🕸	a 🕹 🕹 🐜 🗈) C A 🍾 🤻	ت 🗈 (*	5, 1	JE 📮 📓	-	Enter camera or	directory name	٩	Sele	et all
AxisCamerasMap.json	2) -: [Camera Name SNC-EB630	External ID 12509_4b8c22d6-ea4f-4191-b0b8-d662931	41567	Timezone	GeoLocation
	ameraId": "125 riggerName": "	509_4b8c22d6-ea4f- "TestTrigger"	4149-b0b8-	d66293	1416d7 <mark>*</mark> ,						
7 0 (8 9 -1 10 -1 12 -1 1 -1 1 -1	uleHame": "", riggerHame": "	*TriggeredByRuleNs	me"								
length: 20 Ln:4 Col:	62 Sel:0[0	Unix (LF)	UTF	8	INS	1					

14. Repeat for any rules that you need.

Known Limitations

- Bounding boxes when playing the original video are not supported.
- Support for the H.265 format is done per request. If you want to use the H.265 format with this VMS, please contact BriefCam's support.
- Due to a limitation with the Axis API, no data can be sent to Axis ACS.





Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Bosch	BVMS Bosch Video Security	12.2	2024 R2 HF5	Integration for on-demand and real-time (L2)	No
Bosch	BVMS Bosch Video Security	11	6.3	Integration for on-demand and real-time (L2)	No

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

VMS SDK

- Prior to the plugin installation, install the relevant Bosch SDK (6 videosdk06120078x64) on the BriefCam server.
- If the Processing Server service and/or Alert Processing Server service is installed on a dedicated machine, also install the Bosch SDK on that machine.

Connecting to the Bosch VMS



If the Bosch VRM is installed on a separate machine and not on the VMS, in the BriefCam Administrator Console's **Add Directory** screen's **Address** field, specify the VRM's IP address and not the VMS's IP address.

=BriefCam

Add Directory	×
Fill in the fields below	
Video Integration *	•
Directory Name *	
Address *	
User Name *	
Password	0
Cancel	Add

- 1. Log in to the Bosch VMS.
- For Bosch 11, log in using the Bosch VRM's default user called srvadmin (this is the only user that you can use).
- For Bosch 12.2, create an admin user called **srvadmin** and give it the same password as the default **srvadmin** user. Log in using the admin user that you just created.

User g	Enterprise Access	User Properties	
	Admin	User Properties	
1	Briefcam service	Account is enabled	
	stvadmin	Full name	srvadmin
22	NewUser	Description	





- 2. In the Bosch Configuration Client, go to Devices.
- 3. In the Device Tree, navigate to VRM Devices and right-click on the main device.
- 4. Select Edit VRM device.



5. In the **Edit VRM** screen, check the **Show password** checkbox. The username (srvadmin) and the password that you set here must be used to connect to Bosch VMS, retrieve cameras and export video.




6. Navigate to **VRM Devices**, the main VRM, and **Pool 0**.

7. Right-click on the video streaming gateway (vsg2 in the image below) and select Edit Video Streaming Gateway.





8. In Edit Video Streaming Gateway screen, check the Show password checkbox.

Edit Video Streaming Gateway X							
Device Identification							
Name	vsg2						
Network address / port	172.1.1.233	8443 🜩					
Credentials							
User name	service						
Password	Show password						
State	authenticated	Test					
Security							





To support both VRM and VSG cameras, you need to use same password for VSG and all VRM devices.

-	Chang	e devic	e passwords				
(C) Re	fresh S	tates 🚯 Select A	AII			Show passwords
	Туре	Sta_	Display name	Device ty_	IP addr A	Service	User
	-	3	VSG - Video Strea	VSG	172.1.1.91	•••••	
•	-	6	Bosch - DINION IP	DINION 1 Refresh Select a	172.25.25 state II		
				Authen	ticate		
				Edit pas	sword		

Bosch Settings in BriefCam

🔚 Brief(Cam.Bosch6Fetcher.ini 🔀
1	don't remove this string
2	[Fetching]
3	;LiveDelayMSec = 0
4	L
5	[Rcp]
6	;Schema=
7	;Port=
8	;User=service
9	;Password=
10	L
11	□ [Cache]
12	L;AutoUpdateMinutes=

The BriefCam.Bosch6Fetcher.ini file (located by default at C:\Program Files\BriefCam\BriefCam\BriefCam Server\ plugins) includes the following settings:

Setting	Description
LiveDelayMsec	When configuring the RESPOND module to use Bosch cameras, the timestamp is not delivered as part of the RTSP stream. As a result, BriefCam uses the local system time as the stream time minus a configurable time lag to represent network and systems latency. This time lag can be configured in the LiveDelayMSec setting (default is 0, meaning no delay).
Schema	Set which schema to use: http or https (default).
Port	The port of the video streaming gateway. The default is 8443.
User	The username for the video streaming gateway. For Bosch 11 and above, set this to service and remove the semicolon.
Password	The video streaming gateway password for the user. For Bosch 11 and above, set a password and



	remove the semicolon. Remember that you need to use same password for VSG and all VRM devices.
AutoUpdateMinutes	How often in minutes to check if a change was made to the ONVIF camera configuration and update the cache.

Enabling Live Video Streaming

To enable live video streaming, make the following changes in the BriefCam.Bosch6Fetcher.ini file:

- 1. Make sure the User setting is set to service. For earlier Bosch versions, do not change this setting.
- 2. In the User Name and Password settings, enter the password from the **Edit Video Streaming Gateway** screen (as shown in the image below).



All cameras that are configured in the VMS with this user name and password will work with the live video stream.

3. In the Port setting, enter the port from the **Network port** field from the **Edit Video Streaming Gateway** screen (as shown in the image below).

Edit Video Streaming Gatew	ay .	×	
Device Identification			
Name	375	BrefC	am.Bosch6Fetcher.ini 🖂
Network address / port	172.1.1.233 8443	1	don't remove
		2	[Fetching]
Credentials		3	;LiveDelayMSe
User name	service		
		5	E [Rop]
Password			;Schema=
	Show password		Port=
		8 1	(User=service
State	authenticated Test		; Password=
		10	
Security		11	E[Cache]
		12	-;AutoUpdateMi

- 4. If the Secure connection checkbox is unchecked in the screen above, set the Schema setting to http.
- Enter the following section to the .ini file and fill in the credentials: [Live] OnvifUser=service
 - OnvifPassword=xxxxxxxxxxxxxxxx
- 6. Remove the semicolon before any setting that you changed.
- 7. Restart the BriefCam services.

Known Limitations

- · Only one pool installed on the same machine as the VMS is supported.
- Bounding boxes when playing the original video are not supported.
- When configuring the RESPOND module to use Bosch cameras, the timestamp is not delivered as part of the RTSP stream. As a result, BriefCam uses the local system time as the stream time minus a configurable time lag to represent network and systems latency. This time lag can be configured in BriefCam.Bosch6Fetcher.ini -> LiveDelayMSec property (default is 0, meaning no delay).

CASD Integration





Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
CASD	VisiMAX NVR- RTSP	9.10	2024 R2 HF4	Integration for on-demand and real- time (L2)	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.



Make sure that the VMS and BriefCam servers' operating systems are synced to the same Network Time Protocol (NTP).

Ports Required

The following ports should be available when installing the plugin.

Port #
554, 2088, 3333, 20554N0554, and 22088N2088

Installing the VISIMAX.OCX registry key

Prior to the plugin installation, you need to add the proper VISIMAX.OCX parameter to the Windows registry.

- 1. To add the VISIMAX.OCX parameter to the registry, copy the VISIMAX.OCX file to your BriefCam Server PC and run a Command line as admin (CMD). To do so, click the **Start** button, type cmd, and select cmd.exe from the search list on the right, followed by **Run as administrator**.
- 2. Enter Regsvr32 <full path to the location where you put visimax.ocx> (i.e. Regsvr32 C:\VISIMAX.OCX).
- 3. A pop-up window will indicate that the registry has been added successfully. Click OK.







For additional information on how to add VISIMAX.OCX, please contact your System Integration manager or BriefCam Support.

Working with a VisiMAX Server that has More than Two Ports

In VisiMAX, each port on the VMS represents 16 cameras. Each VMS can contain up to 6 ports (96 cameras).

When adding a VisiMAX directory, you can have all cameras from all ports will appear on the screen in one long list.

There are two ways to do this:

- 1. By entering the address:port combination (for example 'VisimaxServer:2088'), BriefCam will connect to the VMS on that specific port, and retrieve the 16 cameras on that port.
- 2. By entering the address in a specific syntax and editing the VisimaxIntegration32.ini file as described below:
 - a. Enter the address in the address bar optionally followed by the pound key (#) and the number of addresses to search. Note that in this method, you are not required to specify the port in the address but only <IP>#<number of addresses>. Here are two examples:

172.25.25.29#2 will scan both 172.25.25.29 and the next number: 172.25.25.30 and add them to the directory you create.

10.0.0.99#10 will scan IP addresses 10.0.0.99-108

b. When a VisiMAX server has more than two ports (two instances), you need to enable additional ports in the file by uncommenting the ports (removing the semicolon) in the TCP, UDP and RTSP sections of BriefCam's VisimaxIntegration32.ini file (located at: C:\Program Files\BriefCam\BriefCam\BriefCam Server\32\plugins).

For example, if the VisiMAX server is using four ports, find ports 3 and 4 in the file and uncomment them (remove the semicolon) in all sections.

-BriefCam

VisiMaxIntegration32.ini - Notepad	_	×
File Edit Format View Help		
;UseYv12 = true		^
[ТСР]		
Port1 = 2088		
Port2 = 22088		
;Port3 = 32088		
;Port4 = 42088		
;Port5 = 52088		
;Port6 = 62088		
Port1 = 3333		
Port2 = 23333		
;Port3 = 33333		
;Port4 = 43333		
;Port5 = 53333		
;Port6 = 63333		
[RTSP]		
Port1 = 554		
Port2 = 20554		
;Port3 = 30554		
<mark>;</mark> Port4 = 40554		
;Port5 = 50554		
;Portb = 60554		 ~

Enabling an offline port will significantly slow down the connection process.

Known Limitations

- Bounding boxes when playing the original video are not supported.The H.265 video format is not supported.

Dallmeier Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support	Additional License Required
Dallmeier	SeMSy	5	2024 R2 HF4	Integration for on-demand and real-time (L2)	Yes	A floating license is required for each recorder.
Dallmeier	SeMSy	5	2024 M1 (for the Next-Gen engine)	Integration for on-demand and real-time (L2)	Yes	A floating license is required for each recorder.



The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Licenses

A Dallmeier floating license is required for each recorder used by the BriefCam Server. To acquire these licenses, please contact the Dallmeier Support team.

Dallmeier SeMSy III Installation and Configuration

After running the plugin, you need to configure the BriefCam.Dallmeier.SeMSy3.ini file, which by default is located at: C:\Program Files\BriefCam\BriefCam Server\plugins.



If you have more than one physical server running the BriefCam server service all the configurations in the BriefCam.Dallmeier.SeMSy3.ini files (including the connection strings) should be identical.

Recorder and Recorders Sections

This integration supports many recorders and you need to enter the credentials for each of the recorders in the BriefCam.Dallmeier.SeMSy3.ini file.

Remember to remove the semicolon (;) from the beginning of each row that you change.

If all the recorders share the same credentials:

· Set the credentials in the DefaultUserName and DefaultPassword fields, as shown in the image below.



If you are using group login:

• Set the DefaultPassword only. Leave the DefaultUserName row as is.

If each recorder has its own credentials:

If all or some of the recorders have different credentials than the default, list each of them in the [Recorders] section with the recorder name, IP address, username and password.





- Each recorder name needs to be unique.
- If the recorder is using group login, use two sets of double quotes (" ") for the Username.



If some of the recorders have their own credentials:

- 1. Set the shared credentials in the DefaultUserName and DefaultPassword fields.
- 2. For the recorders with credentials different than the default, add each of them to the [Recorders] section.



Live Section

When a live image is received from the recorder/camera, the time of the frame is also received. If this time is invalid, BriefCam will set the frame time to the current time minus the value set in the LiveDelayMSec parameter. For example, if a frame is received with time 01/01/1900 00:00:00, BriefCam will override this time to the current time of the machine and will subtract the configured delay, which by default is 0.

Fetching Section

The FFprobePath parameter is the path to the ffprobe.exe file, which is located in the BriefCam server folder. The default path is set to the BriefCam server path.





Database Section

If the database name is not semsy (the default), change it in the Database section and remove the semicolon.

[Database] ;Name = semsy

Cameras

۲

You only need to add the main directory in the BriefCam Administrator Console. You do not need to add the recorders separately. For information about adding a directory, see the BriefCam Administrator Guide's Camera and VMS Configuration section.

When adding the directory in BriefCam, use the credentials that are used for connecting to the database via the Dallmeier SeMSy 3 DB Configuration Tool.

In the BriefCam Administrator Console, the camera names from the VMS will be prefixed by the area code and a hyphen. In the image below, the area code is 1.

Camera Activation

+ Semsy	Licenses: 1000 Remaining: 978 Activated: 22
	Search Cameras Q
	Name
	1 - Cam 1
	1 - Cam2
	1 - Rec 2.1
	1 - Rec 2.2

Send Alerts to the Dallmeier SeMSy III Database

The alerts are sent to the database only and do not appear in the Dallmeier VMS interface.

To configure the sending of BriefCam alerts to the Dallmeier SeMSy III database, carry out the following steps:

1. Enable the sending of alerts outside of BriefCam, by opening the BriefCam Administrator Console and setting the **Respond.AlertsPublishingEnabled** environment setting to **true**.



2. On the machine where you ran BriefCam's SeMSy III plugin, open the BriefCam.Dallmeier.SeMSy3.ini file (located, by default, at: C:\Program Files\BriefCam\BriefCam\BriefCam Server\plugins).



- 3. Set the following three parameters and remove the semicolon from the beginning of each of the rows:
 - PGuardInterfaceAddress The IP address or hostname of the machine where the PGuardInterface service is installed (localhost by default).
 - PGuardInterfacePort The HTTP port for the PGuardInterface service (configured during the installation of the service; 8282 by default).
 - EventID This is the subalarm ID that needs to be created in PGuard in the "10036 External message" section. This can be any number from 1 to 99999 as long as it is not already in use. See Dallmeier's PGuardInterface documentation for additional information.
- 4. In the BriefCam Administrator Console, start/restart the VSServer service.

Received Alerts

The alerts received in the Dallmeier SeMSy III database will appear as a list of comma-separated values in the following order:

- Alert ID
- Timestamp UTC time in UNIX timestamp format (seconds since 01-01-1970)
- Rule Name
- Alert Type "FA" for fast alerts; "SA" for smart alerts
- Type "FR" for face recognition alerts; "LPR" for license plate recognition alerts; "GEN" for other alerts
- Object Class
- Confidence %
- Description
- Image URL
- Watchlist
- Licence Plate
- Color
- Upper Wear
- Lower Wear
- Bag
- Hat
- Mask

Additional notes:

-BriefCam



When the alert message's limit of 254 characters is reached, data pruning will occur to ensure that the alert can be sent.

Data pruning may occur in the following fields: Rule Name, Image URL, and Watchlist.

Dallmeier SeMSy 5 Installation and Configuration

Working with SeMSy 5 on Distributed Environments

If you are working with SeMSy 5 on a distributed environment, you will need to carry out the following steps:

STEP 1. Create a Virtual Workstation in SeMSy 5 Config

To connect to the Core Server in a SeMSy 5 Distributed installation, there needs to be a Workstation provided, as part of the credentials.

This is done by creating a Virtual Workstation as follows:

- 1. In the SeMSy 5 Config Mode application, open the System Configuration folder.
- 2. Click on the **Workstations** menu.
- 3. In the **Description** field, enter a name for the workstation. Only a name for the workstation is needed. Do not select a server from the Server drop-down, it needs to remain empty.

me sunsy's						
E Adam						
Ø nul.		Louise Dear	General Volume (1) 0	reas (1) Rights		
> 📷 method Waraperson			terte p			
> 📷 temp		🗸 🚰 1 - Aves Des		1 - Anal Des	Conception .	5 10 10 10 10 10 10 10 10 10 10 10 10 10
🗢 🎥 Byrlan Configuration					- **	
2 System Locations						
A then						
el testas	1					
D Research						
🖉 titles Channels	12					
A Chartest Auropeters						
E Falcer Servers						
E Active Servers						
Con Seren						
in the part of						
E Alla Dervers	1					

STEP 2. Create a New Admin User for BriefCam in SeMSy 5

- 1. In the SeMSy 5 Config Mode application, open the System Configuration folder.
- 2. Click the Users menu.
- 3. Add a new user.
- 4. In the User field, enter the username using the following syntax: [REST API user]@[workstation name]

Where the REST API user is the username configured for accessing the Rest API (this is in the Site Login User found in the SeMSy Setup app) and the workstation name is the newly created workstation name from STEP 1 above (Create a Virtual Workstation in SeMSy 5 Config).

For example: admin@briefcam-new

- 5. In the **Password** field, create a password.
- 6. Give the new user Admin rights by checking the Admin checkbox.





A Setting's					
E Attes					
Ø ret.	then Group	Bernel Desarth Ray			
> 📷 mater throughout		tetup Tere	(areageneeran .	1 (me 7 me	
🛩 🏙 Ryellen Configuration	S. atten		I —	Passant Parts	
Ryden Loudies 1			ten Maria Dava		
A then it					
d terms :			5		
D Bottobers 1					
🖗 this Durink 🛛					
di langten 1					
E Falcer bream -					
E Artisteran 1					
E Continent 1					
The second secon					
E Alla Servera 1					
> 🖿 intern					

Cameras

To add cameras:

- Open the BriefCam Administrator Console.
 Open the Camera Management section (see image below), which lists all connected VMS servers on the left and the servers' associated cameras on the right.
 Click the Add Directory button.

BriefCam ADMIN	CAMERA MANAGEMENT								<i>.</i> ? c		See Out
🗊 Evens	Licenses 2000 Remaining 925 Activated 65										
A User Management A											
🕀 Deployment 🔍 👻	Search Directories. Q,		Search Carrie	m. Q,					Div	Key only and	Mic cameras
Heres	Dive store entrance camera (Disabled)	1	0	Name	Activation	Enabled	Overhead	Counting	Path		
(2)	Office entrance (3)	1		Serve DAC / Dilace VMAnn	2021/07/011-				A412083/		0
	Office corridor (10)					-		-		~	*
Services			0	AKIS Q0155 Mix III Netw	2057-01.517				/MiL20R3/	堆	0
C) Setties 🔷 👻				AX65 P3255 CVE Networ	2021/07/211_	•			/MIL20R3/	壚	
Carners Management											
Environment Settings											
Localization											
Events Threshold											
⊴ Antin •											
	Add Directory								O here her	hape: 200_	Aude

The Edit Directory screen will open:



rectory	×
e fields below	
Video Integration	
Dallmeier SeMSy 5 Integration	.
Directory Name *	
SeMSy 5	
Address *	
http://172.1.1.250:9000	
User Name *	
admin	
admin	

6. In the Address field, enter the following URI schema, which is needed for connecting to the SeMSy 5 REST Server:

The URI schema is http(s)://{SeMSy5-address}:{RestServerPort}

You'll find the RestServerPort in the SeMSys 5 Setup application's SeMSy Core tab. The default port is 9000.

SeMSy5 Setup 5.3.361	.0					-		\times
Setup type: All in One		Expert Mode			Dal	llme	16	ſ
General SeMSy Core	Databas	e Device Matrix Import Set	4Sy Sequencer	Archive Database	SeMSy Archive	SeMSy Display Service	seMSy	C • •
General					Service			
Core Active Is Data Provider		Enable s	ystem health che	dis	Run as S Service run	iervice ning	Stop now	,
REST Server								
Port :	9000							
Session Timeout (ms):	30000							

7. In the User Name and Password fields, enter the SeMSy5 Site Login User and User Name and Password. You'll find these in the SeMSy 5 Setup application's General tab (as shown in the image below). If you are using a distributed environment, enter the user and password that you created in the SeMSy 5 Config Mode application (see





🔧 SeMSy5 Setu	s.3.361.0			\times
Setup type: All in One		=1	E	r
General SeMS	y Core Database Device Matrix Import SeMSy Sequencer Archive Database SeMSy Archive SeMSy Display Serv	ice	SeMSy D	• •
Site login				
User:	admin			
Password:	••••			

In the BriefCam Administrator Console, the camera names from the VMS will be prefixed by the area code and a hyphen. In the image below, the area code is 1.

ENVIRO	NMENT SETTI	NGS			
36g	x	Type v	Show settings that have been changed		
Scope	Type	Key	Value	Default Value	Change to:
GLOB	Common	ProWebApiAddress	http://16GPU:80/ProWebApi		https://16GPU/ProWebApi
GLOB	Common	License.LicenseManager	16gpu	localhost	16gpu
GLOB	Common	Qikderver	16gpu	BI_HOSTNAME	16gpu
GLOB	Common	ProWebClientAddress	http://16GPU:80/synopsis	<u> </u>	https://16gpu/synopsis
GLOB	Common	AdminClientAddress	http://16gpu/	http://localhost/	http://16gpu/
GLOB	Pro Web API	clientNotificationEndPoint	http://16gpu:7080/signalr		https://16gpu.7080/signalr
GLOB	Alert Processing	VideoProcessingGateWayUrl	http://16GPU:80/VideoProcer	\longrightarrow	https://16GPU/VideoProcess
GLOB	Common	BaseVideoUrl	http://16GPU:5010/	\longrightarrow	https://16GPU.5010/
GLOB	Common	DBLocalStorageAddress	http://16GPU:80/ProWebApit		https://16GPU/ProWebApiStx
GLOB	Notification Ser	Notification.ListeningEndpoint	http://*.7080	\longrightarrow	https://*.7080

After running the plugin, you can configure the BriefCam.Dallmeier.SeMSy5.ini file, which by default is located at: C:\Program Files\BriefCam\BriefCam Server\plugins.

C:\Program Files\BriefCam\BriefCam Server\plugins\BriefCam.Dallmeier.SeMSy5.ini

File	Edit	Search	View	Encod	ing La	inguage	Settin	gs Tool	s Macro	Run
	-	l 🖹 🔒	ار 🕞	4	ħ (î)	2	2 #	₽ 28 €	; 🔍 🖪	-
🔚 Br	iefCam.	Dallmeier.	SeMSy5.	ini 🗵						
1		;don't	remo	ve th	is st	ring				
2	Ē	[Live]								
3		;LiveD	elayM	Sec =	0					
4										
5		[Fetch	ing]							
6	; L	;FFpro	bePat	h = "	FFPRO	BE.EXH	5 "			

Live Section

When a live image is received from the recorder/camera, the time of the frame is also received. If this time is invalid, BriefCam will set the frame time to the current time minus the value set in the LiveDelayMSec parameter. For example, if a frame is received with time 01/01/1900 00:00:00, BriefCam will override this time to the current time of the machine and will subtract the configured delay, which by default is 0.





Fetching Section

The FFprobePath parameter is the path to ffprobe.exe file, which is located in the BriefCam server folder. The default path is set to the BriefCam server path.



Dallmeier SeMSy 5 was certified with the Dallmeier Recorder version 9.15.12.

Known Limitations

· Motion detection is not currently supported.

Digifort Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Digifort	Digifort Enterprise	7.4.0.4	2024 M1	Real time alerts integration (L2a)	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Initial Setup

In the VideoNative.ini file (located at C:\Program Files\BriefCam\BriefCam Server), change both the RtspConnectionTimeout and the RtspGetNextTimeout parameters to 60000 and remove the semicolons from the beginning of these rows (as shown in the image below).

-BriefCam



*C:\Program Files\BriefCam\BriefCam Server\VideoNative.ini - Notepad++ File Edit Search View Encoding Language Settings Tools Macro R 🗐 🗐 🕞 💦 Ta 🚔 i 🔏 🖬 💼 i D Ċ 艜 📙 Video Native.ini 🗵 1 [Rtsp] 2 3 RtspConnectionTimeout = 60000 4 RtspGetNextTimeout = 60000 5 6 📮 [FFMpeg] 7 ;DecoderSurfaces = -1 8 ;LogLevel = 8 9 ;LiveDecoderBufferSizeMB = 50

Sending Alerts to Digifort

Alerts can be sent to Digifort. To enable this functionality, carry out the steps below.

BriefCam Configuration

In the **Environment Settings** section, there are three settings relevant for sending alerts outside of BriefCam (see the image below):

- To send alerts outside of BriefCam, set the Respond.AlertsPublishingEnabled setting to true.
- To send alerts to a VMS, check that the Respond.AlertsPublishingToVMSEnabled setting is set to true.
- To change the polling interval, use the Respond.AlertsPublishingIntervalInMilliseconds setting.

B	riefCam ADMIN		ENVIRO	NMENT S	ETTINGS				
	Events						_		
2.	User Management	^	publish		Туре		~ L	Show settings that have b	een changed
\oplus	Deployment	^	Scope	Туре	Key			Value	Default Value
G	Settings	*	GLO	Common	Respond J	AlertsPublishingEnabled	d	false	false
	Camera Management		GLO	VS-Server	Respond.4	AlertPublisherAcceptUr	nsafeC	true	true
	Environment Settings		GLO	VS-Server	Respond.4	AlertsPublishingToVMS	Enabled	true	true
	Localization								
	Events Threshold		GLO	V5-Server	Respond	AlertsPublishingInterva	rinMil	1000	1000
зú	Activities	^	GLO	Common	AkkaHost	Config		akka : (loggers : ["Br	
88	Dashboards	^	GLO	Common	Administr	ation.SystemEventsPub	blishin	false	false
			GLO	Common	Administr	ation.SystemEventsPub	alishin	Critical	Critical

• If you make changes to the settings, you need to restart or start the VSServer service.

Digifort Configuration

The preferable method is to configure every camera separately as follows:



1. Open the Digifort Administration Client and navigate to Recording Server -> Cameras tab.

Oigifort - IP Surveillance System - Administration Client

Camera In this register you	a Register must add the cameras the	at the system will manage. I	t's possible to configure seve
V - Digifort V - Digi7.3 V - Recording Server Status Cameras Edge recording > - I (O Devices > - Alerts and Events > - Users	(All objects)	Name Axis Camera 1 Axis Camera 3 Axis-Yasmin ro	Description Kitchen Above Yasmin LPR Camera

2. Double-click on the camera name and go to the Manual Events configuration tab. Click Add to create a new event.

V- III Digitirit	(All objected)	🔎 Search			
- Dep 7.3	- Crystel)	Name	Description		
Kacceding Server	1	Mit Axis Camera 1	Kithen		
- Taha			1 1 1		
Canena Canena	Camera registration (Asis (Camera 1)			
	Cour al	Harual events			
Airts and Events					
S - 🧖 Uters	Netadata	n 🕑 Herusi e	vents		
- Screenstyles	Ardning				
- C Maps	1 Rights	Det ^	Description	Event Actions	
Coervitorial Maps	Users	Object of the second		(Send message), (Request advoviedpr)	
Anarytica	1 PTZ				
Veb Page	Settings				
Settings	Pearls				
Server Information	PT2 Patrol				
- 🜔 Vieb Server	Audery				
> · · · · · · · · · · · · · · · · · · ·	Jayaka				
	Neru control				
> IN cate	0 1/0				
	Input				
	Output				
	1 Events				
	Communication				
	Recording				
2	Hoton delectors		1		
	Audo level detectors				
	Hanual events				
	Device events	A00	Hoary Leens		
	1 Privacy				OK Canol
	il an				
1					1

3. The default event name is bc_event. The name can be changed in the Digifort plugin configuration file.





۲



4. Click Configure Actions.

Manual Event	x
Event	
Manual Event	
Event Name 1	
Event Description	
Configure the actions to execute on event:	
Configure Actions	
2 OK Cancel	

5. Select event actions. Usually, the Send an instant message to the operator and Request operator acknowledge event actions are used.

The **Show objects to operator event** action opens a new live stream player for every new alert, which leads to CPU overload. Make sure that this action is disabled.

allable actions	^		Selected actions	
Send e-mail to a group of contacts			send an instant message to th	e operator
Show objects to operator. The objects will be displayed the same popup	d in		Request operator admowledg	e
Show camera snapshots from the moment of the event operator screen	ton			
)) Play alarm sound in surveillance client				
Play pre-recorded audio clp on selected devices		->		
Call presets from cameras		•		
Activate output action scripts				
Activate or deactivate system objects				
Send a HTTP request				
Create a bookmark				
Download recordings from devices with edge recording			Configure	Scheduling

Every new Alert window will now appear in the Digifort client.



State Strengt Front Discours Incolours)	Liene actions	
Party / Tomas Local (RC201/RC30 L (RC30) - Review (RC201/RC30 L (RC30) R00)	1 mar	
The manual event bc_event of device Axis Camera 2 was triggered by the user admin at 172.25.25.1	G Configure event and an	
Yashin Andrew Statements and a second se		
TRANSFORMER > 7		
	Available actions	Selected actions
THE COURSE STORE STORE	Send e-mail to a group of contacts	Show abjects to operator. The objects will be displayed same popular
	 May alarm sound in surveillance client 	Show camera shapshots from the moment of the event operator screen
A REAL PROPERTY OF A READ PROPERTY OF A REAL PROPER	() Pay pre-recorded audio clip on selected devices	will field an instant nessage to the operator
	Call presets from cameras	Request operator admonietige
	Activate output action sociale	
	Contraction of the system algorith	-6-
and shall a shall be	Send a HTTP request	
Rule: Digifort, Camera: Axis Camera 2, AlertTime: 2020-08-31 10:03:04 646,	Create a bookmark	
Class Person, Class Details: Woman, Color: Black, Personal Attributes: UpperWear: LongSleeves, LowerWear: Long, Bag: HandHeld, Hat: NoHat,	Countined recordings from devices with edge recording subtract	
Masik NoMasik	Create Smer event	
Fil in the observations	1	Configure Scheduling
	The events that are forwarded to users of Surveilance Client can be tary which users will receive the notifications. If no users are selected, the no	pted to specific users or user groups, dick "Configure Receivers" to spec offications are sent to all connected users.
	Configure receivers	
Payback Close		OK

Alternatively, you can configure one global event that will be triggered for all the cameras. However, this method has some restrictions.

1. To enable global event sending, set the plugin configuration file's SendGlobalEvent option to true.



- 2. Open the Digifort Administration Client and navigate to Alerts And Events -> Global Events tab.
- 3. Click Add to create a new event.



Global ever	al ts can	events r	egister grammed actions in the s	system, as well as	
activate or the Surveill an event in	deactiv ance C the sys	ate camera recording. G lient or by external syste stem.	lobal events can be active ms, allowing any externa	ated by users by way al application to activa	of te
Digifort	^	Search			
✓ - I Digi7.3		Name	Description		
 Recording Server 		BC_EVENT	BriefCam Event		
Status					
Edge recording					
> - I/O Devices	10				
Alerts and Events					
Contacts					
Groups					
Global Events					
> - 🔞 Scheduled Events	100				
> - 2 Users					
Screenstyles		2			
Maps Contrational Mana					
Analytics					
Lisansa Dista Dasansika	×				
			10.110		-

4. Click Configure Actions.

anual Event			
Manual Ev	vent		
Event Name	1		
Event Description	I		
Configure the acti	ions to execute on e	event:	

- Select event actions.
 Check that the Show objects to operator action is disabled.



al events register	Actors Configure event actions	
General Rights	Auslabite actions Send e-mail to a group of contacts (1) Play alam sound in surveillance client (2) Play pre-recorded audio dp on selected devices (2) Play pre-recorded audio dp on selected devices (2) Call presents from cameras (2) Activate or deactivate system objects (2) Send a HTTP request	Selected actions Selected actions area opougo Show directs to operator. The objects will be displayed in the speciator stores Select an instant message to the operator Request operator actinowiedge Co
⊘Activate OK Cancel	Download recordings from devices with edge recording support Create simer event	Configure Scheduling
Add Hodfy D 5. IS Port: B000 Forents E	In The events that are forwarded to users of Surveillance Client can be to which users will recover the notifications. If no users are selected, the cantains Configure receivers work	angeted to specific users or user groups, click "Configure Receivers" to specify notifications are sent to all connected users.

Known Limitations

- · Bounding boxes when playing the original video are not supported.
- Live timestamps are inaccurate because of time differences. To solve this issue, set both BriefCam and Digifort to the same NTP.
- BriefCam's alerts are presented in Digifort without an image due to Digifort's SDK limitations.
- Once every few hours, the real-time stream disconnects for 10 seconds and then reconnects again automatically.
- In real-time alerts, recorded video saves the timestamp with a short lag.

Exacq Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Exacq	ExacqVision	23.09	2024 R2 HF4 (including Classic and Next-Gen engine)	Integration for on-demand and real-time (L2)	Yes
Exacq	ExacqVision	20.09	2023 M1	Integration for on-demand and real-time (L2)	No

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.





Ports Required

The following ports should be available when installing the plugin.

Port #
8554 and 22609

Integration Notes

When using the Exacq integration, note the following:

- The username used on Exacq is case-sensitive.
- The specified Exacq user account must have export privileges.
- When you install the Exacq plugin, the default hardware acceleration method is changed from CUVID to CUDA (in the ProcessingServer.ini file's HwAcceleratedDecoder parameter).

Known Limitations

- Bounding boxes when playing the original video are not supported.
- Only K-Lite Mega Codec Pack versions 14.6 and above with the Exacq integration are supported.

FLIR Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support	Additional License Required
FLIR	Latitude	9	6.0	Integration for on-demand and real-time (L2)	Yes	Yes. See the FLIR Licenses section below.

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Ports Required

The following ports should be available when installing the plugin.

-BriefCam



Port

554, 1116, 5000 (± 100), and 5554

VMS SDK

DVTEL Latitude 7.0.0.5780 and 8 SDK (updates should be installed both on the VMS and on the BriefCam Server), is required to be installed on every machine where any of the following BriefCam services are installed: VSServer service, Processing Server service, Alert Processing Server service, and Filtering service. It does not need to be installed on the client PC.

Post Installation Script

For new installations, after installing this VMS plugin you need to run a script that gives the BriefCam user permissions to access the relevant files.

If you will be running the BriefCam user as a domain user, you need to edit the script before running it. To do this:

- 1. Open the set_permissions_for_plugins file, which is located at: C:\Program Files\BriefCam\ BriefCam Server\tools\post plugin installation.
- 2. Edit the script with the correct parameters, including the domain and user.



In all places where the plugin is installed:

- 1. Open PowerShell as administrator.
- Navigate to the following folder: cd {where briefcam server is installed}\tools\
 post plugin installation
- 3. Run the following command: .\set_permissions_for_plugins.ps1

FLIR Licenses

The following FLIR certificates are required for the integration to work properly.

The licenses should be ordered from FLIR. Once you have received the license, apply it following FLIR's instructions on the VMS environment.

FLIR License	BriefCam Component



Server Certificate for v7 and v8	SDK Connection	1 for the VSServer service.
Server Certificate for v9	SDK Connection	 Server license with at least 3 SDK connections, to serve the BriefCam VSServer service and Fetching services. In addition, if there are more Fetching services, the SDK connections should be incremented accordingly, +1 for every additional Fetching service.
Respond Real-time Processing	Mobile User License	1 per GPU that is configured for Alert Processing Server service (RESPOND module).
RTSP Connection	 per real-time channel (this depends on how many workers your GPU can utilize). for the VSServer service. 	

FLIR 9 Settings for Real-Time

If you are using FLIR 9 for real-time, you need to set up the following:

- 1. Open the FLIR 9 AdminCenter.
- 2. Click Physical View.
- 3. Click Gateway server.
- 4. In the Mobile Middleware tab, check the Enable Enterprise Mobile app and Middleware SDK checkbox.

OFLIR Adviso	eater		- = ×
System System Logical View Physical View	Psystem Image: Constraint of the system Image: Constand of the system	Cerneral Mobile Middlewana FLIK Cloud TruWTHESS Actions Gatheway server Contract Extension Contraction Part 1996	+ ::* 0
YT - System Settings - Yideo - Austia - Users and Groups -	Concentration of the second seco	Endergenise Mukde app Status Farinah Indonesi Indané Rojdaj Interest I Display Disconendad Cameso I Autor SC I Inda Lagott	

Enabling MP4 Decoding

To enable MP4 decoding for the FLIR VMS:

- 1. Open the BriefCam.DvtelIntegration32.ini file, located at: Program Files\BriefCam\BriefCam Server\32\BriefCam.DvtelIntegration32\.
- 2. Change the following line: ;EnableMP4Decoding=false to EnableMP4Decoding=true (remove the semicolon (;) and set the value to true).

=BriefCam

📓 C:\Program Files\BriefCam\BriefCam Server\32\BriefCam.DvtelIntegration32\BriefCam.DvtelInte –	×
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?	х
🕞 🗁 🖶 🖻 🕞 🎧 🙏 X 🐚 🖍 🗩 C i 📾 🏂 i 🔍 🤹 🔍 🖾 🔚 1 🏋 🖉 🔊 i	>>
🔚 BriefCam.DvtelIntegration32.ini 🔀	
10 [General]	^
11 ;ScanLogicalPath = true	
12 ;SkipSourceStatusChecks = false	
13	
14 ;DVTEL 7+ only	
15 ;EnableMP4Decoding=false	
16	
17 ;; can be currently 0(auto), 6 , 7 or 8 only	
18 L;ApiVersion =0	
	~
length: 315 lines: 18 Ln: 1 Col: 1 Sel: 0 0 Windows (CR LF) UTF-8 INS	1

Known Limitations

- In FLIR integrations, bounding boxes when playing the original video are not supported.
- In the RESPOND module, when working with FLIR and recording in resolutions above 1080p, the original video bounding boxes do not match objects due to timestamp issues.
- In FLIR 9 integrations, in some scenarios, fetching from the VMS failed. To solve this issue, additional FLIR licenses
 are required.
- In FLIR 9 integrations, in some scenarios, the original video of RESPOND alerts does not play. To solve this issue, additional FLIR licenses are required.
- In FLIR integrations, when downgrading FLIR 9 to a previous version, a directory for the previous version is not installed. To solve this issue, contact the Support team.
- When connecting using DVTel plugin Latitude 7.0 SDK + updates, sometimes the closeup clip and synopsis playback do not run smoothly.
- Support for the H.265 format is done per request. If you want to use the H.265 format with this VMS, please contact BriefCam's support.

Genetec Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support	Additional License Required
Genetec	Security Center	5.13	2024 R2 HF5	Client integration (L3)	Yes	
Genetec	Security Center	5.12	2024 M1 (including Classic and Next-Gen engine)	Client integration (L3)	Yes	Yes. See the Genetec Licenses section below.
Genetec	Security	5.11.3	2024 R2 HF4 (including Classic and Next-Gen engine)	Client	Yes	



	Center			integration (L3)	
Genetec	Security Center	5.11	2023 M1 (including Classic and Next-Gen engine)	Client integration (L3)	Yes
Genetec	Security Center	5.10.4	6.4	Client integration (L3)	Yes
Genetec	Security Center	5.10.3	6.4	Client integration (L3)	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Genetec Settings

If you are using Genetec 5.9.2 and above, you need to set up backward compatibility in Genetec as follows:

- 1. Connect to Genetec's Server Admin of your main server with a web browser.
- 2. Click the main server in the server list.
- 3. In the Secure communication section, from the Allow applications starting from version (backward compatibility) drop-down list, select Genetec 5.8.0.

Secure communication	
Issued to VM13547	Issued by GENETEC-ONLINECA-CA
Valid from 9/5/2019 6:59:14 AM	Expiration 9/4/2020 6:59:14 AM
Allow applications starting from version (backward compatibility) 5.8.0.0	
	Select certificate

4. Click Save.

=BriefCam



Required Genetec Privileges

The following privileges are required on the Genetec side to connect to BriefCam:

To be able to connect: Application privileges -> Log on using the SDK To retrieve a list of cameras: Administrative privileges -> Physical entities -> View camera properties -> View streaming info For live streams: Action privileges -> Cameras -> View live video For fetching: Action privileges -> Cameras -> View playback -> Export video For alerts: Administrative privileges -> Alarm management -> View alarm properties -> Modify alarm properties -> Add alarms Action privileges -> Alarms -> Trigger alarms

Administrative privileges -> System management -> View user properties

Administrative privileges -> System management -> View server properties



Ports Required

The following ports should be available when installing the plugin.

Server	Port #	Description
Alert Processing	654	Used for live streams.



Server		
5500	Used for connecting to Genetec (Get Cameras, etc.) and sending alerts.	
VSServer, Fetching Server	605	Used by the Fetching Service for downloading records.
606	Used in multi-server configurations for connecting to Genetec (Get Cameras, etc.) and sending alerts (same role as 5500). For multiple recorders, an additional 605+ port is required for every recorder.	
654	Used by the Alert Processing Server service for live streams	
5500	Used by the VSServer and Fetching Service for connecting to Genetec (Get Cameras, etc.) and sending alerts.	

Plugin Installation and VMS SDKs

The table below shows you which plugin file to use and which SDKs you will need installed on every machine where any of the following BriefCam services are installed: VSServer service, Processing Server service, and Alert Processing Server service. It does not need to be installed on the client PC.

Genetec Security Center Version	Required Security Center SC SDK	Required Plugin File
5.6 SR4 CU2	 SR4 + Updated Pack CU2 Security_Center_v_5_6_SR4_b977_19_SDK.exe CU2 for Genetec Security Center 5.6.exe 	BriefcamGenetecSC5.6Plugin_ <version_number>.exe</version_number>
5.7 SR3	5.7 SR6 • Security_Center_v_5_7_SR6_b1218_23_SDK.exe	BriefcamGenetecSC5.7Plugin_ <version_number>.exe</version_number>
5.7 SR5	5.7 SR6 • Security_Center_v_5_7_SR6_b1218_23_SDK.exe	BriefcamGenetecSC5.7Plugin_ <version_number>.exe</version_number>
5.7 SR6	5.7 SR6 • Security_Center_v_5_7_SR6_b1218_23_SDK.exe	BriefcamGenetecSC5.7Plugin_ <version_number>.exe</version_number>
5.8 GA	5.7 SR6 + 5.8 • Security_Center_v_5_7_SR6_b1218_23_SDK.exe • Security_Center_v_5_8_1_0_b1004.15_SDK.exe	BriefCamGenetecPlugin.exe

-BriefCam

5.8.1.0	5.7 SR6 + 5.8 • Security_Center_v_5_7_SR6_b1218_23_SDK.exe • Security_Center_v_5_8_1_0_b1004.15_SDK.exe	BriefCamGenetecPlugin.exe
5.9.0	5.7 SR6 + 5.8 • Security_Center_v_5_7_SR6_b1218_23_SDK.exe • Security_Center_v_5_8_1_0_b1004.15_SDK.exe	BriefCamGenetecPlugin.exe
5.9.2	5.7 SR6 + 5.9.2.0 • Security_Center_v_5_7_SR6_b1218_23_SDK.exe • Security_Center_v_5_9_2_0_b380_68_SDK.exe	BriefCamGenetecPlugin5_9.exe
5.9.4	5.9.4 + 5.7 SR6 • Security_Center_v_5_7_SR6_b1218_23_SDK.exe • Security_Center_v5.9.4.0_b580.32_SDK.exe	BriefCamGenetecPlugin5_9.exe
5.10, 5.10.2, 5.10.3, 5.10.4	 5.7 SR6 + 5.10 Security_Center_v_5_7_SR6_b1218_23_SDK.exe Security_Center_v5.10.0.0_b357.0_SDK.exe Note: After installing the Genetec plugin, check that the SDK directory in the BriefCam.GenetecSc59Fetcher.ini file is set to the 5.10 SDK.	BriefCamGenetecPlugin5_9.exe
5.11	 5.7 SR6 + 5.11 Security_Center_v_5_7_SR6_b1218_23_SDK.exe Security_Center_v5.11.0.0_b143.4_SDK.exe Note: After installing the Genetic plugin, check that the SDK directory in the BriefCam.GenetecSc59Fetcher.ini file is set to the 5.11 SDK.	BriefCamGenetecPlugin5_9.exe
5.11.3	 5.7 SR6 + 5.11.3 Security_Center_v_5_7_SR6_b1218_23_SDK.exe Security_Center_v5.11.3.0_b3130.13_SDK.exe Note: After installing the Genetec plugin, check that the SDK directory in the BriefCam.GenetecSc59Fetcher.ini file is set to the 5.11.3 SDK.	BriefCamGenetecPlugin5_9.exe
5.12	5.7 SR6 + 5.11.3 • Security_Center_v_5_7_SR6_b1218_23_SDK.exe • Security_Center_v5.12.1.0_b1239.75_SDK.exe	BriefCamGenetecPlugin5_9.exe



Installing the Genetec Plugin

 When installing the Genetec plugin, in the Genetec v5.9.2.0 SDK Path field, enter the path to the SDK listed in the table above for your version of Genetec. Use the second SDK (not the 5.7 SR6 SDK); for example, when you are using Genetec 5.11, enter the path to the 5.11 SDK in the Genetec v5.9.2.0 SDK Path field.



- 2. After the installation is completed, open to the BriefCam Administrator Console.
- 3. In the **DB.LocalStorageAddress** environment setting, add a prefix, either http: or https: to the value.



Genetec Licenses

The following Genetec certificates are required for the integration with BriefCam to work properly. They are used for the SDK connection between the BriefCam integration and the Genetec Security Center.

The licenses should be ordered from Genetec (see Genetec part numbers in the table below). Once you have received the license, apply it according to the instructions in the Applying the Genetec Licenses section below.

Genetec Security Center license:

Server Certificate

Genetec Security Center Part#: GSC-1SDK-BRIEFCAM-VSEnterprisS

A Genetec Security Center license is required for **every** BriefCam component that integrates with the Genetec SDK as described in the table below.

Component	Description	Number of Licenses
VSServer service	Used by BriefCam for camera management	1 for each VSServer service installed on a machine. 1 additional spare license, as unexpected shutdowns can cause the certificate to be taken for 15 minutes, which means that the BriefCam servers will not be able to connect during that time.
Fetching service	Used by BriefCam's REVIEW & RESEARCH modules to fetch on-demand videos	1 for each Fetching service running on a machine.
Real-time processing	Used by BriefCam's RESPOND & RESEARCH modules to process real-time videos	1 for each Alert Processing Service. Note that on a multi-GPU server, each GPU will use a separate Alert Processing Service. Therefore, a multi-GPU server will consume multiple licenses, 1 per GPU.

Example: A system with 1 server (with all of the BriefCam components installed on it) with 4 GPUs (2 for on-demand, 2 for Real-Time) will consume the following licenses:

Component	Number of Licenses
VSServer service	2
Fetching service	1
Real-time processing	2
TOTAL # of Licenses:	5



늘



Client Certificate

Genetec Security Center Part#: GSC-1SDK-BRIEFCAM-VSEnterprisC

BriefCam Component: 1 per Embedded Client deployed (license per Security Desk client). The client certificate is required in order that the embedded BriefCam client will appear within the Genetec Security Desk application's Video Synopsis tab.

Applying the Genetec Licenses

• After installing the Genetec embedded plugin (when required), replace the Genetec embedded certificate with the certificate file received by Genetec. The certificate file to replace is located, by default, at: C:\Program Files (x86)\Genetec Security Center 5.11\Plugins\BriefCam\certificates.

	> This PC > Local Disk (C:) > Program Files (x86) > Genetec Security Center 5.11 >	Plugins > BriefCam > c	ertificates
	Name	Date modified	Туре
is	BriefCam.GenetecEmbeddedViewer.VideoSynopsisTask.cert	14/07/2023 14:01	CERT File

Pulling Real-Time Streams from Genetec to Create Alerts in BriefCam

Make sure to consult the "Maximum number of Media Gateway camera streams" section in the Genetec "Security Center System Requirements" guide in order to make sure your Genetec VMS is properly configured to support live stream requests by BriefCam.

To pull real-time streams from Genetec to create alerts in BriefCam:

1. Make sure that the Genetec portal is configured to enable RTSP and that the authentication is on.

🗴 Config Tool 📝 == Video	🗤 📉 Network view 🗤 📕 User manag) 🔅 Harris	172.1.1.155	- 6 ×
🍷 General settings 🚵 Roles 💷 Sche	odules 🧔 Scheckvled tasks 🦻 Macros 👹 O	utput behavion 🔹 🛸 降 Media Gabew	*/	
Search Y				Recourses
E Archiver			and address	The sources
Plealth Monitor				
Map Manager		_		
Media Cateway	Enable			
Media Router	Start multicast address	224 . 116 . 117 . 1 : 51914 2		
Naport warager				
🔮 vecs server	Listening part	654 🗣		
B Toue warade.	Sample URL:			
	User authentication			
	Accessible to:	N Admin		
		Ny user1		
		+ × 9		_

- 2. In the BriefCam Administrator Console, when adding a directory, you need to enter the following information:
 - **Directory Name** Enter a name for the directory. The name will be displayed to the end users when selecting cameras.
 - Address Enter the address of the Genetec directory server (host name or IP address).
 - User Name Enter a user name that will be used to authenticate the Genetec directory.
 - **Password** Enter the password for the user above.

Note that RTSP-based integrations do not work when user's credentials include the @ sign.

 RTSP Settings – Turn on this toggle. Since the RTSP's User authentication is on, you need to enter the RTSP credentials. The RTSP user name, password and address will be used for authentication to the RTSP server.



Add Directory

Fill in the fields below

Edan Interation *	
Senetec Security Center 5.9 Integration	*
Virectory Name *	
Senetec	
ddaaa *	
72.1.1.130	
iser Name * Idministrator	
assword	
•••••	0
RTSP Settings	
ese settings can be used to securely define the RTSP credentia	als for the integration

Cancel

Add

×

Genetec Security Center Embedded Client Installation

The following section describes the installation and configuration that need to be performed to allow the BriefCam web client application to become embedded in the Genetec Security Desk Application.

After installing the Genetec plugin and the relevant SDK on the BriefCam Server, and after applying the Genetec certificates, you are ready to install Genetec Embedded Client.

 On the same computer where the Genetec Security Desk Application is installed, run the Embedded Integration Plugin Installation by right-clicking the BriefCamEmbeddedClientForGenetecSecurityCenter_64bit_<Version_number>.exe file and selecting Run as administrator.



- 2. The installation checks for the following prerequisites. If anything is missing, you will be prompted to install the missing prerequisites and click **Install**.
- 3. In the Welcome screen, click Get Started.
- 4. Read and accept the License Agreement terms and click Next.
- 5. Select the installation destination path and click Next.

Note that the installation path must be the same directory where Genetec Security Desk Application is installed.

			×
<i>≂BriefCam</i>		BriefCam Embe Genetec Secur	dded Client For ity Center
Where do you wa For Genetec Secu	ant to install t urity Center p	the BriefCam En Iugin?	nbedded Client
C:\Program Files (x86)	Genetec Security	Center 5.5\	-
Space required:	359 MB		
Back			Next

- 6. In the **Web Server Address** field, enter the BriefCam Web Application URL. For https environments, add https:// to the beginning of the URL.
- 7. In the **Open API (BOA) Server Address** field, enter the address where the BriefCam Open API (BOA) was installed.
- 8. Verify that the provided URL is correct by clicking the **Verify URLs** button (both IP address or hostname values can be specified).





The URL will be saved in BriefCam.GenetecEmbeddedViewer.dll.config, which is located by default in C:\Program Files (x86)\Genetec Security Center x\Plugins\BriefCam.

Once the installation is complete, the URL configuration can be modified manually as needed.

For example:

<appSettings>

<add key="serverAddress" value="x.x.x.x/app/" />

</appSettings>

Both IP address or hostname values can be specified.

- 9. Click Install.
- 10. Your installation is now complete. Click **Finish**.

To establish a connection from the BriefCam client embedded in the Genetec Security Desk Application to the BriefCam Server:

- 1. Launch the Genetec Security Desk Application and log in to the Genetec server.
- 2. Once it is up and running, access the Genetec Security Desk main Tasks view. A Video Synopsis icon for an embedded BriefCam client will appear under the Integration section. Click the Video Synopsis icon to access the embedded BriefCam client in a separate application tab.


3. You will be asked to log into BriefCam upon clicking the VIDEO SYNOPSIS icon. Enter your username and password and click **Sign In**.



4. Upon logging in, the embedded BriefCam client will appear within the Genetec Security Desk application's VIDEO SYNOPSIS tab.





Bookmarks created within BriefCam will not be displayed on Genetec Security Desk application.

Silent Installation of Genetec Plugins

To run a silent installation of the BriefCamGenetecPlugin.exe file, use the following command line:

{ GenetecInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefcam" SDK_PATH="{path to 5.8 SDK}" SD_5_7_PATH="{path to 5.7 SDK}"

To run a silent installation of the BriefCamGenetecPlugin5 9.exe file, use the following command line:

./{ GenetecInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefcam" SDK_PATH="{path to 5.9 SDK}" SD_5_7_PATH="{p ath to 5.7 SDK}"

For information about the various Genetec installers, see: Plugin Installation and VMS SDKs.

Silent Installation of Genetec Embedded Client

To run a silent installation of the Genetec Embedded Client, use the following command line (if you want to install a newer version, see the next section below):

.\{Genetec embedded client installer} /qn BC_WEB_SERVER_ADDRESS="{host of BriefCam web}/app"

Silent Installation of Genetec Embedded Client – Upgrade

To install a newer version, you need to uninstall the previous version.

- 1. Open CMD as administrator and run the following command: wmic product get name
- 2. You will get a list of installed programs on your machine. Execute: wmic product where name="<program_name>" call uninstall

Where <program_name> is the name of the plugin you want to uninstall exactly as listed from the first command. For example:

wmic product where name="BriefCam Embedded Client for Genetec SecurityCenter 64bit" call uninstall

Next time you uninstall this program, you can call just the second command, since you already know the exact name of the program.



Connecting to Genetec Auxiliary Archiver

If Genetec Auxiliary Archiver is configured on the VMS and BriefCam is configured to connect to it, then every request from the VMS will automatically fetch video from the auxiliary archiver. If you want to connect to Genetec Auxiliary, make sure to edit the BriefCam.GenetecSc52Fetcher32.ini file, which is located by default at C:\Program Files\BriefCam\ BriefCam Server\32\plugins - Set the ;UseAuxiliaryArchiver = false parameter to true, uncomment the line and save the file.

Sending Alerts to Genetec

Alerts can be sent to Genetec Security Center's Alarm monitoring tab.

1 mar		_							
A STRICT BIBLING WARD	Tigger als	ens 💰 Porc	ibly acknowledge all a				7 iteres (1 salected)		*
ID Alarm	Priority	Alarm color	Source	Triggering event	Trigger time	State	Context		
1093 🧶 BriefCam Alerts			🎥 Admin	Manual action	25/01/2022 17:42:28	🧧 Active	Camera: 172.25.25.31-Camera-01-new	vname; Class: Person (Bo	y); Color: Red; Attrik tes: Up
1094 🜻 BriefCam Alerts			Note: Admin	Manual action	25/01/2022 18:48:50	🧧 Active	Camera 172252531-Camera-01-new	vname; Class: Person (Bo	y); Colon Reil; Attri des Up
1095 🧶 BriefCam Alerts			🎥 Admin	Manual action	27/01/2022 15/20/39	Sective	Carneral 172.25.25.31-Carnera-01-new	vname; Class: Person (Bo	y); Colori Reit; Attic
1096 🧧 BriefCam Alerts			🎥 Admin	Manual action	27/01/2022 15/22/01	🗧 Active	Carnera 172252531-Carnera-01-new	vrame; Class: Animal (Bir	d); Color: Red; List Name: V
1097 🧧 BriefCam Alerts	-		🎝 Admin	Manual action	27/01/2022 15/22:43	Sective	Camera: 172.25.25.31-Camera-01-new	vrame; Class: Animal (Tir	d); Color: Red; List Names V
1098 🧧 BriefCam Alerts			🎝 Admin	Manual action	27/01/2022 15:43:09	🧧 Active	Camera: 172.25.25.31-Camera-01-new	vname; Class: FourWheel	s (Carl: Color: Orange; Lpr N
1099 🚇 BriefCam Ale	ta 💶		a Admin	Manual action	27/01/2022 15:56:53	🚇 Acti			
e (🖌 Admonistique 💌 🖨 Sa	occe the atarn	®, instigete	🕂 fansed slave	/ talk contend					,

The following information is sent to Genetec:

- Camera Name
- Class
- Color
- Person Attributes (Upper Wear, Lower Wear, Bag, Hat, Mask)
- Watchlist
- Face Recognition/License Plate Recognition Identity Name
- Confidence

On the Genetec-side you need a full admin user.

In the **Environment Settings** section, there are three settings relevant for sending alerts outside of BriefCam (see the image below):

- 1. To send alerts outside of BriefCam, set the **Respond.AlertsPublishingEnabled** setting to **true**.
- 2. To send alerts to a VMS, check that the Respond.AlertsPublishingToVMSEnabled setting is set to true.
- 3. To change the polling interval, use the **Respond.AlertsPublishingIntervalInMilliseconds** setting.



B	riefCam ADMIN	E	INVIRO	NMENT S	SETTINGS			
Ū	Events							
2.	User Management 🔷		publish		X Type		Show settings that have be	en changed
\$	Deployment ^		Scope	Туре	Key		Value	Default Value
G	Settings 🗸		GLO	Common	Respond.AlertsPublis	hingEnabled	false	false
	Camera Management		GLO	VS-Server	Respond.AlertPublish	erAcceptUnsafeC	true	true
	Environment Settings		GLO	VS-Server	Respond.AlertsPublis	hingToVMSEnabled	true	true
	Events Threshold		GLO	VS-Server	Respond.AlertsPublis	hingIntervalinMill	1000	1000
á	Activities		GLO	Common	AkkaHostConfig		akka : (loggers : ["Br	
88	Dashboards		GLO	Common	Administration.System	nEventsPublishin	false	false
			GLO	Common	Administration.Syster	nEventsPublishin	Critical	Critical

4. If you make changes to the settings, you need to restart or start the VSServer service.

When the Genetec plug-in is installed, the BriefCam.GenetecSc58Fetcher.ini file or the BriefCam.GenetecSc59Fetcher.ini file is created at: C:\Program Files\BriefCam\BriefCam\BriefCam Server\plugins. The [Alerts] section contains two parameters:

- DefaultAlarmName This parameter is used as the connection between BriefCam and Genetec.
- TruncateCameraName This parameter lets you send a unique alarm identifier for each camera.

BriefCam.GenetecSc59Fetcher - Notepad							
File Edit Format View Help							
[Alerts] ;SendEvents=false :EventNamePrefix=BriefCam ;DefaultAlarmName=BriefCam Alerts ;TruncateCameraName=false							
;ConfigureRecordingDuration=false ;AlertPostPaddingSec=0							

If the TruncateCameraName parameter does not exist in the .ini file, the default behavior will be as if the parameter is set to false. If the parameter is set to true, every alarm sent to Genetec will have the following identifier:

<DefaultAlarmName> - <Camera name> for example: BriefCam Alarm - Camera-55.





🧧 Alarms 😤 Monitor groups	K > 🛤 🔮 BriefCa	n Alerts		
2 BriefCam Alerts - Canva-Sti	Ŷ		a Iden	Ity Properties Advanced
BriefCan Alet - Camera-501 BriefCan Alet - Camera-502 ReiefCan Alet - Camera-502	Priority:	1 tighest		
BertCan Alet - Camera-509 BertCan Alet - Camera-506 BertCan Alet - Camera-506 BertCan Alet - Camera-507 BertCan Alet - Camera-507 BertCan Alet - Camera-509 BertCan Alet - Camera-510	Recipients: Broadcast mode	Bacpart Bacpart Bacpart Bacado and Bacado		
	Attached entities:			
	Video display option: Content cycling:	Playback Play 4 = \$ sec. before	alarn	

If you expect a large number of alarms to occur simultaneously, set the ReactivationThresholdSec parameter to 0. This ensures that no alerts are missed.

Sending Events to Genetec

You can send events instead of alerts. You do this by setting the SendEvents parameter to true and uncommenting the row by removing the semicolon (;). The parameter is in the BriefCam.GenetecSc58Fetcher.ini file or the BriefCam.GenetecSc59Fetcher.ini file, which is located by default at: C:\Program Files\BriefCam\BriefCam Server\plugins.

2	\Program Files\BriefCam\BriefCam Server\plugins\BriefCam.GenetecSc59Fetcher.ini - Notepad++ 🛛 🗌 🛛 🗙	¢
File	Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ? 🛛 + 🔻	×
6) 🗄 🖻 💫 🦾 🎒 🔏 🐘 🐚 🕽 🗲 🗰 🏪 🔍 🔍 🖳 💁 🖬 🏋 🖾 👁 🛛	>>
🔚 Bri	fCam.GenetecSc59Fetcher.ini 🔀	
16		^
17	[Alerts]	
18	;SendEvents=false	
19	;EventNamePrefix=BriefCam_	
20	;DefaultAlarmName=BriefCam Alerts	

Using Geolocations

To activate geolocation features in the BriefCam system, add the following section to the

BriefCam.GenetecSc59Fetcher.ini file, which is located by default at: C:\Program Files\BriefCam\BriefCam Server\plugins.

[General]

GeoLocationEnabled = true

Using Multiple Gateways

Since version: BriefCam 2024 M1 HF2

You can connect multiple Genetec gateways to BriefCam to share the load of managing your cameras. This is done by adding



entries to the BriefCam.GenetecSc59Fetcher.ini file's Media Gateways section.

The syntax for adding the entries is:

<username:password@MediaGatewayAddress=NumberOfSupportedCameras>

Note that the username and password should be the same for each of the gateways.

For example:

[MediaGateways]

username:password@1.0.0.0:654=100

username:password@1.0.0.1:654=100

username:password@1.0.0.2:654=100

This configures three gateways with the username/password combination and assigns a capacity of 100 cameras to each.

Setting Camera Stream Types in BriefCam

Since version: BriefCam 2024 M1 HF2

By default, BriefCam uses the live stream for all cameras. You can change this for individual cameras or globally.

Global Stream Type

- 1. Locate the DefaultStreamProfile parameter in the BriefCam.GenetecSc59Fetcher.ini file.
- 2. Set the desired stream type. The valid options are:
 - live (default)
 - archiving (recording)
 - highres (high resolution)
 - lowres (low resolution)
 - remote

Individual Camera Stream

- 1. Edit the GenetecCamerasMap.json file. This file contains a list of cameras identified by their CameraName or Camerald.
- 2. Specify the desired StreamType for each camera.

Finding Camera Information

- · CameraName: Look for it in the Genetec VMS.
- Camerald: Look for it using BriefCam's Video Integration Tester (VIT) in the External ID column. This is mainly used if you have two cameras with the same name.

For example:

```
{
```

"CameraName": "Kitchen Camera",

```
"StreamType": "lowres"
```

}





Additional Notes

The GenetecCamerasMap.json file structure employs a JSON array named Items that contains these camera objects. An example with an empty object is provided below to illustrate the format:

```
{
```

"Items": [

{

```
"CameraName": "",
```

/* OR */

"Camerald": "",

```
/* live, archiving, highres, lowres, remote */
```

```
"StreamType": ""
```

}

]

```
}
```

Known Limitations

- Two different versions of the Genetec plugin installed on the same machine will not work with BriefCam.
- Bounding boxes when playing the original video are not supported.
- When using the Genetec VMS 5.7 SR6 integration, videos cannot be processed from cameras when the camera's name contains special characters, such as space, ~, and &, because of a Genetec SDK limitation.
- In Genetec integrations, video rotation is not currently working. To resolve this issue, configure the camera to send a non-rotated video to Genetec.
- In Genetec 5.9.4 integrations, when the processing server starts, in rare scenarios, the first processing tasks may fail. To resolve this issue, reprocess the video.
- In Genetec 5.10 integrations, there are errors when trying to connect to the live camera for the first time or after a server restart. To resolve this issue, restart IIS (by opening the Windows services, right-clicking on the World Wide Web Publishing Service and clicking Restart).
- In Genetec 5.10 integrations, when the Rtsp url was entered in the directory connection setting's Password field: 'VmsPassword RtspUsername:RtspPassword@GenetecRtspServer', alerts were not sent in some scenarios. To solve this issue, set LiveStreamWarmupFrameCount=19 in the plugin's config file and Live.GetLiveImageRetryInterval=500 in the BriefCam Administrator Console's Environment Settings.

See also: Troubleshooting - Genetec Issues

GeoVision Integration

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

=BriefCam



Known Limitations

Support for the H.265 format is done per request. If you want to use the H.265 format with this VMS, please contact BriefCam's support.

Geutebruck Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Geutebruck GmbH	G-Core	7.0.0.52	6.4 Hot Fix 1	Integration for on-demand and real- time (L2)	No

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Known Limitations

- Geutebruck uses a variable FPS that does not include metadata with an exact timestamp per frame. This may result
 in a number of side effects in BriefCam, including REVIEW closeup clips and original videos playing in slow motion
 and the RESPOND alert original video timestamp and bounding boxes being offset. To solve this issue, the
 integrator should configure both the live and archive streams to be at the same resolution and configure the cameras
 to a constant FPS.
- When requesting an on-demand request (REVIEW) on a Geutebrueck integration, the fetching occasionally reaches the default timeout (120 seconds) and causes the fetching to fail. To solve this issue, increase the fetching timeout in the BriefCam Administrator Console's Fetching.TimeoutInSeconds setting and restart the Fetching service.
- Currently, the H.265 format is not supported.

Hanwha Techwin Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Hanwha Techwin	Wisenet WAVE	5.0.0.36410	2023 M1	Real time alerts integration (L2a)	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

-BriefCam

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Installation and Configuration

Setting Up a Wisenet WAVE User

You need to create a Wisenet WAVE user that you will use when setting up the integration between BriefCam and Wisenet WAVE (in the Setting Up BriefCam to Integrate with Wisenet WAVE section below).

- 1. Log into the Wisenet WAVE client as an admin user.
- 2. Navigate to the User Management panel.



3. On the bottom left of the screen, click the **New User...** button.



w System	Administ	ration - Wiser	net WAVE Cli	ent					?	×
General								Routing Manageme		
Q. Sea										
	ogin 🛓	Name						Role		
🗆 ad	lmin							Owner		
Enabl										
A loss to		c.ta p. l.				ما	10100-10-00			
New U	ser	Edit Roles	5			0	LDAP Settings			
							ок	Apply	Cance	ы

- 4. Fill in the Name, Email, and Password fields.
- 5. In the **Role** dropdown menu, select **Viewer**, **Advanced Viewer**, or any custom role that has the necessary permissions. It is recommended not to use the **Live Viewer** role, because this role only has permissions for camera livestreams, and not for video fetching.

🐨 New User Wiser	?	×				
Login	integration					
Password	•••••				GOOD	**
Confirm Password	•••••					**
Role	Viewer	^	Edit Roles			
	Administrator Advanced Viewer		export video.			
	Viewer					
	Live Viewer					
Enabled	Custom			ок	Cance	ł

- 6. Enable digest authentication for the newly created user as follows:
 - a. In the bottom left of the **New User...** panel, next to the **Enabled** toggle button, click on the three vertical dots.
 - b. Click on the Allow digest authentication for this user pop-up message.



c. Set the user password again (can be the same as before):

👿 New User Wiser	net WAVE Client		?	×
Login	integration			
Password	••••••		6000	~*
Confirm Password	•••••			***
Role	Viewer Y Edit Roles			
	Can view all cameras and export video.			
C Enabled		ок	Cance	el
	Allow digest authentication for this user			

Setting Up BriefCam to Integrate with Wisenet WAVE

- 1. Install BriefCam's Wisenet WAVE plugin.
- 2. In the BriefCam Administrator Console, open the Settings section and click Camera Management.



3.



Bı	rief Cam ADM	IN	
Ť	Events		
2 ₈	User Management	^	
\bigoplus	Deployment	~	
	Hosts		
	GPUs		
	Services		
C _@	Settings	~	
	Camera Management		
	Environment Settings		
Click th	ne Add Directory button.		

🦻 💿 (🖘 🗠 CAMERA MANAGEMENT BriefCam ADMIN s: 1000 Remaining 925 Activated 65 Q, ٩, 1 0 Ð Ce 2.4 Cifice entrance (2) 1 Serv SNC VB4 2021/07/011-0 /MIL20R3/ 12 0ffice.com/dor (10) ÷ AXIS Q5155 Mic III Natur 2021-07-211 . 壚 ARSP3255-C/ENet 2021/07/211-壚 ME20E3/_ 0 ^ ee e 🚺 e ee hersbertige: 20. Ande

The Add Directory dialog will open.

- 1. From the Video Integration field, select BriefCam Wave Integration.
- 2. In the **Address** field, enter the directory address in the following format: http://<vms_ip_or_host>:7001, for example: http://172.1.1.243:7001.
- 3. In the **User Name** and **Password** fields, enter the credentials you defined in the Setting Up a Wisenet WAVE User section above.

=BriefCa	am	_
A	dd Directory	×
Fi	II in the fields below	
	Video Integration * BriefCam Wave Integration	Ŧ
	Directory Name * Wave VMS	
	Address * http://172.1.1.243:7001	
	User Name * integration	
	Password	Ø

Sending Alerts and Video Fetching

To enable the sending of alerts from BriefCam to Wisenet WAVE:

- 1. Open the BriefCam.WaveIntegration.ini file, which by default is located at: C:\Program Files\ BriefCam\BriefCam Server\plugins.
- 2. Change the value of the SendAlerts parameter to true and remove the semicolon (;).



This file also includes the SecondsFromNowNotRecordedYet parameter. This setting is for video fetching. It is the number of seconds before the current time to consider that recording is not yet available for export. For example, if the current time is 10:00 AM and the setting value is 1800, any export requests for video after 09:30 AM will fail because the plugin considers that the video recording is not yet available.

IndigoVision Integration





Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
IndigoVision	Control Center	19.4	2024 R2 HF4 (including Classic and Next- Gen engine)	Real time alerts integration (L2a)	No
IndigoVision	Control Center	19.1	2023 M1	Real time alerts integration (L2a)	Yes
IndigoVision	Control Center	18.2	2023 M1	Real time alerts integration (L2a)	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.



The IndigoVision plugin supports IndigoVision's Video Stream Manager.

Prerequisite Configuration

In order for theBriefCam plugin to connect to the Control Center Site Database and be enabled to fetch video, the following conditions should be met:

- The same Windows user (local user) should be configured on all machines (BriefCam Server, BriefCam Database and the machine hosting the Control Center Site Database). The user must have administrator privileges on the machine hosting the BriefCam Server. In case of BriefCam distributed environment setup, you can use the default BCUser that is created during installation and create the same user on the machine hosting the Control Center Site Database.
- 2. The VMS user must be configured with the **Use password authentication** as shown in the image below (and not with the Use Windows authentication, which is the default).

-BriefCam

administrator Properties					
General Settings Body Worn Video					
Login Datails administrator X					
Login Details - administrator					
O Use Windows authentication					
INDIGO-16 Vadministrator Browse					
Use password authentication					
New Deserved					
New Password:					
Confirm New Password:					
OK Cancel Help					
OK Cancel Help					

- 3. The user should have access to the Control Center Site Databasefolder.
- 4. The Control Center Site Database folder should be manually configured in the

BriefCam.Indigo17Integration32.ini file located at C:\Program Files\BriefCam\BriefCamServer\ 32\plugins where the DbFolderPath parameter points to the location of the Site Database as such

\\<[IP or HostName]\FolderName>, for example: DbFolderPath = \\172.1.1.122\ControlCenterDB. Make sure to remove the semicolon (;).

🔚 Brief	Cam.Indigo17Integration32.ini 🔀
1	don't remove this string;
2	[General]
3	;DbFolderPath="\\HOST_IP\SHARED_DB_FOLDER_NAME"
4	;Port=8135
5	;NvrPort=8130
6	;Token="ef182cd2-24f1-445d-bc69-5904e65a0c3f"
7	;UserName=
8	L;Password=
9	[Live]
10	L;LiveDelayMSec=0
11	[Alarms]
12	L;AlarmServerIP="172.1.1.59"

The steps for the above configurations are as follows:

- 1. On the machine hosting the Control Center Site Database, navigate to the DB folder **IndigoSiteDB** and share this folder with the user (for example: bcuser) that is available on all machines. Grant the user full share and access permissions.
- 2. On the machines hosting the BriefCam Server or BriefCam Database, add the IP/host name (with the relevant



credentials) of the machine hosting the Control Center Site Database:

- 3. Navigate to: Control Panel->User Accounts->Credentials Manager.
- 4. Verify that the hostname and user's credentials are entered correctly in the Windows Credentials Manager.
- 5. Click Add a Windows Credential.
- 6. You will be prompted with three fields to fill in: the IP/host name of the machine hosting the Control Center Site Database, the Windows username (of the user that has access to the Control Center Site Database folder), and the password. Be sure to enter the details correctly.
- 7. On the BriefCam Server, set the **VSService** to log on using the username you have already configured with access to the Control Center Site Database folder:
- 8. Open the Services dialog through the Start menu or the Task Manager.
- 9. Locate the VSService service on the list and right click. Click Properties.
- 10. On the **Log On** tab, click the **This account** radio button.
- 11. Enter the username and password for the user that has access to the Control Center Site Database folder.
- 12. Confirm that the user account (for example: bcuser) exists both on the operating system (OS) level and within the IndigoVision Video Management System (VMS).

Post Installation Script

For new installations, after installing this VMS plugin you need to run a script that gives the BCUser user permissions to access the relevant files.

In all places where the plugin is installed:

- 1. Open PowerShell as administrator.
- 2. Navigate to the following folder: cd {where briefcam server is installed}/tools/post_plugin_installation
- 3. Run the following command: .\set_permissions_for_plugins.ps1

H.265 Support for IndigoVision 18.2 or Above

The IndigoVision integration includes H.265 support for version 18.2 and above. For this to work correctly, you need to do the following:

- 1. When cameras are added via the VSM, add them to the Top Site.
- 2. In the Camera Properties, set the ONVIF profile for each camera to the H265 profile.
- 3. Set the Recording Job with an ONVIF Profile that supports H265.

This is applicable for Continuous Recording and Motion Detect Recordings.

Connecting to IndigoVision

IndigoVision version 17.2 supports the following SDKs, which are both installed as part of the IndigoVision plugin:

- SiteDB SDK v17.2
- Video SDK v18

IndigoVision version 19.1 and above supports the following SDKs, which are both installed as part of the IndigoVision plugin:

- SiteDB SDK v19.2
- Video SDK v19.2

To connect to IndigoVision, carry out the following steps:

- 1. Register the IvVideoSDK.dll file by opening the command line as administrator and running the following: Regsvr32 /i "c:\program files\briefcam\briefcam server\32\BriefCam.Indigo17Integration32\lvVideoSDK.dll"
- 2. Run IndigoVision's **Site Database Server Setup** tool and create a new service token.

=BriefCam			
Site Database Server Setup	-		×
Site Database Configuration			
Please select the operation you would like to perform.			
 Create a new site database 			
 Use an existing site database 			
O Change the Site Database Server administrator password			
O Upgrade from a Control Center 16 site database			
Configure as a failover Site Database Server			
 Generate a service authentication token 			
Back Next		Cance	L

- 3. After generating the authentication token, make sure that you click Next and Finish for the changes to take effect.
- 4. Open the BriefCam.Indigo17Integration32.ini file, located at C:\Program Files\BriefCam\ BriefCam Server\32\plugins, and do the following:
 - a. In the Token parameter, enter the token and uncomment the row.
 - b. In the Username and Password parameters, enter the Windows user credentials for the user connecting to IndigoVision's database and uncomment these rows.

Sending Alerts to IndigoVision

Alerts can be sent to IndigoVision's Control Center. To enable this functionality, carry out the steps below.

- 1. Open the following ports:
 - a. On the BC server side, standard port 8130 inbound rule
 - b. On the VMS side, UDP port 49301 inbound rule
- 2. Open the IndigoCamerasMap.json file, located at: C:\Program Files\BriefCam\BriefCam\BriefCam Server\32\ plugins. This file maps between the cameras and the alarms.

$\leftarrow \rightarrow \neg \uparrow \blacksquare$ This PC	> Local	Disk (C:) > Program Files > BriefCam > Br	riefCam Server > 32 >	plugins		
E Pictures	^	Name	Date modified	Туре	Size	
🔚 Videos		BriefCam.DirectShowDecoder32.dll	7/1/2019 4:12 AM	Application extens	43 KB	
🏪 Local Disk (C:)		BriefCam.DirectShowDecoder32.ini	3/6/2019 2:58 PM	Configuration sett	1 KB	
Dark_Side (D:)		BriefCam.DvtelIntegration32.dll	7/1/2019 4:12 AM	Application extens	9 KB	
		BriefCam.IndigoIntegration32.dll	7/3/2019 4:13 AM	Application extens	24 KB	
Network		🔠 BriefCam.IndigoIntegration32.ini	7/3/2019 3:16 PM	Configuration sett	1 KB	
bcfs2		🔥 IndigoCamerasMap.json	7/4/2019 4:29 PM	JSON File	1 KB	
📮 Image						



3. Map BriefCam to IndigoVision by mapping either the camera (Camerald) to IndigoVision's Source ID (Sourceld) or by mapping BriefCam's rules (RuleName) to IndigoVision's Source ID (Sourceld).



- 4. Open the IndigoVision Control Center's administrator client.
 - a. While in Setup mode, open the Alarms Explorer tab.
 - b. Click the Top Site.
 - c. Open the External Systems view.
 - d. Right-click and select New External System.

O IndigoVisio	n Control Center IndigoUltra (Trial Version) - administrator
File View Recording Device Site Alarms Use	rs Alarm Groups Filters Tools Help
🔘 Live 📙 Playback 🧔 Setup 🗲 🤅) Q Ø 🗄 🗙
Alarms Explorer 📮 🕱	1 Top Site 3
Visible Devices	Devices Alarms Activations Zones Maps Relays External Systems Data Sources Data Records Custom Ot < >
Custom Objects	There are no items to show in this view.
(001) Top Site	Heur External Gutter
	Trev Edenia system
Web Pages	Delete Delete
-	
루 Video Explorer 🧟 Users Explore 🐥 Alarms Explo	
Ready	0 items 0 📰 0

- e. Name the new external system BriefCam and add the BriefCam server IP Address (or if the BriefCam server is on a different network, the default gateway of the current network).
- f. Right click the top site, click **New Zone** and name the zone: BriefCam zone.
- g. Click OK.



New Zone Properties
Zone
Zone Name: BriefCam zone Matrix Number: 2
Alarm Server: 🕎 INDIGO-16 🗸 🗸
Schedule: None 🗸
Priority: 5 High Low Highest priority = 1 and lowest priority = 10
OK Cancel Help

- h. Right click on the new zone and click Set.
- 5. For each camera, carry out the following steps:
 - a. From the Video Explorer tab select a camera and write down the camera's name, and service ID.



- b. From the Alarms Explorer tab, right-click BriefCam zone and select New Detector.
- c. Set the detector type to External.
- d. Set the name using the camera name from step 5a and click Next.



New Detector Set Up
Name: Sony
Zone: BriefCam zone
✓ Allow detector to put zone into alarm
Type:
Advanced Analytics
of Basic Analytics
👽 CyberVigilant in Camera
Digital Input
>> Double Knock
External
O Unhandled Alarm
< Back Next > Cancel Help

e. Select the BriefCam external system that you created in step 4.f. Write down the Input Number (the event ID).g. Click Next.





- h. Click Next, click Next again and click Finish.
- i. Go to the IndigoCamerasMap.json file from step 2.
- j. Add a new row under Items by copying the existing row and replace the following values:
- Replace the value in Camerald with the Service ID from step 5a.
- Replace the value in Sourceld with the Input Number (event ID) from step 5f.
- Replace the value in Senderlp with the BriefCam server IP address.

III CFFregeren Flactdiele/Carritele	
🖬 IndipiCimentalitap.com 🕄	
<pre>1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1</pre>	varceId"-3, "GenderIp": "10.0.0.188"), varceId":

In the BriefCam Administrator Console's **Environment Settings**section, there are three settings relevant for sending alerts outside of BriefCam:

- 1. To send alerts outside of BriefCam, set the Respond.AlertsPublishingEnabled setting to true.
- 2. To send alerts to a VMS, check that the **Respond.AlertsPublishingToVMSEnabled** setting is set to **true**.
- 3. To change the polling interval, use the Respond.AlertsPublishingIntervalInMilliseconds setting.



Brief	Cam ADMIN	ENVIRO	NMENT S	ETTINGS		
Event	ts					
ଥି _® User	Management A	publish		Х	Show settings that I	have been changed
🕀 Deple	oyment •	Scope	Туре	Key	Value	Default Value
G Settir	ngs 🗸 🗸	GLO	Common	Respond.AlertsPublishingE	nabled false	false
Came	era Management	GLO	VS-Server	Respond.AlertPublisherAcc	eptUnsafeC true	true
Envir	onment Settings	GLO	VS-Server	Respond.AlertsPublishingTe	oVM5Enabled true	true
Local	ts Threshold	GLO	VS-Server	Respond.AlertsPublishingIr	ntervalinMil 1000	1000
aii Activi	ities 🔥	GLO	Common	AkkaHostConfig	akka : { loggers :	("Br
Dash	boards ^	GLO	Common	Administration.SystemEver	ntsPublishin false	false
		GLO	Common	Administration.SystemEver	ntsPublishin Critical	Critical

4. If you make changes to the settings, you need to restart or start the VSServer service.

When the IndigoVision plug-in is installed, the BriefCam.Indigo17Integration32.ini file is created at: C:\Program Files\BriefCam\BriefCam\BriefCam Server\32\plugins.

Set the AlarmServerIP parameter and remove the semicolon (;). (The other parameters are defined in the section above).

🔚 Brief	Cam.Indigo17Integration32.ini 🗵
1	don't remove this string;
2	[General]
3	;DbFolderPath="\\HOST_IP\SHARED_DB_FOLDER_NAME"
4	;Port=8135
5	;NvrPort=8130
6	;Token="ef182cd2-24f1-445d-bc69-5904e65a0c3f"
7	;UserName=
8	L;Password=
9	[Live]
10	L;LiveDelayMSec=0
11	[Alarms]
12	L;AlarmServerIP="172.1.1.59"

By default, BriefCam sends an alarm to IndigoVision and no further configurations are required to make the alarm appear in the IndigoVision client.

Note that only alerts produced by the IndigoVision connected cameras will be sent to the IndigoVision server.

Known Limitations

- Bounding boxes when playing the original video are displayed with an offset.
- In Indigovision 17.1 integrations, the alerts' start time is in offset.
- The RESPOND module for the IndigoVision VMS is only supported on cameras that are on the actual VMS (ControlSiteDb / NVR) and not cameras that are added through the gateway.

Intellicence Integration

Note that Intellicence was previously known as Verint and then Cognyte.





Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Intellicene	Symphia VMS	8.0	2024 R2 HF4 (including Classic and Next- Gen engine)	Real time alerts integration (L2a)	Yes
Intellicene	Symphia VMS	7.7.20189	2023 M1	Real time alerts integration (L2a)	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Ports Required

The following ports should be available when installing the plugin:

Port #
554, 5005, 7005, and 40000

Integration Installation Prerequisites

The Windows user must have access to the VMS file system in order for BriefCam to be able to fetch video from the VMS. Grant access by performing the following steps:

- 1. On each of the servers (BriefCam Server, Processing Server, and Alert Processing Server):
- 2. Open File Explorer and navigate to the VMS by entering the VMS installation path in the navigation bar (remember to add \\ before the actual IP address or host name).



3. Add the VMS IP/host name with the relevant user in the credential manager by navigating to **Control panel->User** accounts->Credentials manager and click Add a Windows credential.





4. You will be prompted with three fields to fill in: the VMS IP/host name, the actual Windows username, and the password. Make sure to enter the details correctly.

Add a Windows Credential	
← → × ↑ 🔤 > Control Panel > All Control Panel Items > Co	redential Manager > Add a Windows Credential
Type the address of the we Make sure that the user name and	ebsite or network location and your credentials
Internet or network address (e.g. myserver, server.company.co User name:	m):
Password:	
	OK Cancel

- 5. Set the **VSService** to log on as the user you have already configured to have access to the VMS file system. Do so by opening the **Services** dialog through the start menu or the task manager.
- 6. Locate the **VSService** service in the list and right click on it, select **Properties**, and then select the **Log on** tab.
- 7. Click on the **This account** radio button and fill in the details (account name and password). Make sure that you enter the credentials correctly and that the account name is the same as the user chosen in the previous steps.

Note that Intellicence VMS login credentials are case sensitive.



Post Installation Script

For new installations, after installing this VMS plugin you need to run a script that gives the BriefCam user permissions to access the relevant files.

In all places where the plugin is installed:

- 1. Open PowerShell as administrator.
- 2. Navigate to the following folder: cd {where briefcam server is installed}/tools/post_plugin_installation
- 3. Run the following command: .\set_permissions_for_plugins.ps1

Thumbnails

By default, thumbnail images for alerts sent by the Intellicence integration always have their name set to "Thumbnail.bmp". This can cause problems when the thumbnails for different alerts are saved to the same place – the wrong thumbnail is shown for the alert.

If you want each thumbnail to have its own name (the camera name with the alert start time), set the BriefCam.IntelliceneIntegration32.ini file's UseCustomThumbnailName parameter to true and remove the semicolon from the beginning of the row.





Sending Alerts to Intellicence

Alerts can be sent to the Intellicence client's UI (starting with Verint 7.6).

😨 Antha Roblesian 🛛 🕺	+	- 8 1
€ → C © bohot000/	NetReinstrajo	* 8 0
9 9 9		ALL B. A. S. T. VERINT
The best		
Nama Nam Danquitan.		
Jam Pierly		
Alem Note:		
	Tem 0 Documents ∰100100014338 3 Antipical one 3100014383914984492Canase RelayCanase 300-0-19-19-200 30 minutes from them 2	
	Red Tran Alleren	Activate Windows On to Scatery is Careful Pauri to activate Windows
🖽 🔚 🐼 😁		- 🖬 to 10 to 11/100

The alerts are sent to Intellicence via events.

To enable this functionality, carry out the steps below in the VMS Control Center.

Create a new event.

- 1. Click the System Components tab.
- 2. Click the Event Manager option.





- 3. In the Event Manager section, click Custom Events.
- 4. In the **Custom Events** section, click the plus (E) button.
- 5. Click the **General** tab.
- 6. Define the Event Settings. Note that the event must be named AnalyticsEvent.
- 7. To save your changes, move to another table.

¥		VMS Control Center
File Tools Help		
VERINT Ster localitost User a	inisinis 🗾 1	
Global Settings () Device Discover	7 🏘 System Components 🐳 HealthCheck 🔵 Maps	
Event Manager	Custom Events	
Scenarios 4		
Source Labels		
y Custom Events	Custom Event Name Event Category	
	GOLING Coston Security Events Custom Security Events	
λ^3	Custom Security Events	
	5	
	General Advanced parameters	
	Event Settings	
	Event Name: AnalyticsEvent	
	Description: Analytics Event	
	Event Category: Custom Security Events	-
	Generate System Alert. 🔽	
	Event Source Type: Camera	•
	6 - Event Priorite	
	Divide 1	
	riving.	
	(Higher)	(Lowest)
B. Devices	Critical (1) High (6) Medium (11) Low (16)	
The second		
Video Quality		
Recording and Archiving		
Virtual Matrix		
🚱 Event Manager 🛛 🔸	2	
E Client Connections		

Define the events' advanced parameters.

- 1. Click the Advanced parameters tab.
- 2. Click the plus (button.
- 3. Decide which of the following information you want to send with the event and based on that, define the relevant customer fields (using these exact names): RuleName, RuleType, ObjectId, AlertId, AlertTime, CameraId, CameraName, Thumbnail, Face Name, Face Source URL, Face Confidence, Lpr No, Lpr Confidence, Class, Class Details, List Name, Color, Person Attributes.
- 4. Make sure to set the Value Type to String for all the fields.





Add a new scenario.

- 1. In the Event Manager section, click the Scenarios option.
- 2. Click the plus (button.
- 3. In the General tab, define a scenario. In the image below, it was named BC_Scenario.





Add a scenario trigger event.

- 1. Click the **Event** tab.
- 2. Select the type of trigger. In the image below, the Event A only trigger is selected, which means that the scenario will be triggered with only one event (the event created in step 1).
- 3. Select the event created in step 1, by checking the AnalyticsEvent checkbox.
- 4. In the Source section, select the sources (cameras) for which you want to trigger the event.





Configure the scenario response.

- 1. Click the **Response** tab.
- 2. Click the plus () button.
- 3. In the Alarm Name field, give the name alarm. In the image below, the name given is BC_Alarm.
- 4. You can also configure a message that will be displayed in the client. It can contain all custom fields from an event, Verint default fields (Event Name, Received Timestamp, Source Name, Source Label) and event attachments.
- 5. Click **Apply**.



Note that there is no default timestamp field in the event. Therefore, the delay between the time that BriefCam generates the





alert and the time it is received at Intellicence may cause an incorrect record playback start position.

In the BriefCam Administrator Console's **Environment Settings** section, there are three settings relevant for sending alerts outside of BriefCam:

- To send alerts outside of BriefCam, set the Respond.AlertsPublishingEnabled setting to true.
- To send alerts to a VMS, check that the Respond.AlertsPublishingToVMSEnabled setting is set to true.
- · To change the polling interval, use the Respond.AlertsPublishingIntervalInMilliseconds setting.

B	rief Cam ADMIN		ENVIRO	NMENT S	ETTING	S			
Ē	Events					-			
2.	User Management	^	publish		×	Туре	× L	Show settings that have be	en changed
#	Deployment	•	Scope	Туре	Key			Value	Default Value
G	Settings	*	GLO	Common	Resp	ond.AlertsPublishingEnabled	d	false	false
	Camera Management		GLO	VS-Server	Resp	ond.AlertPublisherAcceptUr	nsafeC	true	true
	Environment Settings		GLO	VS-Server	Resp	ond.AlertsPublishingToVMS	Enabled	true	true
	Localization		00	VE.Exput	Barro	and AlastaD blicklastana	and a second	1000	1000
	Events Threshold		GLU	A3-Server	Kesp	ondukiertsHubilshinginterva	IIIIPAIL	1000	1000
зú	Activities	•	GLO	Common	Akka	HostConfig		akka : { loggers : ["Br	
83	Dashboards	^	GLO	Common	Admi	inistration.SystemEventsPub	olishin	false	false
			GLO	Common	Admi	inistration.SystemEventsPub	alishin	Critical	Critical

· If you make changes to the settings, you need to restart or start the VSServer service.

Known Limitations

• When working with Intellicence integrations, the view original video in Real-time alerts is offset and the object is sometimes not shown.

IPOrchid Fusion Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
IPConfigure	Orchid Fusion	2.6.5	5.6	Integration for on-demand and real- time (L2)	No

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.





3. From the Select a Version drop-down list, select the BriefCam version you are using.

Integration Plugin Installation

The address in Orchid needs to be in the following format: http://<hostname>:<port>.

The port value is optional (port 80 is used by default).

The port value needs to match the port specified in the Orchid Fusion installation, which is the same port used for the Orchid web client.

Known Limitations

Support for the H.265 format is done per request. If you want to use the H.265 format with this VMS, please contact BriefCam's support.

ISS Integration

Note that the information below is regarding the L2 integration carried out by BriefCam. A L3 integration with ISS SecureOS 10.10 was carried out by ISS. To obtain this plugin, contact ISS. For help installing and working with the SecurOS 10.10 plugin for BriefCam, contact ISS's Support team at https://support.issivs.com/. For additional information, see Third Party Integrations.

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
ISS	SecurOs	11.8	2024 R2 HF4	Integration for on-demand and real-time (L2) Note that a client integration (L3) was created by the VMS partner.	No
ISS	SecurOs	11.6	2024 M1	Integration for on-demand and real-time (L2)	No
ISS	SecurOs	11.2	2024 M1	Integration for on-demand and real-time (L2)	No

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.





ISS Ports

BriefCam uses the following outbound ports for the ISS integration: 8088 and 8888. Make sure that these two ports are available on the VMS and on the cameras.

If you set different ports on the VMS or on the cameras, remove the semicolon from the following lines in the BriefCam.IssIntegration.ini file's General section and enter the relevant port numbers:

OnVifPort = [port number for the camera];

RtspServerPort = [port number for the VMS server];

C:\Program Files\BriefCam\BriefCam Server\plugins\BriefCam.lssIntegration.ini - Notepad++

File Edit	Search View Encoding Language Settings Tools Macro Run Plugins
🕞 占 🗄	토 🕞 🕞 😂 🖌 🛍 🛅 구 ㄷ # 🏂 🤏 🔍 🍱 🔂 🚍 1
🔚 BriefCam.l	ssIntegration.ini 🗵
1	; Empty Line
2 8	[Fetching]
3	<pre>;MaxExportRetrying = 3</pre>
4	;SecondsToWaitBetweenRetrying = 5
5	;MaxParralelTasks = 3
6	;MinChunkDurationSec = 7
7	;GetCameraStatus = false;
8	;FFmpegPath = FFMPEG.EXE;
9	;PadTimeInSeconds = 5
10	
11	
12 8	[General]
13	;LiveDelaySeconds = 0;
14	;OnVifPort = 8088;
15	;RtspServerPort = 8888;
16	

Configuring ISS for Integration with BriefCam

1. Open the SecurOS configuration tab.

-BriefCam



2. Find Integration & Automation, click the plus (+) button, and click REST API.

-BriefCam

	_			_	
~		Sen	vers & Workstations		
	~	1	Computer ISS-105 [ISS-105]		
			Archive Converter (ISS-105) [1]		
			Health Monitor (ISS-105) [1]		
		>	E Desktops		
		>	💐 Devices (Cameras & Microphones)		
		•	Notifications		
		•	Integration & Automation	6	External application
		>	Mobile & Web Servers	ON	ONVIE Server
		٠	🚛 Remote systems (MCC VC/VR-connection)	RE	REST API
	>	_	Operator Workstation [OPERATOR]	RT	RTSP Server
				-	Space Keeper
				4>	VB/JScript programs

3. Configure the REST API (the defaults are shown below). If you use a non-default ISS port configuration, the ports need to be set in the plugin's .ini file as described in the ISS Ports section above.

~

4. From Integration & Automation, click the plus (+) button, and click RTSP Server.

~	Ser	vers & Workstations			
	~ 1	Computer ISS-105 [ISS-105]			
		Archive Converter (ISS-105) [1]			
		Health Monitor (ISS-105) [1]			
	>	Tesktops			
	>	🔜 Devices (Cameras & Microphones)			
	•	Notifications			
	~	Integration & Automation	6		
		REST REST API 1 [1]	Exe ON	External application	
	>	Mobile & Web Servers	VIF	ONVIF Server	
	•	Remote systems (MCC VC/VR-connection)	SP	RTSP Server	
	> 🛃	Operator Workstation [OPERATOR]		Space Keeper VB/JScript programs	

5. Select cameras.



TSP port:	554	•	HTTP port:	81	•	RTSP Specification:	RFC 2326	~
✓ ∑ Se	curOS Premiun Computer ISS Camera A	n [1] - 105 [IS xis(0):0	S-105] [1]					
	Camera A	vie(1)-0	[2]					

6. From Integration & Automation, click the plus (+) button, and click ONVIF Server.

~	Ser	vers & Workstations				
	~ 🗎	Computer ISS-105 [ISS-105]				
		Archive Converter (ISS-105) [1]				
		Health Monitor (ISS-105) [1]				
	>	Tesktops				
	>	🔜 Devices (Cameras & Microphones)				
	•	notifications				
	~	Integration & Automation	0		-	-
		REST API 1 [1]	Ē	X	External application	
		CTCP Convert [1]	V)N /IF	ONVIF Server	
		RTSP RISP Server 1 [1]	R	T	RTSP Server	
	>	Mobile & Web Servers		1	Space Keeper	
	•	Remote systems (MCC VC/VR-connection)		4	VB/JScript programs	

7. Select the RTSP Server and click Apply.

ONVIF port:	8088	÷
RTSP Server:	Not specified	~
	Not specified	
	RTSP Server 1	
	Not specified RTSP Server 1	

Known Limitations

- Bounding boxes when playing the original video are not supported.
- Support for the H.265 format is done per request. If you want to use the H.265 format with this VMS, please contact BriefCam's support.

LenelS2 OnGuard Integration




Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
LenelS2	OnGuard	8.2	2024 R2 (including Classic and Next-Gen engine)	Real time alerts integration (L2a) only	N/A
LenelS2	OnGuard	8.1 Cloud	2024 R2 HF4 (including Classic and Next- Gen engine)	Real time alerts integration (L2a) only	N/A
LenelS2	OnGuard	8.1	2024 R2 HF4	Real time alerts integration (L2a) only	N/A
LenelS2	OnGuard	8.0	2024 R2 HF4 (including Classic and Next- Gen engine)	Real time alerts integration (L2a) only	N/A

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Prerequisites

The LenelS2 OnGuard API license should be installed on the Lenel side. For more information, see: https://www.lenels2.com/en/security-solutions/third-party-integration/oaap-partners/briecam-video-analytics-platform/.

The Video Analytics Platform API requires a LenelS2 OnGuard API license and has a unique part number. Contact your LenelS2 Value Added Reseller for pricing.

Receiving BriefCam Alerts

This section explains how to get alerts from BriefCam to your OnGuard® access control system.

- Right-click on the BriefCamLenelS2OnGuardPlugin.exe file and select Run as administrator. The installation
 path for the plugin is: {BriefCam Server Folder}\PushAlertsService\plugins\. After successful
 installation there will be a new folder created LenelS2OnGuard inside the plugins folder.
- 2. In the BriefCam Administrator Console, open the Hosts screen and click on the host's settings icon
- 3. Check the **Push Alerts Service** checkbox and click **Apply**.

-BriefCam

Enable Services		×
	Milestone SSO Provider	
	Multi-site Hub BI Data Gateway	
	Multi-site Hub SSO Gateway	
	Multi-site Site BI Export Service	
	Notification Service	
	Outbound API Gateway	
	Processing Server	
	Push Alerts Service	
	Rendering Service	- 1
	Task Management Service	
\checkmark	Video Streaming Gateway	- 1
	VS Server	
Cancel		Apply

4. Open the Services screen and make sure that the Push Alerts Service is set to Running.

Entities	✓ Hosts	Status	~	
	Entity ~	PID	Host	Status
	Notification Service	48164	Brief-Radoslave	Running
	Outbound API Gateway	12840	Brief-Radoslave	Running
	Processing Server	N/A	Brief-Radoslave	 Stopped A
	Push Alerts Service	11092	Brief-Radoslave	Running
	Rendering Service	15952	Brief-Radoslave	Running
	Task Management Service	12780	Brief-Radoslave	Running
	Video Streaming Gateway	15552	Brief-Radoslave	Running
	VS Server	41764	Brief-Radoslave	Running

5. From the Environment Settings screen, search for the text: PushAlertsService.



ENVIRONMENT SETTINGS

Eventeetstanoised	× Type	✓ Bhow settings that have been changed			
Scope	Туре	Key	Value	Default Value	D
GLOBAL	Common	Agent AgentSupportedServices	ProcessingServer.exe,AlertP	ProcessingServer.exe;AiertProcessingServ	s
GLOBAL	Common	Push-WertaServiceEnabled	THE	fatse]
OLOBAL	36	PushWertsBervice.LenelThusbAllCertificates	tue	THE	r
GLOBAL	36	PushViertsService LenelDirectoryld	84	id-1]
GLOBAL	35	PushAlertsService.LenelLogicalSource	Briefcam	Briefcam	1
OLOBAL	36	PushWertsBervice.LeneiLoginiRatBeconds	60	60	1
GLOBAL	36	PushAlertsService.LenelKeepAliveSeconds	60	60	s
GLOBAL	35	PushAketsService.LenelSendAketsRetries	1	4	R
OLOBAL	36	PushAlertsBervice.LeneiLoginTokenExpirationBeforeMinutes	5	6	P
GLOBAL	26	PushAlertsService.LenelUsemame	38]
GLOBAL	36	PushWertsService.LenelPasaword	*****		
GLOBAL	36	PushAlertsBervice.LenefTargetEndpoint	https://172.1.1.135.6080; http:		1

6. Update the following environment settings:

- **PushAlertsServiceEnabled** Set to **true**.
- PushAlertsService.LenelDirectoryId Enter the OnGuard directory ID. To get a list of the different Lenel Directories, use the following URL to retrieve a list of directory ids: https://OnGuard server address:OnGuard port/api/access/onguard/openaccess/directories?version=1.0

For example: https://172.1.1.245:8080/api/access/onguard/openaccess/directories?version=1.0

- PushAlertsService.LenelLogicalSource Select the logical source if it is different than the default value (Briefcam).
- PushAlertsService.LenelUsername Enter a user created in the Lenel system.
- PushAlertsService.LenelPassword Enter the user's password. The value is protected by displaying asterisks only.

Note that OnGuard credentials (the username and password above) should be the same on all OnGuard instances, if there are multiple instances set up in the **PushAlertsService.LenelTargetEndpoint** environment setting.

 PushAlertsService.LenelTargetEndpoint – Enter the OnGuard instance/instances where alerts will be sent followed by a colon (:) and the OnGuard port. If multiple OnGuard instances are setup, the addresses need to be separated by a semicolon (;). In addition, a pool will be created of available instances, where users can map RESPOND rules. The addresses of the OnGuard instances in this setting should match the ones mapped in the EndpointRuleMapping.json file.

Single instance example: "https://{OnGuardAddress}:8080"

Multiple instance example: https://{OnGuard1Address}:8080; https://{OnGuard2Address}:8080; https://{OnGuard3Address}:8080;"

7. From the BriefCam Administrator Console, restart the **Push Alerts Service**. This reloads the configuration of the environment settings.

Set Up Endpoint Rule Mapping

By default the **Push Alert Service** will not send alerts to the pool of OnGuard instances.

To send alerts to an OnGuard instance, the Rule Name and the OnGuard instances need to be mapped.

This is done in the LenelS2OnGuard.EndpointRuleMapping.json file located in the LenelS2OnGuard Plugin directory.

The file is structured with key-value pairs ("key": "value") where:

- Key Name of the RESPOND rule
- Value List of OnGuard endpoints (one or multiple)

For example:

=BriefCam

{

"RespondRule1": ["OnGuardInstanceEndpoint1", "OnGuardInstanceEndpoint2", "OnGuardInstanceEndpoint3"],

"RespondRule2": ["OnGuardInstanceEndpoint1", "OnGuardInstanceEndpoint5"],

```
"RespondRule3": [ "OnGuardInstanceEndpoint2" ]
```

```
}
```

 BriefCare Protect 						NUMBER REPORT	* essente 👔 Enterfaction of 🤤
ALISTS							
Q tush.							• •
o 🖦	E Creek	12 may	Crusted	E NATA	12 244	E blate	
Refarmer Gelerand			000000 (Date Per				
D BrotCarr Maid Kinter Carera			0.0310874				
🔚 LenelS2OnGuar	.EndpointRuleMapping	json 🖾					
1 🖂 🕻							
2 "B	riefCam-Rule2-	Kitchen-Came	ca": [" <u>ht</u> :	tps://172.1.1.	134:8080"],		
3 "B	riefCam-Rulel-	Outside-Came	ca": [" <u>ht</u>	tps://172.1.1.	<u>134:8080</u> ", "	https://172.1	.1.135:8080"]
4 -}							
5							

After the mapping in the json file is updated, the **Push Alerts Service** needs to be restarted, in order for the new configuration to reload.

Once started with the rule mapping, the **Push Alerts Service** will send the alerts from each mapped RESPOND rule to the respectively mapped OnGuard instance endpoints.

The OnGuard instance endpoints should match the ones set up in the **PushAlertsService.LenelTargetEndpoint** environment setting.

If the endpoint is mapped in the Mapping file and not in the **PushAlertsService.LenelTargetEndpoint** environment setting, an error will be displayed in the PushAlertService.log file.

Create an OnGuard Logical Source

A BriefCam Logical Source needs to be created on each OnGuard instance that will receive alerts from BriefCam. This is needed for mapping incoming alerts.

To create an OnGuard logical source:

- 1. Log in to the OnGuard System Administration application.
- 2. From the Additional Hardware menu, select Logical Sources.



3. Create a Logical Source named BRIEFCAM and click the Add button.



in System Administration - System	Account - [Logical Sources]							
Application Edit View Administration	Access Control Mgnitoring Video Additio	nal Hardware Logical Access	Window Help					
🔍 🗟 🕭 📍 🔏 🦂	8 🗈 🚍 📲 🖧 🖵	G 🛛 🖏	💷 🖻 🕙 🍋	0 digh				
16 🖉 🖽 🗉 🖂	🗑 🕑 😂 🎘 🗮	🕪 🗔 🧸 🛞	۶ 🖇 🚥 🥐 📼	🕑 🛍 👻 🕾 🧏				
Logical Seurces Logical Devices Logical Sub-Devices								
Name ***	Name: BRIEPCAM	C Online						
	World time zone: (SMT+02.00) Jerusalem	~						
	Daylight savings							
Add Modily Delete Help.	Multiple Selection							

Create an OnGuard Logical Device

Logical devices need to be created for each camera that will be used for RESPOND rules that generate alerts and are being sent to OnGuard instances.

This means that depending on the mapping between RESPOND rule and OnGuard instance endpoints, logical devices need to be created on the OnGuard instances that are receiving the RESPOND alerts.

For each RESPOND rule alert sent, the target endpoint should have the Rule Camera Name set up as a logical device under the BRIEFCAM logical source.

To create an OnGuard logical device:

- 1. Log in to the OnGuard System Administration application.
- 2. From the Additional Hardware menu, select Logical Sources.
- 3. Open the Logical Devices tab.
- 4. In the **Name** field, set the name of the logical device to the desired camera name. Note that the camera name should be the same as is in the VMS.
- 5. From the Logical Sources field, select the BRIEFCAM logical source.
- 6. Click the **Add** button.



🕼 System Administration - System Account - [Logical Sources]	
Application Edit View Adginistration Access Control Mgnitoring Video Additional Hardware Logical Access Window Belp	
S # ? & * # = = = * & V V V v = = = = = * · *	
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
Logical Sources Logical Devices Logical Sub-Devices	
Device Logical Scut Name: EXchanner_1721.0.100 BRERCAAM Note:	
LineCones BRITCAN LineCones BRITCAN	
Control wheel - carene 172.1.1. BREFCAM Logical Source: Logical Source: DebiduetrifunciesControl Control Cont	
<u>د</u>	
Add Modiy Delate Heb Maliple Selection	
🔯 System Administration - System Account - [Logical Sources]	
Application Edit View Administration Access Control Mignitoring Video Additional Hardware Logical Access Window Help	
S & # ? & & # B = # & T G G O E = ■ B O E &	
「	ŝ
Logical Sources Logical Devices Logical Sub-Devices	
Device Logical Seau Name: McGerban, 170,13.508 REECLAM Consentional	
a Level Comers BRUCAM	
Datsile street - carries 172.11 BREFCAM Lagical Source: Rest-Class Rest-Rest-Rest-Rest-Rest-Rest-Rest-Rest-	
Calment President and Calment	
۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲	
OK Carcol One Heb.	

Lensec Integration

Integration Summary

VMS	Product	Version	Last Tested BriefCam	Integration Level	H.265
-----	---------	---------	----------------------	-------------------	-------



Partner			Version		Support
LENSEC	Perspective VMS	6.0.0	2024 M1 HF2	Real time alerts integration (L2a) only	No

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Prerequisites

To view BriefCam alerts in Lensec, the Lensec user needs to be part of an operator group (on the Lensec VMS) at the minimum.

Installation Steps

- 1. From the BriefCam Administrator Console, stop all currently running services.
- 2. Check "Programs and Features" to confirm that the Lensec plugin is not already installed.
- 3. Download the BriefCam Lensec plugin:
 - a. Open the following URL: https://www.briefcam.com/installation-downloads/.
 - b. From the Select a Product field, select VMS PLUGINS and from the Select a Version field select BRIEFCAM 2024 M1 HOTFIX1 (FEB 12, 2024).

=BriefCam	SOLUTIONS	WHO WE SERVE	WHAT WE DO	WHAT'S NEW	PARTNERS	CONTACT	REQUEST A DEMO	۹
	INS	TALL	ATIO	N DO	own	ILOA	DS	
	Select a F	Product				Select	a Version	
VMS PLUGINS				BRJE	FCAM 2024 M1	HOTFIX1 (FEB, 1)	2, 2024)	

- 4. Run the downloaded BriefCam Lensec plugin.
- 5. Open the Briefcam.LensecIntegration.ini file (located at C:\Program Files\BriefCam\BriefCam Server\plugins) and change the FFmpegPath setting to: C:\Program Files\BriefCam\BriefCam Server\FFmpeg.exe. Save the changes.

1	;don't remove this string
2	E [Live]
3	;LiveDelayMSec = 0
- 4	L
5	[Fetching]
6	;FFmpegWrapperDebugLog = false
7	<pre>FFmpegPath = "C:\Program Files\BriefCam\BriefCam Server\FFmpeg.exe"</pre>

- 6. Add the Lensec Integration to BriefCam:
 - a. In the BriefCam Administrator Console, open the Settings tab and click Camera Management.
 - b. Click the Add Directory button.



BriefCam ADMIN	CAMERA MANAGEMENT						₽ ©	(E) Sign Ca	
E feets	Litenset 1000 Renaining 125 Activated 45								
2. User Management A		0					0.000		
🔂 Deployment 🛛 👻	and the second s	 en. 4						rony analysis can	-
Horts	Shoe store entrance camera (Disabled)	Name	Activation	Enabled	Overhead	Counting	Path		
GPUs	Office entrance (3)	Sarry INC/US6ex/UM6ex	2021/07/211	•			ML2083/.	a 0	
Services	Contestantin (14)	ANS QUELS ME IN NOV.	2021-07-211				/ML2083/	a 0	
C) Setting 🗸 👻		AUES P3255 CVE Nature	2021/07/211				ML2083/_	4	
Carriers Management									
Environment Settings									
Localization									
Events Threshold									
≦Í Activitius →									
	Add Divertory						O tenterty	n 199. And	•

- c. From the Video Integration field, select Lensec Integration.
- d. In the **Directory Name** field, enter a display name for the user directory.
- e. In the Address field, enter the Lensec server address, for example: 172.1.1.111.
- f. In the **User Name** field, enter, for example: **admin**.
- g. In the **Password** field, enter a password of up to 12 characters, for example: **Tadmin#**.
- h. Click Add.



Add Directory	×
Fill in the fields below	
Video Integration * Lensec Integration	
Directory Name *	.
Address *	
User Name * administrator	
Password	
Cancel	Add

- 7. In the Add/Edit Cameras screen, activate the desired Lensec cameras.
- 8. Restart all BriefCam services.
- On the Windows machine, restart Internet Information Services (IIS).
 From the BriefCam Administrator Console, make sure that all services are running properly.

March Networks Integration





Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support	Additional License Required
March Networks	Command Enterprise Software (CES)	2.20	2024 R2 HF5	Forensics only integration (L1)	No	Yes
March Networks	Command Enterprise Software (CES)	2.17	2024 R2 (including Classic and Next-Gen engine)	Forensics only integration (L1)	No	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Configuration of the March Networks System

Creating a BriefCam User Profile

In the March Networks CES administration:

- 1. Click the March Network logo in the top left corner.
- 2. From the drop-down list, select the User Management option.
- 3. Select the **Profiles** tab.
- 4. Click the Add New Profile button (top left part of the screen).
- 5. Create the BriefCam Profile.
- 6. Enable the following rights (leaving all other settings as-is):
 - Live Video
 - Archive Video
 - Export to CME
 - Device Management
 - Add Device
 - Export to External Media

Click the Save icon (top left part of the screen).





C REALING			84 C	¥ 📲	
A Lonei Rinepmet	Der Haupenet 👘 🗰 🗉				
RC Alternationant Research	then und longs				
	1 11				
The One Reception of	Public Loss I Desiglion				
9K ton	Advanceuror An advanceuror of constant Enderprise				
O Information	b trafun hufe at				
in the second se	Retri	Second Rights		Records Rights	Application Rights
	Ballon India	 Dre viteo 	Server Lings	Applace Tree	
<u>∎</u> 100 - 1	Decision of the local	 Andrew tistes Andrew tistes 	Internet to External Management	0.000	
7 140 1	н	Depicts RM (K3MMAC)	Enders Yout Acres	O Heater	
E inde		Hada Calatian	Gase and Tag Hanaparteri	Logical Trees	
E licines 4		Take Stuppfor	Watermark.	O site	
 Harsh L (Camera 1) 		lade .	(S North	O rieben	
 March Carrol JOanness (1) 		Talk BTT Contract	O tatleni	Periodal Tree	
		Realth Restanting	Privaty Instantia	Lawood	
* 🛅 Usol	Restort accessing data states	Aigen Northring	NOT TOWNED	C short	
Camera 1	the budge Trend	Rass Ranapment	International with finites		
	R Terr	itse Hangamark	and and a sub-provide state		
	O ush screen	 Device Management 			
	O US M	2 addresss			
	Timeset II (minubo))	Remote Center			
•	Access to menter two, centrel PTC convers, an	d more archive relea			
	h Martane Suffcet rgits to martan auton.				
n helona .					
- C feomi					
1 I					
1 I					
1 I					
1 I					
1 I					

Creating the BriefCam User

In the March Networks CES administration:

- 1. Click the March Network logo in the top left corner.
- 2. From the drop-down list, select the User Management option.
- 3. Select the Users tab.
- 4. Click the Create New User button.
- 5. Fill in the User Name.
- 6. From the **Profile** drown-down list, select the previously created BriefCam Profile.

- Set the Status to Enabled.
 Set the User Password.
 Drag and drop the System and Logical resources that will be used by the BriefCam integration.
- 10. The System and Logical resources can be Recorders, Individual Cameras or the Whole System. If the integration needs to access the entire CES system, just drag and drop the entire System and Logical folders. Make sure only to drag and drop the resources that will be used.
- 11. Click the Save icon.

COL440010				왕 삼 😽	
NORM 1	A Use Respond	***			
4, X % M	Police User Locificage				
× 7.	I C H B C B ;	Alter Mark Notice The			
2404 *		T Date F Derline T Polis T by	ion Tentory P Lapial Tentory	T See T Geblair F G	in I
- D Spian	 L strat 	budied ideas Advancestor to	tan Lapur	Lincal about Rome	
- S Hudets	 Litefan funer 	Oxded BC,Aurent Briefum Polite Se	tan Lapisi	Uncal item None	
	+ 👗 BisCan fumer	Initial K. Arran Briefan Polis In	iam Legiul	Local Derr. Norm	
	- T BACH DA.	bookd itcher information public to	ten Lapor	Licit der Rine	
	tree Information			_	
	Die Tate	SCAW Profile	Bridge Polite	-	
	Full Name	BrefCan User Mater	2 bulled	- 1	
	Ernal Address		-		
	Territor Inc. Base	Cwth	ale fore	1	
	The second second second		E lagat she catholic is enough		
* Inplut -	Paston	Pare	PE Dange B to a charge of the	City	
 In 1907 	Ratoper				
Gross 1	multiple Records				
	Contract Contract	Select All	ai 14	dag all	
	D lyin		inglasi		
		Debb		Debrie	
	 I Biefan Totler 	Oxded N_Yorke Bielian Polic So	tan Lopisi	Local iter None	
	+ 👗 Brieffan Terlan	Insteil Kryteinel BinKan Polle by	ien Lepid	Local Dev. Name	
f front -					
- D Pesnel					



In the March Networks CES administration:

- 1. Click the March Network logo in the top left corner.
- 2. From the drop-down list, select the License Management option.
- 3. Select the Additional Components tab.
- 4. Select the BriefCamIntegrationPlugin.
- 5. Drag and drop all needed cameras from the Logical tree to the Licensed Resources.



Configuration on the BriefCam Side

- 1. Install BriefCam's March Network plugin.
- 2. In the BriefCam Administrator Console, open the Settings section and click Camera Management.
- 3. Click the **Add Directory** button.

-BriefCam ADMIN	CAMERA MANAGEMENT							<i>.</i> ? (0 🤇	Spr Out
EVents	Licenses: 2000 Remaining: 925 Activated: 65									
₿ ₈ UserManagement ▲										
🖶 Deployment. 🔍 👻	Search Directories. Q	Search/Carr	wm. 9,						tellar only a	unalytic carmenas
Halo	Shoe store enhance camera (Disabled)		Name	Activation	Enabled	Overhead	Counting	Path		
GPUs	Office entrance (3)		Sary SNC-VB6xx/VM6xx	2021/07/211.				/MIL2083/_	虛	0
Services	 A second (a) 		ANDS Q0525 Mit 11 Netw	2021/07/211				/MIL2083/_	壚	0
C) Series v			AKSP225FD/E Networ	2021/07/211				/ML2083/	堆	
Camera Management										
Environment-Settings										
Localization										
Events Threshold										
<u>⊴i</u> Asivitis ∧										
	Add Directory							O Banch	erapi 20	And

The Add Directory dialog will open.

1. From the Video Integration field, select March Network Integration.

-BriefCam

- 2. In the Directory Name field, enter a display name for the user directory.
- 3. In the **Address** field, enter the IP/host address of the March Network recorder. Note that http:// or https:// must be added before the address.
- 4. In the **User Name** and **Password** fields, enter the March Network server user name and password that was set up in the previous steps. This user must have permissions in the VMS to the cameras exposed for BriefCam.
- 5. Click Add.
- 6. Repeat the steps above for each recorder.

Configuring the Integration

When the March Networks plugin is installed, you'll have a Briefcam.MarchNetworksIntegration.ini configuration file, which by default is located at: C:\Program Files\BriefCam\BriefCam\BriefCam Server\plugins.

```
🔚 Briefcam.MarchNetworksIntegration.ini 🔀
 ;don't remove this line
[Live]
 ;LiveDelayMSec = 0
[Fetching]
 ;FFmpegWrapperLog = false
 ; FFmpegPath=FFMPEG.EXE
 ;FFmpegContainer=mp4
;AllowedGapMSec = 500
[General]
 ;OperationTimeoutSecs = 30
[Alarm]
 ;NOTE: Alarm will be extended for this time interval
 ;ExtendBySec = 0
 :NOTE: Consider the alarm status "On" only after this time interval
 :ArmingTimeSec = 0
 ;NOTE: Maximum time interval of "On" status. Use 0 for infinite
 ;MaximumSec = 1
 ;TimeoutCreateAlarmSourceSec = 30
```

This file includes the following parameters:

- LiveDelayMSec Sets a delay for incoming live streams if the clocks of the VMS and BriefCam are out of sync and the live stream times are different than the BriefCam time.
- FFmpegWrapperLog Enables additional logs for FFmpegWrapper.
- **FFmpegPath** The path to the ffmpeg.exe file.
- FFmpegContainer The type of container used by FFMPEG.
- AllowedGapMSec The number of milliseconds gap allowed in the fetched video.
- OperationTimeoutSecs The timeout for all general operations between the VMS and BriefCam.
- ExtendBySec The alarm will be extended for this time interval.
- ArmingTimeSec The alarm status will be considered "On" only after this time interval.
- MaximumSec The maximum time interval of "On" status. Use 0 for infinite.
- TimeoutCreateAlarmSourceSec Timeout for creating alarms.

See also: Troubleshooting - March Networks

Milestone Integration





Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Milestone	XProtect Corporate	2025 R1	2024 R2 HF5	Workflow integration (L4)	Yes
Milestone	XProtect Corporate	2024 R2	2024 R2 HF5	Workflow integration (L4)	Yes
Milestone	XProtect Corporate	2024 R1	2024 R2 HF5	Workflow integration (L4)	Yes
Milestone	XProtect Corporate	2023 R3	2024 R2 HF4 (including Classic and Next- Gen engine)	Workflow integration (L4)	Yes
Milestone	XProtect Corporate	2023 R2	2024 M1	Workflow integration (L4)	Yes
Milestone	XProtect Corporate	2023 R1	2023 M1 (including Classic and Next-Gen engine)	Workflow integration (L4)	Yes
Milestone	XProtect Corporate	2022 R3	2023 M1 (including Classic and Next-Gen engine)	Workflow integration (L4)	Yes
Milestone	XProtect Corporate	2022 R2	6.4 HF2	Workflow integration (L4)	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.







To install the SSO provider, BriefCam Open API (BOA), which is licensed separately, must be used on the BriefCam Server.

Ports Required

The following ports should be available when installing the plugin:

Port #
8030, 8080, 80, and 554

Milestone Integration Plugins

To integrate BriefCam and Milestone, you need to install the following plugin:

BriefCam Plugin	Where to Install
F Milestone F plugin	For OX5 environments, on every machine where the BriefCam Server, Processing Server, or Alert Processing Server is installed.

To embed BriefCam in the Milestone XProtect Smart Client you also need to install the following two plugins:

BriefCam Plugin	Where to Install
Embedded Client for Milestone XProtect plugin	On every machine running the Milestone XProtect Smart Client where embedded access to BriefCam is required.
Milestone XProtect Management Client plugin	On every machine where the Management Client is installed.

BriefCam Milestone Plugin Installation

 Run the VMS Integration Plugin Installation by right-clicking on the BriefCamMilestonePlugin_
 Version_number>.exe file and selecting Run as administrator. You need to install the VMS integration plugin on every machine on which the BriefCam Server/Processing Server/Alert Processing Server is installed.

Note: If you are using the latest Windows Update and a Windows Defender alert appears, click the **More info** link and click **Run anyway**.



Windows protected your PC

Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk. More info

- 2. Click the **Get Started** button.
- 3. Read and accept the License Agreement terms. Click Next.
- 4. Select the path to the plugin installation directory. Note that it should be the same directory as the BriefCam Server directory. By default, it is set to C:\Program Files\BriefCam\BriefCam\BriefCam Server\. Click Next.
- 5. If you do not want to enable SSO on the BriefCam Embedded XProtect Client, leave the **Configure the Milestone** SSO provider checkbox unchecked and click Next.
- 6. If you want to enable the BriefCam Embedded XProtect Client, on the main BriefCam server where the Milestone SSO Provider Service is enabled:
 - a. Check the **Configure the SSO provider** checkbox. On all other machines, such as a machine with the Processing Server or Alert Processing Server, do not select the checkbox

Х

- b. Enter the Milestone VMS address and the SSO provider address. The SSO provider address should point to the host running the MilestoneSSOProvider service. for example: http://briefcam-server:8030/ MilestoneSSO/.
- c. Verify that the provided URLs are correct by clicking the Verify URLs button.
- 7. Click Install.

-BriefCam

	*
=BriefCam	Install Milestone Plugin
SSO Settings	
To enable SSO on the Br Client, you need to conf Service.	riefCam Embedded XProtect figure the Milestone SSO Provider
Select the checkbox belo on the server where the is enabled.	ow if you are installing this plugin Milestone SSO Provider Service
✓ Configure the Miles	stone SSO Provider service
Milestone VMS address (host or IP)	10.1.2.44
SSO provider address (for web listener)	http://localhost:8030/Milestor
Verify URLs	
Back	Install

8. If your organization will be using BriefCam's RESPOND module, install Milestone's Open Network Bridge component. This allows the Milestone plugin to fetch video stream from the Milestone VMS. The component is not included in the standard Milestone management + recorder installer.

To download the component, go to: https://www.milestonesys.com/downloads/ and click the **Download Software** option. Log in with your Milestone user and password and from the **Product** field, select **Milestone Open Network Bridge**.

When configuring Milestone's Open Network Bridge, a user and password is created. Make a note of these, because you will need them when configuring the Milestone directory in the BriefCam Administrator Console.

See also: Setting Up Multiple RTSP Bridges

Silent Installation of Milestone Integration Plugin

To run a silent installation of the Milestone Plugin without SSO, use the following command line:

{ MilestoneInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefcam"

To run a silent installation of the Milestone Plugin with SSO, use the following command line:

{ MilestoneInstaller file name} /qn APPDIR="\$env:ProgramFiles\briefcam" INSTALL_SSO_PROVIDER="YES"

=BriefCam



MILESTONE_VMS_ADDRESS="{ip/hostname}" SSO_PROVIDER_ADDRESS="{address url}"

Milestone Embedded Client Installation



When using the embedded client, BriefCam can only work with a single Milestone VMS.

After you have installed the Milestone plugin on the BriefCam Server(s), you are ready to install the Milestone Embedded Client.

1. On each of the XProtect Smart Client machines where you want to embed BriefCam, right-click the BriefCamEmbeddedClientForMilestoneXProtect_<Version_number>.exe file and select Run as administrator.

Note: If you are using the latest Windows Update and a Windows Defender alert appears, click the **More info** link and click **Run anyway**.



- 3. Accept the terms of the license agreement.
- 4. Click **Next** and the following screen will appear.





- 5. Select the installation destination path. Note that the installation path must be the same directory where Milestone XProtect Smart Client is installed.
- 6. Select which edition of BriefCam you are using.
- 7. Click Next and the following screen will appear.





- In the Web Server Address field, enter the BriefCam Web Application URL (which should point to the server where BriefCam and BriefCam Open API (BOA) are installed). Do not include http: in the URL, because http: is added automatically by the installer.
- 9. In the **Open API (BOA) Server Address** field, enter the address where the BriefCam Open API (BOA) was installed.

Once the installation is complete, the URL configuration can be modified manually as needed. 10. Verify that the provided URLs are correct by clicking the **Verify URLs** button.

The URLs will be saved in BriefCam.MilestoneEmbeddedViewer.dll.config, which is located by default at C:\Program Files\Milestone\XProtect Smart Client\MIPPlugins\BriefCam.

- 11. Click Install.
- 12. After the installation is completed, on the VMS server, open the

BriefCam.MilestoneEmbeddedViewer.dll.config file (located by default at C:\Program Files\ Milestone\XProtect Smart Client\MIPPlugins\BriefCam).

13. The server address within this file must include a forward slash ("/") after "app". This forward slash is missing by default and will cause a 404 error if not added.





- <appSettings> < !-- Client site address (.. /synopsis/# or .. /app) --> -- Client site address cadd key="serverAddress" value="int-svetan/app/"/> <!--Boa site address--> <add key="boaServerAddress" value="http://int-svetan/BOA"/> <add key="InstallationType" value="SMB"/> <add key="allowSelfSignedSSL" value="false" /> < --- add key="boaVersion" value="1.0" /--> <!--add key="keepAliveIntervalMS" value="60000" /-->
 <!--add key="httpTimeoutMS" value="120000" /--> < --- add key="pageLoadTimeoutMS" value="1000" /--> < --- add key="browserLog" value="false" /--> < --- Custom path to extract DotnetBrowser Chromium files--> <!--add key="dotnetBrowserChromiumDirectory" value="" /--> <!-- add key="BrowserLogLocation" value="c:\DotNetBrowserLog.txt" / --> </appSettings>
- 14. You now need to install the Management Client for Milestone plugin as described below in the Management Client for Milestone Installation section.

Silent Installation of Milestone Embedded Client

To run a silent installation of the Milestone Embedded Client, use the following command line:

.\BriefCamEmbeddedClientForMilestoneXProtect_{version number}.exe /qn BC_WEB_SERVER_ADDRESS="{path to synopsis}" BC_BOA_SERVER_ADDRESS="{path to BOA}" INSTALLATION_TYPE="{SMB or Default}" APPDIR=="\$env:ProgramFiles\BriefCam"

Where SMB is the value when using the XProtect Rapid REVIEW platform and Default is the value when using the **Protect** or **Insights** platform.

The APPDIR flag is optional and points to the location where the Smart Client is installed. If it is not specified, the Milestone Embedded Client will be installed at: C:\Program Files\Milestone\XProtect Smart Client\.

Management Client for Milestone Installation

Since version: BriefCam 2024 R1

You will now install BriefCam's Management Client for Milestone plugin on the same machine where Milestone's XProtect Management Client is installed.

- 1. On the same computer on which the Milestone XProtect Management Client is installed, right-click on the BriefCam Milestone XProtect Management Client plugin and select Run as administrator.
- 2. In the Welcome screen, click Get Started.
- 3. Read the license, accept the License Agreement terms, and click Next.
- 4. Select the installation destination path and click Install.
- 5. Log into the Milestone XProtect Management Client.
- 6. Right-click on the Roles section and add a new role, for example: BriefCam Users as shown in the image below.
- 7. Make sure that the new role is selected and click the **BriefCam** tab at the bottom of the screen. In the Milestone XProtect Management 2023 R1, the tab is named **MIP**





- 8. From the Role Settings section, select the BriefCam role, as shown in the image below.
- 9. Give these users access to BriefCam by selecting the Allow access to video analytics platform checkbox.

Milestone XProtect Management Client 2023 R3



10. If the checkbox is not checked, the user will see the following message when clicking the BriefCam tab:







For embedded environments, you will now connect the Milestone XProtect Smart Client to the BriefCam server as described below.

Connecting Milestone XProtect Smart client to the BriefCam Server

To establish a connection from the Milestone XProtect Smart Client to the BriefCam Server:

- 1. Carry out the Initial Setup as described in the BriefCam Administrator Guide.
- 2. In the BriefCam Administrator Console, open the Deployment section and then Hosts.
- 3. Find your host and click on its gear icon.

=BriefCam ADMIN	HOSTS		P	Sign Out
Events			Search	٩
User Management ✓	Address ~	Status	Last Update	
Users & Groups Directories	BC-Appliance	Not reachable	2019/08/13 16:33	\$
Deployment	16GPU	Running	2019/08/14 10:29	۵
Hosts				

4. Select the Milestone SSO Provider service and click Apply.

-BriefCam

Enable Services

Х

Templates	~	
	Service Type ^	
	Alert Processing Server	
\checkmark	BI Rule Engine Service	
	Face Recognition Service	
\checkmark	Fetching Service	
	Milestone SSO Provider	
~	Notification Service	
	Processing Server	
\checkmark	Rendering Service	

Cancel Ap

- 5. After installing the plugin, you need to carry out the following steps:
 - a. Open the BriefCam Administrator Console and verify that the **SSOEndpoint** environment setting point to the hostname running the Milestone SSO Provider.
 - b. On the machine running the Milestone SSO Provider, verify that the AuthenticatorAddress key in the MilestoneSSOProvider.exe.config file (located at: C:\Program Files\BriefCam\BriefCam Server\) points to the hostname running the Milestone SSO Provider. For example: http://BCServer:8030/MilestoneSSO/.
 - c. On the machine running the Milestone SSO Provider, verfiy that the BriefCam user that runs the BriefCam services has the necessary permissions to open up a listener, by running the following command in PowerShell as Admin:

netsh http show urlacl

You should see a Reserved URL value and a User value, for example:



Reserved URL : http://qa-inst-02:8030/Milestone550/ User: QA-INST-02\bcuser

d. If such an entry does ot exist, run the following command (replacing the **url** and **user** values with your environment's values):

netsh http add urlacl url=http://BCServer:8030/MilestoneSSO user=bcuser

- e. If you made any changes as part of this step, restart the Milestone SSO provider services on the server and the IIS on the Web services machine.
- 6. In the Services section, start the Milestone SSO Provider service.

-BriefCam ADMIN	SERVI	CES					🖉 🕣 Sga Out
Events	Entitles	v Hasta	~	Status	~		Search Q
≟ _@ User Management →	0	Entity ~	PID	Host	Status	Last Update	
Users & Groups Directories		BI Rule Engine Service	13980	16GPU	Running	2019/08/14 10:34	
🕀 Deployment 🗸 🗸		Face Recognition Serv	13252	16GPU	Running	2019/08/14 10:34	
		Fetching Service	14524	16GPU	Running	2018/08/14 10:34	
GPUs		Millestone SSO Provider	N/A.	16GPU	Stopped	2019/08/14 10:34	= 🕨 ర
Services		Notification Service	9360	16GPU	Running	2019/08/14 10:34	Start



User names are automatically created by the SSO when logging into the Milestone client using the Basic authentication or Windows Authentication method.



To use Windows Authentication with the Milestone Embedded client, the BriefCam VSService windows service must use a domain admin user that is also in the Milestone Administrators role.

Viewing the BriefCam Tab in Milestone

- 1. Launch XProtect Smart Client and log into the Milestone server.
- 2. Once it is up and running, a BriefCam[®] tab will appear in the XProtect client's main application window.
- 3. Click the BriefCam[®] tab and you will be automatically logged into the embedded BriefCam client.





Bookmarks created within BriefCam will not be displayed on the Milestone XProtect Smart Client application.

Hostname Resolution for the Milestone Server

To ensure BriefCam services can correctly resolve the Milestone server's hostname, two entries must be added to the hosts file if the server uses a hostname, such as: "milestone-server-name". These entries should include both the hostname itself and the hostname appended with ".briefcam.local", such as: "milestone-server-name" and "milestone-server-name" name.briefcam.local". Replace "milestone-server-name" with the actual hostname of your Milestone server.

To modify the hosts file:

- 1. Navigate to the hosts file, located at: C:\Windows\System32\drivers\etc\hosts.
- 2. Open the hosts file with a text editor (like Notepad) as an administrator.
- 3. Add the following two lines to the hosts file, replacing 192.168.1.102 with the actual IP address of your Milestone server:
- 192.168.1.102 milestone-server-name
- 192.168.1.102 milestone-server-name.briefcam.local

Remember to substitute the example hostname and IP address with your specific values.

4. Save the hosts file.

5. From the BriefCam Administrator Console's **Camera Management** section, edit the Milestone directory by setting the **Address** field to the full address name: milestone-server-name.briefcam.local.

In the screenshot below, the name of the server is: mil-2024-r1.briefcam.local.





Sending Alerts to Milestone

Alerts can be sent to Milestone's Alarm Manager.



In the BriefCam Administrator Console's **Environment Settings** section, there are three settings relevant for sending alerts outside of BriefCam:

- 1. To send alerts outside of BriefCam, set the Respond.AlertsPublishingEnabled setting to true.
- 2. To send alerts to a VMS, check that the Respond.AlertsPublishingToVMSEnabled setting is set to true.
- 3. To change the polling interval, use the Respond.AlertsPublishingIntervalInMilliseconds setting.



	Uker Management		publish		X Type v	Show settings that have b	een changed
~• €8	Deployment	^	Scope	Туре	Key	Value	Default Value
G	Settings	~	GLO	Common	Respond.AlertsPublishingEnabled	false	false
	Camera Management		GLO	VS-Server	Respond.AlertPublisherAcceptUnsafeC	true	true
	Environment Settings		GLO	VS-Server	Respond.AlertsPublishingToVMSEnabled	true	true
	Localization		GLO	VS-Server	Respond.AlertsPublishingIntervalInMil	1000	1000
si	Activities	^	GLO	Common	AkkaHostConfig	akka : (loggers : ['Br	
89	Dashboards	^	GLO	Common	Administration.SystemEventsPublishin	false	false
			GLO.	Common	Administration SystemEventsPublishin	Critical	Critical

Only alerts produced by the Milestone connected cameras will be sent to the Milestone server.

Sending Analytic Events to Milestone

Milestone can receive Analytic Events from BriefCam.

To send analytic events (instead of alerts), you need to make changes on both the BriefCam and Milestone side:

BriefCam Configuration

- 1. Open the BriefCam.MilestoneIntegration.ini file, which is located at: C:\Program Files\BriefCam\ BriefCam Server\plugins.
- 2. Change the SendAnalyticEvent to true and remove the semicolon (;).
- 3. If you do not want to send data about the Class and Color and Person Attributes, change the **ExtendedTypeField** to **false** and remove the semicolon (;).

The AlertsGrouping parameter lets you set what happens when an object triggers multiple rules:

- true A single alert is sent out for multiple rules.
- false One alert is sent for each rule.

=BriefCam

📔 *C:\	rogram Files\BriefCam\BriefCam Server\plugins\BriefCam.MilestoneIntegration.ini — [×
File Ed	Search View Encoding Language Settings Tools Macro Run Plugins Window ?	?	х
🍙 📑	3 🖻 🗟 🐚 🍰 🕹 🖿 🖿 🔿 🗲 📾 🆢 🔍 🔍 💁 🖬 📜 💭 🤇	A) 🚞	>>
🔡 BriefC	m.MilestoneIntegration.ini 🔀		
25	;DecoderInitChunksCount=5		^
26	;ReconnectionSleepMSec=500		
27	;InputBufferSize=1000		
28	;MaxItemsToTakeFromInputBuffer=20		
29			
30	[Alert]		
31	;Vendor = BriefCam		
32	;Description = BriefCam Respond Alarm		
33	Message = BriefCam Respond Alarm		
34	SendAnalyticEvent = true		
35	;AlertsGrouping = false		
36	;ExtendedTypeField = true		
37			
			~
length : 7	0 lines : 3 Ln : 37 Col : 1 Sel : 0 I 0 Unix (LF) UTF-8-BOM	INS	
			-11

Milestone Configuration

- 1. Within the XProtect Client's BriefCam tab, navigate to RESPOND and create a rule.
- 2. Make a note of the Title and check that the Status is Active (Processing).

BriefCam Protec	ct				REVIEW	RESPOND	.80
ALTETS RULES							
				Status	Schedule		
RedCar	Matarway	03/25/20 11:11 AM	Smart Alerts	Adhe (Proceeding)	Continuous		

- 3. Open the Milestone XProtect Management Client.
- 4. From the **Tools** menu, select **Options**.
- 5. Open the Analytics Events tab, select the Enabled checkbox, and click OK.



vidence Lock	Audio Messages	Privacy settings	Access Control Settings	Analytics Events	Customer Dashboar
VIDENCE LOCK	Abdio Messages	Fillodcy settings	Access Control Settings	Analytics Events	Customer Dashboart
Analytics even	ts				
Enabled					
Port:					
9090					
Security					
Events allow	ed from:				
Al netwo	rk addresses				
	network addresses				
O Specified	Thermore dedicesees.				
Add	fress				
•					
	Import				
	ingrone				

- From the Site Navigation pane, open the Rules and Events folder.
 Right-click on the Analytics Events entry.

- Select Add New.
 Name the analytics even with the exact same name as the rule created in BriefCam (making sure that the spaces and upper/lower cases are all identical).





- 10. Navigate to **Rules and Events > Rules**, right-click and add a new rule.
- 11. To trigger an event from a BriefCam Analytic Event, under **Perform action on event**, select the Analytic Event created in the step above.



a design of the second s	x line and	Billion and a statements			
VMDESKTOP - (25.1v)					
Benics	Celault Goto Preset when PTZ is don	Norse			
License Islomation	Default Play Audio on Request Rule	1			
Site Information	Celevit Record on Bookmark Hule	Description			
Servers di la	Default Record on Request Rule				
Hacording Servere	Cellault Statt Judio Feed Rule				
Denices.	Cells & Start Video Faed Fulle				
'Re Canadae	Carl Service Services (Services, Services, Ser		100000000		
P Hicrophones			Managa Rulo		- 0
C Speakers		- Victive	diam'r	Alternative Controls	
Fieldan		Detotion	nove	Incoment was the	
Cuted			- Description		
Ciest			Active.	2	
Caroupe View Groupe				Ship 1. Type of rule	
Smart Client Profiles			Select the rule i	type you want to create	
D Date and E and			Contract in a	action of develop	
TTI Hand			C Performant	action or a crecuming times	
CO Treast Toble	Select an Event		A		
Reference Profiles	Events				
User defined Events	III C Haldware				
Analytics Events	10 50 Devices				
of Security	IN AN ADDRESS STORE				
Roles	10 C Dber				
& Rasic Users	C Analytics Events		Edit the rules	Proposition (CPU) and entitled tem)	
System Destboard	End Car (Analytica Events)	/	Performan action	tor emet	
	\sim			and the second second	
Current Tasks					
Current Tasks					
Content Tasks					
Correct Tasks Configuration Reports Server Lags					
Corrent Tasks Configuration Reports Service Logis Access Control Transact					
Correct Tasks Configuration Reports Server Logs Access Control Transaction Sources Transaction Sources					

12. Complete the rule with the camera and actions of your choosing. For example, if you want the rule name to appear, from the **Available** columns, select **Rule** and click the icon to move it to the **Selected columns**.

Note that the **Object** and **Type** columns will only appear if the ExtendedTypeField setting in the BriefCam.MilestoneIntegration.ini file is set to true (for more details, see the BriefCam Configuration section above).

The table below shows what is sent from BriefCam to Milestone when a specific Milestone action is used.

Milestone Action	Data Sent from BriefCam to Milestone	Example
Object	Class (Class Data)	Person (Man)
Туре	Color and Person Attributes (if the class is Person) A combination of the following fields: Lower Wear, Upper Wear, Hat, Bag. In the form of FieldName: Value,	Color: Red, Lower Wear: Long, Upper Wear: Long Sleeves, Hat: No, Bag: No
Тад	For Face Recognition (FR) alerts: List name (face name) For License Plate Recognition (LPR) alerts: List name (license plate number) Others: Empty	For FR alerts: Suspects (Frank Smith) For LPR alerts: Restricted Cars (2175834)
Descriptions / Instructions	For FR / LPR alerts: Confidence: [] Others: Empty	Confidence for Suspects1 (Frank Smith) = 81%, Confidence for Suspects2 (Frank Smith) = 37%,
Vendor	BriefCam	BriefCam





- 13. To trigger alarms into the Alarm Manager, navigate to Alarms > Alarm Definitions.
- 14. Right-click and add a new alarm.
- 15. From the **Triggering Event** field, select **Analytics Event** and your desired Analytics Event previously created, followed by the related camera.



Milestone XProtect Management Client 2020 RT			- 🗆 ×
le Edit View Action Taols Help			
199.0			
wilauption + 9 X Numm	Alarr. Definition information		
WINDESKTOP - (20.1a)	n Definitions Alaem defeation		
I Cal Ration	Interview Red Car. Brukle		
The Ste Information	None.	Matanaa Red Car	1
e D Servers			
Recording Servers	Perudiana		
Devices			
The Carrenas	Tegger		
Morophones	Teggering event.	Analytica Events	
C Speakers		BelCe	
de input			
Q Output	Sources	Motorway	Seed
P Ver Grope	Activation period	-	
Swart Olient Profiles	Tree public	Always	-
C Matrix	O Event based	34	Sape.
B Roles	CONTRACTOR OF A	daw.	and the second se
Time Profiles			
Motification Profiles	Operator action required	(march)	
Class-defined Events	100 PM	1 earlie	
Serence Events	Events triggeesd	-	Selid.
E 🚅 Security	Other		
R finic Users	Related carvests:		Select
System Daubdoard	Palated map		-
Current Tasks	Initial alarm owner:		~
Server Logs	keited alarm smoth	1.044	
Access Control			
C EL Trenet	ream: caregory		
and a second sources	Events triggered by alarm:		Select.
3. Horns	Autoretication aliante		
A Alarm Definitions	Alarm assignable to Administrations	8	
Sound Settings			
1000 10021001-001			

Alarm Events and thumbnails will now appear in the Alarm Manager (as shown in the image below).



Creating a VIDEO SYNOPSIS[®] Directly from Milestone

If you installed the enhanced BriefCam XProtect[®] client, you can create a synopsis directly from Milestone.

When you are viewing a video in Milestone (in the Live tab, Playback tab and a floating image), you can click the BriefCam icon at the bottom right of the screen. This will create a new VIDEO SYNOPSIS[®] in BriefCam.





1. Click the BriefCam icon and the following screen will appear.



- 2. Adjust the time frame using the slider button.
- 3. At the top right of the screen, select either to Create a new case or Add to existing case, and then click OK.







You will see a screen, such as the one below.



Non-Masked Video from Milestone

It is now possible to pull non-masked video from the Milestone VMS even if masking was configured in the VMS.

To enable this feature:

- 1. Open the BriefCam.MilestoneIntegration.ini file, which is located at: C:\Program Files\BriefCam\ BriefCam Server\plugins.
- 2. Set the LiftPrivacyMask setting to true and remove the semicolon (;).
- 3. In the BriefCam Administrator Console, restart the VS Server service.

Setting Up Multiple RTSP Bridges

You can configure the Milestone plugin to utilize multiple RTSP bridges for efficient camera stream management. This approach, similar to adding extra lanes to a highway, distributes camera streams across multiple bridges (servers) to improve overall performance and reduce the load on any single bridge. This allows you to manage more cameras effectively.

To set up multiple RTSP bridges:


- 1. Open the BriefCam.MilestoneIntegration.ini file, which is located at: C:\Program Files\BriefCam\ BriefCam Server\plugins.
- 2. Find the **RtspBridge** section. If it is not in the .ini file, add the following to the file:

[RtspBridge]

;DefaultRtspServerCapacity =

;DirectoryRtspBridges =

- 3. Optional. Set the DefaultRtspServerCapacity setting to the default number of cameras that each RTSP bridge can handle. For example, if you know that each bridge can typically handle 10 cameras, set the value to 10. Leave it blank to use the plugin's default value. If you change the default value, remove the semicolon (;) from the beginning of the row.
- 4. Set the DirectoryRtspBridges setting. This setting uses a JSON structure to define the mapping between Milestone VMS addresses and their corresponding RTSP bridges. Remove the semicolon (;) from the beginning of the row.

The structure of the mapping is:

Key - The address of the Milestone VMS.

Value – A list of RTSP bridges associated with the Milestone VMS. Each bridge can optionally have a "Capacity" value defining its camera handling limit. You can configure RTSP bridges for multiple VMSs, by adding additional **MilestoneVMSAddress** sections in the JSON file.

```
    [RtspBridge]
    /DEfaultKispBrverCapecity = 2
    /DEfaultKispBrverCapecity = 2
    /DEfaultKispBrverCapecity for each address
    e.g., { "Mil2023R1": [("BridgeAddress": "172.1.1.2", "Capecity": 1}, ("BridgeAddress": "172.1.1.5")], "mil2023r2": [("BridgeAddress": "172.1.1.3")])
```

Example DirectoryRtspBridges Configurations

Here are example configurations for the DirectoryRtspBridge setting (JSON format):

Single VMS with multiple bridges (default capacity) – example 1:

[RtspBridge] ; Set the default capacity for each bridge (optional) ; DefaultRtspServerCapacity= (recommended channel limit per bridge) DirectoryRtspBridges = { "MilestoneVMSAddress": [{"BridgeAddress": "BridgeIPAddress1"}, {"BridgeAddress": "BridgeIPAddress2"}, {"BridgeAddress": "BridgeIPAddress2"}, {"BridgeAddress": "BridgeIPAddress5"}, {"BridgeAddress": "BridgeIPAddress5"}, {"BridgeAddress": "BridgeIPAddress5"}, {"BridgeAddress": "BridgeIPAddress5"}] }

- This example shows how to configure the plugin for a single Milestone VMS with multiple RTSP bridges. We'll
 assume each bridge can handle the recommended number of cameras.
- The configuration ensures all available bridges are used to distribute the total number of channels from the VMS for
 efficient management.
- If DefaultRtspServerCapacity is not defined, the plugin will use its internal default for bridge capacity, which is 100.
- The DirectoryRtspBridges section assigns all bridges to the single VMS address, ensuring all available resources are utilized.

Single VMS with multiple bridges (default capacity) – example 2:

DirectoryRtspBridges = { "MilestoneVMSAddress": [# Single VMS entry {"BridgeAddress": "BridgeIPAddress1"}, {"BridgeAddress": "BridgeIPAddress2"}, {"BridgeAddress": "BridgeIPAddress3"}, {"BridgeAddress": "BridgeIPAddress4"}, {"BridgeAddress": "BridgeIPAddress5"}, {"BridgeAddress": "BridgeIPAddress6"}], "DefaultRtspServerCapacity": 240 # Default capacity for each bridge }

- This configuration assumes all 15 recorders/archivers are working under a single Milestone VMS server.
- We have 6 bridges, and each bridge can handle approximately 240 channels (according to Milestone).
- Therefore, all 6 bridges are assigned to the single "MilestoneVMSAddress" entry.



- This configuration ensures all 1,200 channels can be distributed across the available bridges for efficient management.
- By setting the DefaultRtspServerCapacity to 240, the plugin will prioritize assigning a maximum of 240 channels to each bridge during camera distribution. This helps ensure a balanced workload across the bridges and avoids overloading any single bridge.

Single VMS with multiple bridges (custom capacity):

DirectoryRtspBridges = {"MilestoneVMSAddress": [{"BridgeAddress": "BridgeIPAddress1", "Capacity": 1 }, {"BridgeAddress": "BridgeIPAddress2", "Capacity": 2 }, {"BridgeAddress": "BridgeIPAddress3", "Capacity": 3 }]}

In this scenario, you have a single VMS with three bridges with custom capacities: "BridgeIPAddress1" can handle 1 camera, "BridgeIPAddress2" can handle 2, and "BridgeIPAddress3" can handle 3 cameras.

Multiple VMSs with multiple bridges (default capacity):

DirectoryRtspBridges = {"MilestoneVMSAddress": [{"BridgeAddress": "BridgeIPAddress1" }, {"BridgeAddress": "BridgeIPAddress2" }, {"BridgeAddress": "BridgeIPAddress3" }], "MilestoneVMSAddress1": [{"BridgeAddress": "BridgeIPAddress3" }], "MilestoneVMSAddress1": [{"BridgeAddress": "BridgeIPAddress5" }, {"BridgeAddress5" }, {"BridgeIPAddress6" }]}

This scenario demonstrates multiple Milestone VMS servers. The first VMS ("MilestoneVMSAddress") has three defaultcapacity bridges, while the second VMS ("MilestoneVMSAddress1") has three bridges with unspecified capacities (assuming default values).

Multiple VMSs with multiple bridges (custom capacity):

DirectoryRtspBridges = {"MilestoneVMSAddress": [{"BridgeAddress": "BridgeIPAddress1", "Capacity": 1 }, {"BridgeAddress": "BridgeIPAddress2", "Capacity": 2 }, {"BridgeAddress": "BridgeIPAddress3", "Capacity": 3 }], "MilestoneVMSAddress1": [{"BridgeAddress": "BridgeIPAddress5", "Capacity": 2 }, {"BridgeAddress4", "Capacity": 1 }, {"BridgeAddress": "BridgeIPAddress5", "Capacity": 2 }, {"BridgeAddress6", "Capacity": 3 }]}

Camera Distribution

This plugin uses the DirectoryRtspBridges JSON data to distribute cameras to available RTSP bridges. It takes into account bridge capacities and sorts cameras by display names (or IDs if names are identical).

For example, for one Milestone VMS with 100 cameras, 10 RTSP bridges and a bridge default capacity of 10, 10 cameras will be mapped for each RTSP bridge.

Bridge Selection Priority

Bridges defined in the .ini file's DirectoryRtspBridges section have priority over those configured through the plugin's Directory Settings.

Additionally, any RTSP bridge defined in either the .ini file or the Directory Settings will be added to the pool of bridges used by the plugin. This means that even if a bridge is not included in the DirectoryRtspBridges JSON list, it can still be used for camera distribution if capacity allows. For example, if you have a bridge defined only in the Directory Settings and it has available capacity, the plugin might assign cameras to it.

Known Limitations

- The BriefCam Server stops extracting new objects while Milestone archives data. It restarts automatically, but there is a temporary delay of a few minutes.
- In Milestone Embedded integrations, a rule with a comma (,) in the name is sent as two different alerts (identical) from two different rules.
- On the Milestone client, a white screen sometime appears instead of the BriefCam tab. To resolve this issue, run MilestoneSSOProvider under a domain user that is recognized by Milestone.
- In Milestone 2023 R2 integrations, when installing or upgrading, recordings are sometimes not fetched for high resolution cameras. . To solve this issue, copy all files and directories from <BC server>\MilestoneSDK\ and paste them (with override) into the <BC server> directory.
- · After upgrading the BriefCamMilestonePlugin, a white screen appears for a few seconds in the Milestone 2020 R3 -



XProtect Smart Client. To resolve this issue, wait a few seconds or move to another tab and then back to the BriefCam tab.

• In Milestone 2020 R3 integrations, when retrying after fetching failed, an error similar to the following appears in the FetchingService log (but does not have any effect on the user):

ERROR - Removed old \\19AIO562\BriefCam\ServerData\VideoData\VideoFiles\FetchedFiles

\22\05-05-2021 12_05_00\Project.scp [In: BriefCam.MilestoneIntegration.MipsVideoExporter. ExportFolderClea n]

- The Milestone Embedded SSO Authentication fails on distributed environments. To solve this issue:
 - 1. In the BriefCam Administrator Console's **SSOEndpoint** environment setting, change localhost to the hostname running the Milestone SSO Provider.
 - 2. On the machine running the Milestone SSO Provider, give the BriefCam user that runs the BriefCam services a specific permission to open up a listener, by running the following command in PowerShell as Admin (replace the url and user values with your environment's values):
 - netsh http add urlacl url=http://BCServer:8030/MilestoneSSO user=bcuser
 - 3. Restart the Milestone SSO provider services on the server and the IIS on the Web services machine.

See also: Troubleshooting - Milestone Issues

NX (Network Optix) Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
NX (Network Optix)	NX Witness VMS	5.0.0.35270	6.4 Hot Fix 1	Integration for on-demand and real- time (L2)	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Directory Connection

The NX Integration plugin uses a URI to connect to the VMS. The syntax of the URI is:

http://{vms-ip-address/hostname}:{vms-port}

For example: http://172.1.1.1:7001 or http://nxwitness:7001





Add Directory		×
Fill in the fields below		
Védeo Informético é		
RiefCam Ny Integration	-	
Directory Name *		
NxWitness		
Address *		
http://172.1.1.1:7001		
User Name *		
admin		
Password		
	\odot	
Cancel		Add





The user's credentials for the Directory connection are setup in the Nx Witness Client's **System Administration** in the **Users** panel.

The user must have at least an Administrator role.

8	V System Administration - Nx Witness Client											х
										Routing Management		
	~											
	ų		rcn use								All users	
		Lo	gin ≞	Name						Role		
		ad								Owner		

The NX Integration plugin uses a digest authentication, which needs to be set up for the user that will be used for BriefCam integration.



System Administration - Nx Witness O	lient				?	×
				iting Management		
Q Search users					All users	
🖂 Login 🗧 Name				Pole		
admin New User Nx W	itness Client			? ×		
User Information						
	h an desire					
Login	bcadmin					
	bcadmin					
	bcadmin@briefcam.co	m				
	•••••			600D 👡		
	•••••			~		
	Live Viewer 🗸	Edit Roles				
C Enabled	: Allow dispet outboati	estion for this upor	ок	Cancel		
	Allow digest addreno	cation for this user				
New User Edit Roles		0	LDAP Settings			
			ОК	Apply	Cancel	

Once the digest authentication is setup, this user's credentials can be used for setting up the directory in the BriefCam Server.

Settings File

There is one setting in the BriefCam.NxIntegration.ini file.

[Fetching]

;SecondsFromNowNotRecordedYet = 300

This setting is used when the VMS has not yet recorded the newest footage to the archive. This setting prevents the user from accessing videos that are too new and returns NoRecordings.

To use this setting, remove the semicolon from the beginning of the row. If the semicolon is not removed, the plugin will always fetch the newest recordings.

Known Limitations

· Bounding boxes when playing the original video are not supported.

Pelco Integration





Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Pelco	VideoXPert	3.24	2024 R2 HF4 (including Classic and Next-Gen engine)	Client integration (L3)	Yes
Pelco	VideoXPert	3.19	2023 M1 (including Classic and Next-Gen engine)	Client integration (L3)	Yes

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Pelco Plugins

There are two Pelco plugins – One to install the Pelco integration and one to install the Embedded Client. If you want BriefCam to be embedded in Pelco, first run the BriefCam Pelco plugin and then run the BriefCam Pelco Embedded plugin.

Pelco License

You will need a Pelco license. To request a license, contact Pelco and use the following product code: **INT-BRIEFCAM-M1**. This license needs to be activated from Pelco VxToolbox, in the **Licensing** tab.

Configuring the Integration

When the Pelco plugin is installed, you'll have a BriefCam.Pelco.ini configuration file, which by default is located at: C:\Program Files\BriefCam\BriefCam Server\plugins.

```
[Connection]
;Port = 443
;UseSSL = true
[Live]
;LiveDelayMSec = 0
```

This file includes the following parameters:

- Port: The port number where the HTTPS accepts connections.
- UseSSL: When this parameter is set set to true, which is the default, the integration uses HTTPS.
- LiveDelayMSec: Sets a delay for live streams if the clocks of the VMS and BriefCam are out of sync and the live stream times are different than the BriefCam time.



COLUMN STR



.....

Sending Alerts to Pelco

To receive alerts in the VMS, set the PushAlertsServiceEnabled environment setting to true.

(second test in x) & second test	EX Defective in 196.		×	VaOpsCenter Valles Workshop
The User Ver			Des Mark	petp-3-24 alone
Event Vewer			×	Pipe dit to all part land to the
14.0		Sorthy: Time	Cocordig Indiagram According	+ Vent
Ever Source The	BrinCase Alarm Bilastion Julis Adventinger		need at a second second	+ forset (BARH)(Papel)
	BriefCare Alem Situation Auto Editorentingeri		MARCAN AND SURION	+ Her Cl 212 Dr
From th	BriefCam Alarm Situation Auto Admonderged			III P Canese - MAC1_APS111EP - Volum
1160004 EE 11150004 EE 1200 PM () 550 PM ()				
Diversion with status	BriefCeen Alarm Bituation Auto Addrowindged		Anti-Astrowedged	
11.PTogrees Admonweaged	BriefCare Alarm Bitastion Auto Actorevicespee		• Evert Source	
Severty	BriefCase Alarm Bilastion Just Adversionger			
1400 1 2 1 0 0 2	BriefCase Alarm Situation Auto Adversion(get)			
C ATOMS +	BriefCase Alarm Situation Auto fully codesigned			
Only show user related actions				
ton Extend				
Bindfair Ann Bhallan -	BrinCare Alarm Bilastion Auto Adventionaged			
	BrinCase Alarm Bilastion Auto Advestinged			
	BriefCase Alarm Bitaation Auto Autorenietigen)			
			and the second sec	

Configuring the Embedded Integration

After installing the BriefCam Pelco Embedded plugin:

- 1. Open the PelcoEmbeddedViewer.dll.config file. By default, the file is located at: C:\ProgramData\Pelco\ OpsCenter\Plugins\BriefCam\BriefCam Embedded Viewer.
- 2. Change the value of the BriefCamAddress key to the IP/hostname of BriefCam.



After a successful installation and configuration, the BriefCam plugin should appear in the VXOpsCenter's **Plugins** tab (as shown in the image below).





Troubleshooting

If you encounter video fetching timeouts, increase the **Fetching.TimeoutInSeconds** environment setting. The default value is 120 seconds, but sometimes this is not enough for the VMS to prepare the files needed. Try to increase the timeout to 600 seconds. If this does not work, try to increase the timeout to 3600 seconds.

Qognify Nicevision Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Qognify	NiceVision Qognify SVR	3.2 UP2	2024 R2 HF4	Integration for on-demand and real- time (L2)	Yes
Qognify	NiceVision Qognify SVR	3.2 UP2	2023 M1 (Next-Gen engine)	Integration for on-demand and real- time (L2)	No

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Ports Required

The following ports should be available when installing the plugin:





Port

80, 500, 2001, 2011, and 50000

VMS SDK

Prior to plugin installation, make sure you have the required Qognify SDK installed on the BriefCam Server.

- For NiceVision 3.1 you need PlayerComponent Package 12.1.0.147.exe.
- For NiceVision 3.2 you need PlayerComponent Package_12.2.0.133.exe.
- For NiceVision 3.2 UP2 you need PlayerComponent Package_12.2.2.193.exe.

The SDK is required to be installed on every machine on which any of the following services is installed: BriefCam Server service, Processing Server service, and Alert Processing Server service.

Integration – Plugin Installation

When installing Qognify NiceVision 3.2, you will be asked to provide the path to the SDK in the Player component path field.





Post Installation Script

For new installations, after installing the **VisionHub** VMS plugin you need to run a script that gives the BriefCam user permissions to access the relevant files.

In all places where the plugin is installed:

- 1. Open PowerShell as administrator.
- 2. Navigate to the following folder: cd {where briefcam server is installed}/tools/post_plugin_installation
- 3. Run the following command: .\set_permissions_for_plugins.ps1

Silent Installation of NiceVision and VisionHub Plugins

To run a silent installation of the NiceVision Plugin, use the following command line:

{ NiceVision Installer file name} /qn APPDIR="C:\Program Files\BriefCam\BriefCam\BriefCam Server\" SDK_PATH="{Path to the

NiceVision SDK Player component}"

-BriefCam



{ VisionHub Installer file name} /qn APPDIR="C:\Program Files\BriefCam\BriefCam Server\" SDK_PATH="C:\Users\Public\Qog nify\Player"

Known Limitations

- Support for the H.265 format is done per request. If you want to use the H.265 format with this VMS, please contact BriefCam's support.
- For Qognify VisionHub integrations, bounding boxes are not supported.

Qognify Ocularis and Qognify VMS Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Qognify	Ocularis	6.1 SP1	2024 R2 HF4 (including Classic and Next-Gen engine)	Real time alerts integration (L2a) Note that An L3 integration was created by the VMS partner.	Yes. Ocularis 6.1 hotfix SP1 patch is required to support H.265.
Qognify	Qognify VMS	7.4	2024 R2 HF4 (including Classic and Next-Gen engine)	L2a	Yes. Ocularis 6.1 hotfix SP1 patch is required to support H.265.

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

For L2 integrations download: BriefCamOnSSISeeTecPlugin_<version number>.exe.

For L2a integrations, also download: BriefCamQognifySaiPlugin_<version number>.exe

Ports Required

The following ports should be available when installing the plugin:

Port #	
--------	--

7676, 9100, and 62000





Integration Plugin Installation

For both QVMS and Ocularis integrations

- 1. Install: BriefCamOnSSISeeTecPlugin_<version number>.exe.
- 2. If you want L2a integration, you also need to install: BriefCamQognifySaiPlugin_<version number>.exe on the VMS machine.



SGS and Transcoding modules should be installed on the VMS in order for BriefCam to work properly. For more information, please contact your system administrator.

After installing the integration:

- Open the BriefCam.SeeTecIntegration.ini file, which by default is located at: C:\Program Files\ BriefCam\BriefCam Server\plugins.
- 2. Change the StartupFrameSkipCount parameter to 10.



Sending Alerts to Ocularis and Qognify VMS

To configure the integration and configure QAI events from BriefCam to Ocularis and Qognify VMS follow the sections below.

Prerequisites

All communications between QVMS, the SAI plugin and BriefCam are done with the hostname. **An IP address will not work.** Ensure that the prerequisite steps detailed below are done correctly.

Prerequisites in BriefCam

- 1. On the BriefCam Server machine, open: C:\Windows\System32\drivers\etc\hosts.
- 2. Add the host of the Qognify VMS instance to the file.
- 3. Log into BriefCam Administrator Console.
- 4. Navigate to the Environment Settings section.
- 5. Set the Respond.AlertsPublishingEnabled environment setting to true.
- 6. Set the **Respond.ExternalUrlUploadAlerts** environment setting to the URL where the SAI plugin is listening. For example: http://< QognifyVMS_server_hostname>:7073/Events/.

The URL can also be changed in the Briefcam.QognifySai.dll.config file. In addition, there can be multiple URLs separated by semicolons.

7. If you make changes to settings in the BriefCam Administrator Console, you need to restart or start the VSServer service.

-=BriefCam



- 1. On the Qognify VMS Server machine, open: C:\Windows\System32\drivers\etc\hosts.
- 2. Add the host of the BriefCam Server instance to the file.

Installation and Setup of SAI Plugin

- 1. Open the Qognify VMS server and download the BriefCamQognifySaiPlugin.exe file.
- 2. Right-click on the BriefCamQognifySaiPlugin.exe file and run as an administrator.
- 3. Open the VMS VA Administration Tool.
- 4. Right-click on the VAConfig root node.

		- x
Configuration	Configuration —	
AnalyticsPipeline Motion Detection Module 0 Q Motion Detection Module 1 Q AVExport AVExport SGS	Module name Module ID Service ID -1 Type	Core server IP Core server port
GIN SGS Module 3	Module IP Module port	Connection test Streaming port
		<u> </u>

5. Select Add new module and then Analytics interface.





- 6. The configuration fields will be populated for you. Check that in the VCA plugin field, the BriefCam plugin is selected.
- 7. Click the Save button.



- 8. Open the QVMS Client with Administrator.
- 9. On the left-hand side, navigate to the **Configuration Mode**.
- 10. On the right-hand side, open the **Server** menu.
- 11. Select the BriefCam SAI module.
- 12. Set the Username and Password for BriefCam.

Note that the user must be a Basic User (and not an administrator user) and have access to the rules that need to be sent to QVMS.

13. Set the Hostname of the BriefCam instance. (Remember that IP addresses will not work.)

Note that the value in the **Port** field is not used and should be left as 0.



Server configuration: Brieft			Company 0.111
	General .		Company (administration)
Sec. 4	General		
	Tank	Implan Set Module	
	Server	17211.201408471	
	Nelson module	Oundrian T	
	Details		
	Warufschurer	Breturn	
	104	Braham Miglioph	
	All version	Pan .	
	Administra		
	2 to advertise		0 0 / 1 A
	User name	M.	Company 0 FT #
	Parameter 1		m) and prove and the second
	External anvice		and Aliantia
	2 the estimate service		E) Lapers
	Host (P address or same)	14-07-147	El mete
	Parts .	8 ÷	Chamber of the second
		lane est b	C marphi
			- Parson
			III Video with
			and Linear olds comm
			D terrer
			B. Setter
			Second A 11 A
		Const Auto Inc	E DeviceManager, geno 1-2
			E Distante geno 14
Search			Di Brattan LU Mukar
Kana	• 1.0	Description Figure Section 1995 Name Section 1995	E 101 mid.de 1 O/M0 1 0
			 Distance of the state of the st
			E De Martines Determines Mindade 1 (2)/MC

- 14. Click the **Save** button.
- 15. Navigate to the Other Hardware menu.

Note that under **Other Hardware**, all cameras from BriefCam directories will be added as channels.

											Company	
		Ceneral					 	_			 Company Edmini 	er word
-	General	Canad										
		Nane	BriefCare LA Ma	dale								
_		Lanan.	172/114040411									
22		faile-ar nobula	to no us bio-	÷								
		Datab										
		Manufacturer	Brieften									
		Tex.	Briefsen S-R plug									
		API remiers	7.1.1									
		Authentication										
		2 Verschertigter									10.00	
		Der rame	hed								Company	0 11 0
		Innert	10.00 M								A Ceneral	
		Internal process									E Other hardware	
		When external service									E Gvent Interfaces	
		Post IP address or served.	april ord			_					L Uners	
		Pp.1	2.0								La Graups	
					Besterl model						#1 Profiles	
											🖸 Time managem	
											🟥 Company calen	fars.
											BB Alarma	
											🔝 Layers	
											E Mapo	
											(The bookson	
											Barban Dyber 1	Long (DEC 11
			Canvel	feety	law.						🖬 💣 Brisham, Dybli, 1	Jung (Dec 41
											 # Status, Ovhil, 13 	Ling Jine (B
	earth										 A sintan pyners 	Carries 2 - 40
- H	Vers			Description		Is used in the following contents	No.		here		E d'anistan, constru	Camera, J, Ma
	1.200			and party set					1944	_		

16. Select a Camera channel.



Configuration of other 1			E Campany 0 111
-	General		Company (constant)
Course of Courses	E Actional		
Children Terra	General		
Unavailable Autor (1)	form	Barkan, DMIN, Garwa, L., Anapa	
*	Video analysis module:	Braffan Sel Molve #	
	Carreno		
	Take cashaton	1000 ¥	
	Frame and for analysis (bpd)	B 2	
	Authentication		
		The mobile actings for authentication the from same a	0.07.0
	lise rame		Company @ * 1 #
	Password		A Cameras
	External services		👹 Other hardware
	Use external service	Darbar area	E Event Interfaces
	Not 17 address or name)		🚊 Users
	Paris		All Groups
	Ceneric parameters		git Profiles
	5 m	Table 1	② Time management
			Company calendars
			D4 Alarma
			🗔 Layers
			22 Mape
			Other bardware @ * 2 a
			Internet and a state of the
		Genot Avely See	🖬 💣 Stantana, DVMD, 7.2, Song, DNC 4
			E Status DML 71 Son DML
- Indexed		A used in the following contacts	# Siden.there.t
Name	104	beciptor III III IIII	 # # Helen, DMSR, General, J. M

17. From the Camera Channel menu, additional mapping can be done for the events that are received by BriefCam.

Configuring the Integration

When the SAI plugin is installed, you'll have a Briefcam.QognifySai.dll.config file, which by default is located in the SAI installation directory.

```
<?xml version="1.0" encoding="utf-8"?>

<configuration>
</appSettings>
</add key="listeningUrl" value="<u>http://*:7073/Events/</u>" />
</add key="connectionMonitoringInterval" value="60000" />
</add key="camerasMonitoringInterval" value="60000" />
</add key="httpRequestTimeout" value="30000" />
</appSettings>
<//configuration>
```

This file has the following parameters:

- listeningUrl The URL that listens for incoming BriefCam events, which by default is set to listen to all addresses.
- connectionMonitoringInterval The interval in ms between polling KeepAlive requests. The default is 60000 ms.
- camerasMonitoringInterval The interval in ms between fetching cameras list. The default is 60000 ms.
- httpRequestTimeout The timeout for the HTTP client to send a request to BOA (BriefCam Open API). The default is 30000 ms.

Filtering Camera Channels

When there is a single directory in BriefCam, you can filter out the needed cameras. This is done with the VMSCameraList.json file. The file is located at:

<QognifyVMSInstallationDirectory>\VersatileApplications64\VcaPlugin\. The VMSCameraList.json file contains the mapping between BriefCam directories and their cameras and other hardware channels that are created in the Qognify VMS. Cameras can be filtered by directory or by directory and camera name.

To add a directory to the file, use the following syntax:



"directory": "<Directory Name>",

"cameras":[]

}

 \cdot To add a directory with specific cameras to the file, use the following syntax:

{

```
"directory": "<Directory Name>",
```

```
"cameras":["<CameraName1>", "<CameraName2>",]
```

}

When there are more directories in BriefCam than are needed in QVMS, you have to filter out all the cameras from the needed directory. Cameras have to be filtered by directory and camera name. Multiple directories can be included as a list in the VMSCameraList.json file.

To add a directory with all cameras from it to the file, use the following syntax:

{

```
"directory": "<Directory Name>",
```

```
"cameras":["<CameraName1>", "<CameraName2>",<.....>,]
```

}

To add multiple directories with all cameras from them to the file, use the following syntax:

```
{
```

```
"directory": "<Directory Name>",
```

```
"cameras":["<CameraName1>", "<CameraName2>",]
```

},

```
{
```

```
"directory": "<Directory Name2>",
```

```
"cameras":["<CameraName3>", "<CameraName4>",]
```

}

There is an example file in the Plugin installation directory called VmsCameraListSample.json. The following is an example configuration:



```
[
  {
    "directory": "qvms7.4",
    "cameras": [ "Axis Kitchen" ]
  },
  {
    "directory": "Qvms7.2|",
    "cameras": []
  }
]
```

Plugin Installation Directory

The plugin installs the files to the following location: <QognifyVMSInstallationDirectory> VersatileApplications64\VcaPlugin.

For example: C:\Program Files\Qognify\VMS\VersatileApplications64\VcaPlugin

SAI Plugin Logs

The log files are located in the following locations:

- <QognifyVMSInstallationDirectory>\VersatileApplications64\VcaPlugin\logs\ Briefcam.QognifySai.log
- <QognifyVMSInstallationDirectory>\log\VA_VCAPI_<ID>.log

Known Limitations

- The Restart Module button in QVMS does not work. If the SAI plugin needs restarting use the VMS Service Manager. The service that hosts the SAI plugin is the VA service.
- All communications between QVMS, the SAI plugin and BriefCam are done with the hostname. An IP address will
 not work.
- · Bounding boxes when playing the original video are not supported.
- The OnSSI hotfix SP1 patch (for OnSSI 6.1) is required to support H.265.
- In Ocularis integrations, rules may get stuck in Recovering status due to slow loading time. To resolve this issue, in the VideoNative.ini file (located at C:\Program Files\BriefCam\BriefCam Server), change both the RtspConnectionTimeout and the RtspGetNextTimeout parameters to 60000 and remove the semicolons from the beginning of these rows.

-BriefCam



File Edit Search View Encoding Language Settings Tools Macro
Image: Section Timeout 60000 RtspGetNextTimeout 60000
Image: Solution of the solution of
VideoNative.ini X
1 2 [Rtsp] 3 RtspConnectionTimeout = 60000 4 RtspGetNextTimeout = 60000
2 [Rtsp] 3 RtspConnectionTimeout = 60000 4 RtspGetNextTimeout = 60000
3 RtspConnectionTimeout = 60000 4 RtspGetNextTimeout = 60000
4 RtspGetNextTimeout = 60000
6 [FrMpeg]
; DecoderSuriaces = -1
8 ;LogLevel = 8
9 ;LiveDecoderBufferSizeMB = 50

Salient Integration

Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Salient	CompleteView Pro	5.5	6.2	Integration for on-demand and real- time (L2)	No

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Salient Integration Modes

With Salient integrations, videos streams can be pulled directly from the cameras or from Salient's RTSP server.

Pull streams directly from the cameras: Salient provides a .json file with all the cameras and their links to the RTSP. In this mode, network access to the cameras is needed.

Pull streams from Salient's RTSP server: The customer needs to install Salient's RTSP Server (a separate component) and set the following connection details in the BriefCam.SalientIntegration.ini file:

;UseRtspServer=true





;RtspPort=[port]

*C:\Program Files\BriefCam\BriefCam Server\plugins\BriefCam.SalientIntegration.ini - Notepad++ [Administrator]

🔡 Brief (Cam.SalientIntegration.ini 🔀
1	[Fetching]
2	;SecondsFromNowNotRecordedYet = 300
3	L
4	[General]
5	;DefaultProtocol=http
6	;DefaultPort=4502
7	L
8	E [Live]
9	;CameraToRtspMappingFile = "\\SamplePath\CameraToRtspMappingFile.json"
10	:LiveDelavMSec=500
11	UseRtspServer=true
12	RtspServer=
13	RtspPort=554
14	75kips N first frames from live stream (in order to ensure a keyframe is received,
15	;LiveStreamWarmupFrameCount=20

Port Configuration

When configuring the Salient directory using the BriefCam Administrator Console, it is important to specify the VMS HTTP port number. The port number can be found on the Salient CompleteView Server configuration application, as shown below:



To configure the directory in the BriefCam Administrator Console, set up the Server IP followed by the port number in the following format: http://IP_Address:Port#.



CAMERA MANAGEMENT		
licenses: 10000 Remaining: 9986 Activat	ed: Add Directory	×
Search Directories Q	Fill in the fields below	
+ M14 (2)	Video Integration * Salient Integration	*
	Directory Name * North corridor	
	Address * http://10.10.123.144;1023	
	User Name *	
	Password	
	Cancel	Add
Add Directory		

Known Limitations

- In Salient 5.2 integrations, in some environments, RTSP streams take longer than expected to initialize. This delay
 causes new RESPOND tasks appear in Recovery mode, miss objects and fail due to timeout. To avoid failures,
 increase the BriefCam timeout configuration by modifying the Live.MaxGetLiveImageRetries environment setting.
- Salient's RTSP stream does not support timestamps.
 - This can lead to object clips that play in fast forward in some configurations.
 - This can lead to a small offset when playing the original video playback. To correct this offset, consider adding a constant offset to BriefCam's playback request by editing the LiveDelayMSec parameter in the BriefCam.SalientIntegration.ini file.
- In Salient integrations, motion detection does not work when the clips are shorter than 5 seconds long. Some objects will not be detected if the clips are shorter than 5 seconds. To solve this, configure the cameras to either disable motion detection or create clips that are always longer than 5 seconds.
- Support for the H.265 format is done per request. If you want to use the H.265 format with this VMS, please contact BriefCam's support.

Teleste Integration





Integration Summary

VMS Partner	Product	Version	Last Tested BriefCam Version	Integration Level	H.265 Support
Teleste	Teleste	5	5.4.1 UP1	Forensics only integration (L1)	No



The RESPOND module is currently not supported for this VMS.

The most up-to-date list of supported VMSs can be found here: https://www.briefcam.com/partners/supported-vms/.

Before beginning the installation of the VMS plugin, make sure that BriefCam is installed. For a reminder of the order of installation, click here.

To download the VMS plugin:

- 1. Go to http://briefcam.com/installation-downloads/.
- 2. From the Select a Product drop-down list, select VMS Plugins.
- 3. From the Select a Version drop-down list, select the BriefCam version you are using.

Teleste API Token Setup

An API token (software key) should be provided by Teleste to allow integration with the VMS. This token should be manually added into the BriefCam Teleste plugin ini file's API Token section. The ini file is located on the BriefCam Server at: ...\plugins\BriefCam.TelesteIntegration.ini.

Known Limitations

- In Teleste integrations, although the processing is reported to be completed successfully, occasional frames may be dropped and indicated in the logs.
- The FFmpeg tool cannot process Teleste V5 video files using the cuvid hardware acceleration method, which is BriefCam's default method. To solve this use, change the method in the ProcessingServer.ini file's HwAcceleratedDecoder parameter. Remove the semicolon and change the value to either:
 - NoAccel for no hardware acceleration. Note that disabling the hardware decoding is not advisable since it will impact performance.
 - Cuda for CUDA hardware acceleration

```
C\\Program Files\BriefCam\BriefCam Server\ProcessingServer.ini - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window
G 😖 🖶 🗞 🕼 🕹 🕹 👘 🌔 🗩 d | 📾 🦕 🔍 🔍 🖫 🔜 1 🌉 🖼 🖉 💷 👁 🔍 🖽 🖽 🕬
ProcessingServer.ini 🖾
     [General]
      ;DBType = Proxy
      ;VideoArchiveMode = VMSFetchOnDemand
      MaxTaskExecutions = 15
  4
      ;CheckForNewTaskInSec = 5
      ;;FFMpeg Decoder: 0CB279A5-F203-4096-929E-975CBB8A71CD (default), DirectShow Decoder:
      E196D49F-D384-46A9-9D76-4CD0326930E8
      ;VideoDecoderId = 0CB279A5-F203-4096-929E-975CBB8A71CD
      ;AllowHwAcceleratedDecoder = true
       ;;;HwAcceleratedDecoder values are [ NoAccel | Cuda | Cuvid | CuvidNoHWFallback ]
    ;HwAcceleratedDecoder = Cuvid
```



• Support for the H.265 format is done per request. If you want to use the H.265 format with this VMS, please contact BriefCam's support.

Proprietary Format Support

There are a number of plugins that can be used to process files with a proprietary format: Dahua, HIK, Infodraw and Timespace.

These plugins are available for the BriefCam Investigator, Investigator for Teams and Protect versions.

When installing any of these plugins, the plugin needs to be installed on every machine on which the BriefCam Server/ Processing Server is installed.

The path that you select to install the plugin should be the same directory as the BriefCam Server directory. By default, it is set to C:\Program Files\BriefCam\BriefCam Server\.

Dahua Integration

In BriefCam, to process files created by the Dahua recorder, such as .DAV files, install BriefCam's Dahua plugin.

Post Plugin Installation

1. Enable the DAV decoder in the RenderingService.ini file's SupportedDecoders section on the Server directory, by removing the semicolon character from the ;BriefCam DAV Decoder row:

RenderingService - Notepad	_		\times
File Edit Format View Help			
			^
[SupportedDecoders]			
;entire section must be in prod			
;BriefCam HB Decoder = 41C3EB5C-B217-4837-AE9A-734B6EA9988E			
;BriefCam NVF Decoder = 12822F5F-EA45-44B3-A814-590BF60C61D3	1		
;BriefCam Dvt Decoder = 063B2341-F4DB-4BB8-BABE-BF1DD9B82D71	Ļ		
;BriefCam PQZ Decoder = A1C398C2-D1A9-46B7-BC82-0D46FCF7FF34	ļ.		
;G64 Decoder for Genetec versions < 5.7			
;BriefCam G64 Decoder = 8ADC1460-2D0D-4CAD-AB78-DAF3F013C3A6	j.		
;G64x Decoder for Genetec version == 5.7			
;BriefCam Genetec G64x Decoder = 627654c5-8aed-4f92-8745-a36	f8d46d	le28	
BriefCam FFMpeg Decoder = 0CB279A5-F203-4096-929E-975CBB8A71	CD		
;BriefCam InfoDraw Decoder = 5ae7da91-25d6-4e0f-be32-9b415d3	89b4c		
BriefCam DirectShow Decoder = E196D49F-D384-46A9-9D76-4CD032	6930E8	3	
BriefCam DirectShow Decoder32 = 32B7FF55-B4BE-464B-B774-D8C4	996D06	532	
:BriefCam HTK Decoder = 29955860-26EA-4B2D-BE57-0AADD836BBE8			
;BriefCam DAV Decoder = BB47C1F7-5E83-4555-A538-C8A904155F5E			
;BrietCam AVE Decoder = SUBUEIUE-BAS3-4205-93/F-4ESBDD4F/DD5			
;BriefCam XPEG Decoder = A637C67D-0D3D-4A64-B143-00C6F857405	A		

2. Restart the Rendering service.

Known Limitations

When using the Dahua decoder, the Rendering service fails to verify .DAV files that have Chinese characters in the file name. This is because the decoder only supports ANSI format, which requires that the file name use the same language as the operating system. To solve this issue, if your operating system is in English, for example, change the file names to English as well.





HIK Integration

In BriefCam, to process files created by the HIK recorder, install BriefCam's HIK plugin.

Post Plugin Installation

- 1. Enable the HIK decoder in the RenderingService.ini file's SupportedDecoders section on the Server directory, by removing the semicolon character from the ;BriefCam HIK Decoder row.
- 2. Restart the Rendering service.

Infodraw Integration

BriefCam supports the Infodraw DVR exported file format (MP4 and .FLV file formats).

Post Plugin Installation

- 1. Enable the Infodraw decoder in the RenderingService.ini file's SupportedDecoders section on the Server directory, by removing the semicolon character from the ;BriefCam Infodraw Decoder row.
- If the InfoDraw files are encrypted, specify the password in the BriefCam.InfoDrawDecoder.ini file's XorKeyword parameter. This file is located by default at: C:\Program Files\BriefCam\BriefCam\BriefCam Server\ plugins.

🧾 В	riefCa	m.InfoDra	wDeco	der.ini - Notepad	ł	_	\times
File	Edit	Format	View	Help			
[Ini XorK	t] eywo	ord = "					^

3. Restart the Rendering service.

Timespace X300 Integration

BriefCam supports the Timespace X300 DVR exported file format (XBA file format, single stream & multi-stream).

Post Plugin Installation

- 1. Enable the XPEG decoder in the RenderingService.ini file's SupportedDecoders section on the Server directory, by removing the semicolon character from the ;BriefCam XPEG Decoder row.
- 2. Restart the Rendering service.

Known Limitations

When deleting one stream on Timespace multi-stream files, all other streams from the same file are deleted as well.

Technical How-tos

Changing Default Ports Configuration

Moving the BriefCam Network Share





Running BriefCam in Virtual Environments

Configuring Single Sign-On (SSO)

SAML – ADFS Relying Party Setup for BriefCam Requirements

Installing and Configuring NGINX

Configuring RESEARCH and Web Services Distributed Environment

Adding a New Cluster in the RESEARCH Module

Updating the LDAP Password of the AD User

Changing Default Ports Configuration

To define alternative ports in case one of the default ports is occupied, follow the steps below.

RESEARCH HTTP Port (8090)

- In the Qlik Management Console (open a browser and use the following URL: https://RESEARCH_Host_Name/ qmc), select **Proxies** on the QMC start page or from the **Start** drop-down menu to display the overview. Select **Central** proxy and click **Edit**. Click the **Ports** tab on the right-side menu.
- 2. In the **Proxies** window, select **Edit Proxy** and change the default 8090 port on **Service listen port HTTP** to an available port.

# Rat *			😧 Help 🔻 beauer 🕶
Pooles Edit prog			
A Proces	X falt prog		
Curani	104N7191CATION		Properties
	Node	Central	✓ Identification
	PORTS		✓ Perts
	Service later port HTTPS (default)	843	Advanced
	Authentication listen port HTTPS (default)	R1M	Logging
	Kerberos authentication	0	Tan she
	REST API later port	00	Decordy
	Allow HTTP	x	Tags
	Service lister port HTTP	10M	Custom properties
	Authentication listen port HTTP	12.01	Associated Hemo
			Virtual process

3. On the machine where the Web Services are installed, edit the RESEARCH HTTP Port in the Web config file. The file is located in the BriefCam Web Services installation folder (i.e. C:\Program Files\BriefCam\WebServices\ProWebApi), by updating QlikHttpPort value to the same port you have configured on the Qlik Management Console: <add key="QlikHttpPort"> value="8090" />

RESEARCH API Ports (4242, 4243)

- 1. In the Qlik Management Console (open a browser and use the following URL: https:// RESEARCH_Host_Name/ qmc), select **Proxies** on the QMC start page or from the **Start** drop-down menu to display the overview.
- 2. In the **Proxies** window, select **Edit Proxy** and change the default 4242/4243 ports on REST API listen port/ Authentication listen port HTTP to an available port.

# Stat *			🖨 Help 🔻 bouter 🔻
Pooles Edit prog			
A Protes	X felt prog		
CHON	IDENTIFICATION		Properties
	Node	Central	✓ Identification
	PORTS		✓ Porta
	Service listen port HTTPS (default)	44)	Advanced
	Authentication listen port HTTPS (default)	4244	Logaina
	Kerberos authentication	8	
	REST API listen port	4243	second
	Allow HTTP	*	Taga
	Service laten port HTTP	8090	Custom properties
	Authentication listen port HTTP	4248	Associated Items
			Virtual provins



3. On the machine where the Web Services are installed, edit the RESEARCH API Ports in the Web config file. The file is located in the BriefCam Web Services installation folder (i.e. C:\Program Files\BriefCam\WebServices\ProWebApi), by updating QlikQrsPort /QlikProxyPort values to the same ports you have configured on the Qlik Management Console:

<add key="QlikProxyPort" value="4243" />

<add key="QlikQrsPort" value="4242" />

Moving the BriefCam Network Share

Ó

The steps below can now be done automatically using the Move Storage tool.

If you want to move the BriefCam network share that contains all BriefCam visual artifacts to another location, carry out the steps below.

- 1. From the Windows services, stop the VSService.
- 2. Create a folder on the new location (such as on a remote server).
- 3. Share the new folder:
 - a. Right-click the folder and click Properties.
 - b. Select the Sharing tab.
 - c. From the Sharing window, click Advanced Sharing.
 - d. Check the Share this folder box.
 - e. Click Permissions.
 - f. Add the desired user(s) and assign them with the same permissions that were applied on the previous shared folder.
- 4. Copy the ServerData folder to the new location.
- 5. Update the database paths by running the following commands in a database console, such as PGAdmin:

update BC_VIDEO_ARCHIVE set exportfolder=replace(exportfolder,\\Machine_A',\\Machine_B')

update BC_VIDEOFILE_INFO set path=replace(path,'file://Machine_A','file://Machine_B')

update BC_SETTINGS set setting=replace(setting,'\\Machine_A','\\Machine_B') where field = 'VideoProductsPath'

update BC_SYSTEM set value=replace(value,'\\Machine_A','\\Machine_B')

- 6. Update IIS Physical Paths with the new machine name:
 - a. Open IIS, in the **ProWebApiStorage** site click on all virtual directories, open the **Basic Settings** on the right and edit the **Physical Path** field.
 - b. In the VideoStreamingGateway site, click on the the VideoService virtual directory, open the Basic Settings and edit the Physical Path field.
 - c. Restart IIS (by opening the Windows services, right-clicking on the **World Wide Web Publishing Service** and clicking **Restart**).

After restarting the IIS services, it might take a minute or two to get results when filtering objects for the first time after the restart.

7. Start the **VSService**.

8. From the BriefCam Administrator Console, restart the **Rendering Service**.

Running BriefCam in Virtual Environments

BriefCam generally recommends using dedicated physical hardware servers for production environments, as per the specifications outlined earlier in this section. In some cases, customers may wish to employ VMs (Virtual Machines) to run BriefCam software. While this is technically possible, VMs tend to excessively depend on virtualization solution resources, and may be impacted by other concurrently running VMs. BriefCam, therefore, cannot guarantee optimal performance for





customers using such environments.

If customers want to use VMs in accordance with the limitations stated above, they will need to assure that VMs conform with the physical hardware server specifications recommended by BriefCam, and specifically that the virtualization products reserve and allocate the GPU, CPU and RAM resources required by BriefCam. Additionally, disk IOPS performance (whether of the virtual machines or of external NAS or SAN storage devices) must be guaranteed to be similar to that of a local disk.

Configuring Single Sign-On (SSO)

BriefCam offers three ready-made options for single sign on, and an interface to implement a custom single sign on solution.

The three built-in SSO options are:

- 1. SAML-based SSO where you can authenticate an existing SAML token provider. See SAML-based SSO for information about how to deploy this.
- 2. Active Directory single sign on, where we connect to an active directory and synchronize users and group from there. See the Microsoft Active Directory Integration section in the BriefCam Administrator Guide for information about how to deploy this.
- 3. Milestone XProtect single sign on. In Milestone installations we offer an option to use the Milestone Client and Directory to provide a single sign on solution.

SAML-based SSO

To integrate an existing SAML token provider (such as Microsoft ADFS) with BriefCam, use the BriefCam SAML infrastructure, by entering your own token provider's information and URLs in the appropriate places in the **Environment Settings' Pro Web API** section:

- SamILoginUrI This is the SAML login endpoint, which is a SAML token provider that responds to SAML authentication requests. When logging in to BriefCam, the user is rerouted to this address with a parameter that tells the endpoint to return the login information to BriefCam after logging in.
- **SamILogoutUrl** This is the SAML logout endpoint, which provides logout functionality. Users will get redirected to this address once they sign out of BriefCam.
- SamICertificate This is the SAML certificate fingerprint, which is a unique identifier given by Windows for this SAML certificate. The certificate, which should be installed on the local PC, is used to encrypt the communication between BriefCam's SAML client, and the SAML token provider.

-Brie	f Cam ADMIN	ENVIRC	NMENT SETTI	NGS	
E Eve	ents	Search	Q	Pro Web API	Show settings that have been changed
₽ _₽ Us	er Management	Second	Turne	Var	Makan
⊕ Þ¢	ployment A	Scope	type	NEY	value
[] Se	ttines. 🗸	GLOBAL	Pro Web API	minimumObjectWidth	4
		GLOBAL	Pro Web API	General.SettingUpdateInten	val 10
Ca	mera Management	GLOBAL	Pro Web API	SamiLoginUrl	https://localhost/adfs/is/idpin
En	vironment Settings		D	6	
Lo	calization	GLOBAL	Pro Web API	SamiLogoutUri	
Ev	ents Threshold	GLOBAL	Pro Web API	SamiCertificate	

See also SAML - ADFS Relying Party Setup for BriefCam Requirements.

SAML – ADFS Relying Party Setup for BriefCam Requirements

- 1. To use ADFS to log in to your BriefCam instance, you need the following components:
 - An Active Directory instance.
 - A server running Microsoft Server 2012 or 2008. This guide uses screenshots from Server 2012R2, but similar steps should be possible on other versions.



- An SSL certificate to sign your ADFS login page and the fingerprint for that certificate.
- After you meet these basic requirements, you need to install ADFS on your server. Configuring and installing ADFS is beyond the scope of this guide, but is detailed in a Microsoft KB article.



BriefCam uses the user's email provided by ADFS as part of the SAML assertions in order to identify the user.

2. When you have a fully installed ADFS installation, note down the value for the **SAML 2.0/W-Federation** URL in the **ADFS Endpoints** section. If you chose the defaults for the installation, this will be '/adfs/ls/'.

Step 1: Adding a Relying Party Trust

- 1. At this point you should be ready to set up the ADFS connection with your BriefCam instance. The connection between ADFS and BriefCam is defined using a Relying Party Trust (RPT).
- 2. Select the **Relying Party Trusts** folder from ADFS Management, and add a new **Standard Relying Party Trust** from the **Actions** sidebar. This starts the configuration wizard for a new trust.

\$ 1	Add Relying Party Trust Wizard
Welcome	
Welcome Steps • Welcome • Select Data Source • Configure Multi-factor Authentication Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.
	< Previous Start Cancel

3. In the Select Data Source screen, select the last option, Enter data about the relying party manually.

=BriefCam

\$ 1	Add Relying Party Trust Wizard		
Select Data Source			
Steps Velcome Select Data Source Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network: Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.		
	< Previous Next > Cancel		

4. On the next screen, enter a **Display name** that you'll recognize in the future, and any notes you want to make.



\$ 1	Add Relying Party Trust Wizard
Specify Display Nan	ne
Steps	Enter the display name and any optional notes for this relying party.
Welcome	Display name:
Select Data Source	BriefCam relying party
Specify Display Name	Notes:
 Choose Profile 	
 Configure Certificate 	
Configure URL	
Configure Identifiers	
Configure Multi-factor Authentication Now?	v
 Choose Issuance Authorization Rules 	
Ready to Add Trust	
 Finish 	
	(Depring Next) Consel
	< rrevious Next > Cancel

5. On the next screen, select the **AD FS profile** radio button.





6. On the next screen, leave the certificate settings with their defaults.

-BriefCam

\$ 1	Add Relying Party Trust Wizard		
Configure Certificate			
Steps	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the		
 Welcome Select Data Source 	claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse		
 Specify Display Name Choose Profile 	Issuer: Subject: Effective date:		
Configure Certificate			
Configure URL Configure Identifiers	View Browse Remove		
 Configure Multi-factor Authentication Now? 			
 Choose Issuance Authorization Rules 			
 Ready to Add Trust Finish 			
	< Previous Next > Cancel		

7. On the next screen, check the box labeled **Enable Support for the SAML 2.0 WebSSO protocol**. The service URL will be: https://<WebServices>/ProWebApi/AuthenticationApi/AuthenticateSaml

Replace <WebServices> with your BriefCam WebServices server address. Note that there's no trailing slash at the end of the URL.

%	Add Relying Party Trust Wizard
Configure URL	
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Cetificate Configure URL Configure Identifiers	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party. Enable support for the WS-Federation Passive protocol The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol. Relying party WS-Federation Passive protocol URL: Example: https://fs.contoso.com/adfs/fs/
Configure Mubi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Enable support for the SAML 2.0 WebSSO protocol The SAML 2.0 single sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol. Relying party SAML 2.0 SSO service URL: https:// <webservices>/ProWebApi/AuthenticationApi/AuthenticateSamI Example: https://www.contoso.com/adfs/ts/</webservices>

8. On the next screen, add a Relying party trust identifier.

https://<WebServices>/prowebapi must match the exact prowebapi address in the settings (it is case sensitive).



\$	Add Relying Party Trust Wizard		
Configure Identifiers			
Steps	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying	ng	
Welcome	party trust.		
Select Data Source	Relying party trust identifier:		
Specify Display Name	Add		
Choose Profile	Example: https://fs.contoso.com/adfs/services/trust		
Configure Certificate	Relying party trust identifiers:		
Configure URL	Remove	e	
Configure Identifiers			
 Configure Multifactor Authentication Now? 			
 Choose Issuance Authorization Rules 			
Ready to Add Trust			
e Finish			
	Previous Next > Cannel		

HTTPS is required in the address.9. On the next screen, you can configure multi-factor authentication but this is beyond the scope of this guide.



\$	Add Relying Party Trust Wizard			
Steps Welcome Select Data Source	Configure multifactor authentication settings for this relying party trust. Multifactor authentication is required if there is a match for any of the specified requirements.			
Specify Display Name Chaose Profile Configure Certificate Configure URL Configure Identifiers	Multi-factor Authentication Requirements Users/Groups Not com Device Not com Location Not com	Global Settings figured figured		
Configure Multi Actor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	I do not want to configure multi-factor authentication Configure multi-factor authentication settings for this You can also configure multi-factor authentication set	settings for this relying party trust at this time. relying party trust. ttings for this relying party trust by navigating to the		
	Authentication Policies node. For more information, s	<pre>contiguing Autrentication Policies.</pre>		

10. On the next screen, select the **Permit all users to access this relying party** radio button.
-=BriefCam



11. On the next two screens, the wizard will display an overview of your settings. On the final screen, use the **Close** button to exit and open the **Claim Rules** editor.





Step 2: Creating Claim Rules

Once the relying party trust has been created, you can create the claim rules.

1. To create a new rule, click on Add Rule. Create a Send LDAP Attributesas Claims rule.

\$ 0	Add Transform Claim Rule Wizard	×
Select Rule Templat	le	
Steps Choose Rule Type	Select the template for the claim rule that you want to create from the following list. The description provide details about each claim rule template.	8
Configure Claim Rule	Claim rule template:	
	Claim rule template description:	
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumbe Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.	स >
	< Previous Next > Cancel	

- On the next screen, using Active Directory as your attribute store, do the following:

 From the LDAP Attribute column, select E-Mail Addresses.
 From the Outgoing Claim Type, select E-Mail Address.



- 3. Repeat step for UPN.
- 4. Click **OK** to save the new rule.

Step 3: Configuring BriefCam

- 1. After setting up ADFS, you need to configure your BriefCam instance to authenticate using SAML.
- 2. You'll use your full ADFS server URL with the SAML endpoint as the SSO URL.
- 3. The fingerprint will be the fingerprint of the token signing certificate installed in your ADFS instance. In the Windows certificate utility, this is also referred to as the SHA-1 Thumbprint.
- 4. Export the ADFS token signing certificate (on the ADFS server) in PowerShell as admin:

\$certRefs=Get-AdfsCertificate -CertificateType Token-Signing

\$certBytes=\$certRefs[0].Certificate.Export([System.Security.Cryptography.X509Certificates.X509ContentType]::Cert)

[System.IO.File]::WriteAllBytes("c:\foo.cer", \$certBytes)

- 5. Copy c:\foo.cer to the BriefCam server.
- 6. Launch mmc.
- 7. File -> add remove snap ins.
- 8. Certificates -> add -> computer account -> local computer.
- 9. Go to Certificates -> Personal -> Certificates.
- 10. Right click on Certificates and select All Tasks -> Import foo.cer.



🕌 Console1 - [Console Root	t\Certificates (Lo avorites Windo	ocal Computer)\ ow Help	Persona	I − □ ×	1 75.04
🗕 🔿 🙍 💼 🛍 🙆	🔒 🛛 🖬			J	/5%
Console Root		Issued To	^	Actions	
 Certificates (Local dor ~ ⁽ⁱ⁾ Personal 	nputer)	°⊒ ।	E	Certificates 🔺	
Certificat			_	More Actions	-
> 📑 Trusted Root	All Tasks		›	Request New Certificate	
> 📔 Enterprise Tr	View		> L	Import	
> intermediate > intermediate	New Window fr	om Here		Advanced Operations	>
> 🔛 Untrusted Co	New Taskpad Vi	ew			
> Third-Party F	Refresh				
> 📫 Client Authe	Export List				
> 🧾 Preview Buil > 🧾 Test Roots	Help				
> Cther People					
> SIM Certification	Authorities				

- 11. Double click the new certificate, go to the details tab and copy the certificate thumbprint.
- Paste the thumbprint into a text editor, remove the spaces, then copy and paste it into the ProWebAPI section in the web admin > Settings SamICertificate field.
- 13. Configure the following fields in the BriefCam Administrator Console's environment settings:
 - **SamlLoginUrl** = https:// <ADFS Server address>/adfs/ls/idpinitiatedsignon
 - **SamILogoutUrl** = ADFS server logout URL
 - ProWebApiAddress = https://<ProWebApi address>:8666/
 - ProWebClientAddress = https://<ProWebClient address>/app/#/
 - SamICertificate = <SAML Certificate>
- In IIS manager on the WebServices computer, go to BriefCam Web Services > Bindings > Add, from the Type drop-down menu, select https and click OK.

Internet Information Services (IIS) Mar	raðei	- 🗆 X
← → ● + 16GPU + Sites +	Briefcam Web Services 🔸	🔤 🖂 🔒 🔒 •
File View Help Connections Q 2 2 9.	Site Bindings ? × Add C** "Inding ? × Add_	Actions
Gene (16GPU/Administrator) Gene (16GPU/Administrator)	4 Eddress: Port: Eddress: Parmove https ~ All Unassigned ~ 443 Remove Host name: Browse Browse Browse Browse Browse	Edit Site Binding Basic Settings View Applications
	Require Server Name Indication	View Virtual Directories Manage Website

15. Restart the IIS Services (by opening the Windows services, right-clicking on the **World Wide Web Publishing Service** and clicking **Restart**).

16. You should now be set up and ready to go. To test, run:https://localhost:8666/authenticationApi/ RequestAuthenticationRoute

If you were re-routed to the login page, logged in, and received a valid output (session id and username), congratulations you have successfully survived this guide.

Otherwise, make sure you followed all the steps correctly.

Installing and Configuring NGINX

This section describes the steps to take to use NGINX.

=BriefCam



To work with SSL and BriefCam, using a load balancer is required. BriefCam recommends using NGINX.

Recommendations

It is recommended to install the load balancer on a separate machine.

If you are working in a virtualized environment, the load balancer must be on a separate machine.

If you are working in a non-virtualized (physical servers) environment, you can have the load balancer on the same machine as the Web Services (although it is not recommended). However, if you install the load balancer on the same machine as the Web Services, IIS has to work on a different port (not 80, since 80 is for NGINX).

Prerequisites

- Make sure that port 80 is not in use by another application.
- If IIS is installed, make sure to stop it or change its default port.

Steps

1. To run the BriefCam NGINX Installation wizard, right-click on the BriefCamNGINX_<Version number>.exe file and select Run as administrator.



2. In the Welcome screen, click Get Started.





3. Accept the terms of the BriefCam license agreement and click Next.

-BriefCam



4. Read the license agreement and click Next.





 Enter the IP address or the hostname (if there is a DNS resolution) for each of the relevant services below, and click Next. Note that once you enter the Research host, you can click the "Click to use the RESEARCH host for all service" button to fill in all the fields with this value. -BriefCam

			×
<i></i> =BriefCam			Install NGINX
Clickt	o use the RESEA	RCH host for	all services
✓ Use New Stora	age Service		
Research	product1		Internal Port 8090
Notification			Internal Port 7080
Video Streaming			Internal Port 5010
Web Services			Internal Port 80
Processing		Port 49149	Internal Port 5002
VMS Agent		Port 49151	Internal Port 1120
Visual Assets		Port 49251	Internal Port 5011
Storage Service			Internal Port 5012
Back			Next

6. Decide whether to run with a secure communication.



7. If you check the checkbox, enter the paths to the certificate and private key.

You need to create or use an existing self-signed certificate separated into two files: .crt and .key.

- 8. If your SSL certificate is protected by a password, you need to configure NGINX to read a list of passwords that are stored in a separate file. If the private key is not in this file, NGINX will not start. You do this as follows:
 - a. Create a new text file named ssl_passwords.txt and save it to a separate folder than where the SSL certificate is located.
 - b. Set the file to be readable only to the user running NGINX.
 - c. Enter the certificate password into the first line of the ssl passwords.txt file.
 - d. In the nginx config file, add the following line above the existing certificate lines:

ssl_password_file /var/lib/nginx/ssl_passwords.txt;e. Distribute this file separately from the configuration file.

9. Click Next.

The following screen appears.



- 10. In the **Database Host** and **Database Port** fields, enter the name and port of the machine where you installed PostgreSQL.
- 11. In the **Application User** and **Application Password** fields, enter the username and password that you entered when installing PostgreSQL.
- 12. Click the Test Database Connection button.
- 13. Click Next.
- 14. Confirm or select the drive where you want to install NGINX and click Install.





- 15. If you have more than one web service hostname, after installing NGINX, open the nginx.conf file (located by default at: C:/nginx/conf) and in the http section, copy and paste the existing rows and update the new rows with the additional hostnames.
- 16. On any host that is running the application (browser) make sure the domains (or host name) can be resolved by the DNS. If no DNS is available, you can edit the hosts file and add the IP address of the load balancer using the following syntax:

10.x.x.x www.example.com example.com

For example: 10.0.0.143 www.example.com

- 17. Open the following three web config .js files on the BriefCam server (by default these three files are at C:\Program Files\BriefCam\WebServices):
 - \app\webConfig.js
 - \ProWebAdminClient\web.config.js
 - \ProWebClient\webConfig.js

-BriefCam



18. In each of the three web config .js files, set the endpoints (endPointApi) to point to the load balancer. In the example below, you would just change PRODUCT1 to the address of the load balancer. Make sure that "http:" does not appear in the path.



- Open the QLIK QMC with the user that was used to install the RESEARCH module (https://<hostname>/qmc).
 Browse to virtual proxies and add two new parameters using the hostname of each of the machines (for example,
 - the QLIK machine and the NGINX machine host names as shown in the image below) to both proxies:
 - Virtual Proxies->bc->advanced->Host white list
 - Virtual Proxies->Central Proxy (Default)->advanced->Host white list

Host white list 5	
	C Add new value
glik-server-name	
www.example.com	



On some systems, you might be required to add the host name, FQDN and IP address of the load balancer and all the web services instances into the virtual proxies white list in QMC.

21. In the **User directory connectors** screen, go to the **Visible connection string** and add the domain name to the server value. For example, in the image below, Stress-DB was the original value and now it is Stress-DB.briefcamdev.com.



🖷 Start 🔻			😨 Help 🕞
User directory connectors Edit user dir	ectory connector		
 User directory connectors 	1. Edit user directory connector		
RESEARCH_USERS	IDENTIFICATION		Properties
	Name	RESEARCH_USERS	✓ Identification
	Тура	COBC	✓ User sync settings
	USER SYNC SETTINGS		Connection
	Sync user data for existing users	When this option is cleared, user data is synced for all users in the user directory, not only existing users.	Tegs Associated items
	CONNECTION		User access
	User directory name	RESEARCH_USERS	Tasks
	User table name	bc_bl_users	
	Attributes table name	bc_bl_usrat	
	Visible connection string	driver=[PostgreSQL Unicode(x64)] server=Stress-DB briefcamdev.com, stabase=briefcam;	

- 22. Check that the following environment settings are set to the NGINX IP address or hostname and if you selected to use a secured connection (https), make sure the URLs begin with https:
 - BaseVideoUrl
 - clientNotificationEndPoint
 - DB.LocalStorageAddress
 - LoadBalancerAddress This setting should be set to the NGINX hostname (FQDN)
 - ProWebApiAddress
 - ProWebClientAddress
 - QlikServer
 - Site.Url
 - StorageGatewayUrl
 - SSOEndpoint If you want to use an embedded client, this value should be set to: http[s]://<NGINXhost>:8030/MilestoneSSO/
- If you are installing a Linux-based OX engine, make sure that the value for the OX6.EngineOutputGatewayGrpcPort environment setting matches what you entered in the installer's Processing box (default 49149).
- 24. If you are installing a Linux-based OX engine, make sure that the value for **OX6.VmsAdapterGrpcPort** environment setting matches what was entered in the installer's **VMS Agent** box (default 49151).



- 25. Restart the BriefCam services.
- 26. If you selected to use a secured connection (https), browse to the application and check that it works with https requests. For example:
 - https://www.example.com/app
 - https://www.example.com/admin





NGINX Windows Service

The BriefCam NGINX installer creates a BriefCam NGINX Web Server service in the Windows Services screen. This service is responsible for making sure the NGINX process is constantly running and the load balancer is ready to accept requests. The user that runs this service is the BriefCam Windows user.

Services			-		\times
File Action View Hel	p				
💠 🔶 📷 📷 🎰	🛛 🗊 🕨 🗰 🖬 🕪				
Services (Local)	Services (Local)				
	World Wide Web Publishing Service	Name	Description		^
	Stop the service Restart the service Description: Provides Web connectivity and administration through the Internet Information Services Manager	Bluetooth Audio Gateway Service Bluetooth Support Service Bluetooth User Support Service_1111a7 BriefCarche BriefCam NGINX Web Server BriefCam VSService BriefCamPostgreSQL - PostgreSQL Se	Service suppo The Bluetooti The Bluetooti This service c BriefCam NG	orting the h service : h user ser aches net INX Web	aud supp vice tworl Serv
		Capability Access Manager Service CaptureService_1111a7 CaptureService_1111a7 Cellular Time <	Provides facil Enables optio This service s	ities for n mal scree ets time b	nana n caj asec v
	Extended Standard				

Generic Configurations

For any other type of load balancer, such as Amazon ELB, Google Cloud Platform Load Balancer and so on, you need to configure redirect rules based on the URL. The following are the redirect rules:

Logging

To handle the log rotation:

- 1. Download the log rotation script from this link (external link).
- 2. Save the script to C:\NGINX.
- 3. Create an OS user (such as bcuser), a user on the OS level or create a Windows user account. The user does not need admin rights.
- 4. Edit the C: \NGINX folder's security options and give the user that you created in step 3 full control.
- 5. Run the Local Security Policy utility.





Go to Security settings->User Rights Assignment and add the user to Log on as a batch job.
 Add a daily scheduled task to run the C:\NGINX\LogRotation.bat file. Make sure to check Run whether user is logged on or not. By default, the last 10 days will be kept (retention period in days). If you want a different number of days, when running the batch file, pass the required number of days as a command line argument. For example, if you want 20 days, you would use: C:\NGINX\LogRotation.bat 20.

Adding a New Cluster in the RESEARCH Module

This how-to provides a step-by-step description on how to build and configure a RESEARCH cluster environment. This includes a failover option between the Scheduler node and the Central and/or failover between two Central nodes to achieve high availability.





Introduction

As the amount of data grows and the business logic becomes more complex, additional resources are necessary to calculate the results and deliver them to users. If a Single Node (small) site is used, its performance may deteriorate over time, which could compromise the credibility and quality of BriefCam's RESEARCH module.

To address this issue, a RESEARCH module cluster is employed as a distributed architecture to alleviate the data and application loads from the main RESEARCH server that controls the entire RESEARCH site. The Central node, also known as the "manager", delegates some of its tasks to a secondary machine, referred to as the Scheduler node or the "worker." When receiving a task ID from the manager, the worker reads the task from the local repository database and performs the necessary computations. Once the task is completed, the worker returns the task state (successful or failed) to the manager.

Hardware Specification for the Scheduler Node

The following are the minimum requirements for the Scheduler node:

CPU	2 x Intel(R) Xeon(R) Gold 6234 CPU @ 3.30 GHz (32 vCPU)
Memory	512 GB
Storage	2 x 100 GB SSD 1 x 25.5 TB SSD capacity drives

Implementation Steps

Adding a New Cluster in the RESEARCH Module

To add a new cluster in the RESEARCH module:

- 1. Verify that the existing Qlik server is reachable from the new server by opening the following path on both the file explorer and in a browser: \\[QlikServer]\qlikshare.
- 2. Make sure that the firewall and antivirus are disabled on the new server.
- 3. Make sure that a PostgreSQL Unicode (x64) driver is installed. You will need this to create the two ODBC connections in the next step.
- 4. Add two ODBC connections RESEARCH and RESEARCHPostgreSQL.

or DSN	System DSN	File DSN	Drivers	Tracing	Connection Pooling	About	
System D	ata Sources:						
Name		Platform	Driver				Add
pgBrief(Cam	64-bit	Postgre	SQL Unic	ode(x64)		
RESEARCH 64-bit PostgreSQL Unicode(x64)			Remove				
RESEA	RCHPostgre SQ1	64-bit	Postgre	SQL Unio	ode(x64)		
							Configure

a. For the RESEARCH ODBC connection, map the database to the BriefCam database server.

-BriefCam

ata Source	RESEARCH	Description		
Database	briefcam	SSL Mode	prefer	~
Server	BEN-NGINX-01	Port	5432	
User Name	brief	Password	•••	
ptions				

b. For the RESEARCHPostgreSQL ODBC connection, map the database to the RESEARCH database server.

PostgreSQL Ur	nicode ODBC Driver (psq	IODBC) Setup		×
Data Source Database Server	SEARCHPostgreSQL QSR BEN-NGINX-03	Description SSL Mode Port	prefer 4432	~
Options Datasource	Global	Password	(ye)	Test Cancel

*Port 4432 is required to be opened inbound on the 1st RESEARCH machine so that the 2nd RESEARCH machine could access its Postgres database.

- 5. Create a service account user (by default, BCUser is the user that runs Qlik services). In the Computer Management, check that the user is in the Administrators group.
- 6. Make sure that the service account user created in the step above is included in the Log on as a service local policy:





- 7. Download the Qlik vanilla installer (located in your Git account at: https://github.com/qlik-download/qlik-sense-server/ releases). It is important that the version be the same as the version installed on the existing server.
- 8. If you are installing the Qlik May 2022 version, download and install .NET 4.8 Framework Runtime from this link: https://dotnet.microsoft.com/en-us/download/dotnet-framework/net48.
- 9. On the existing Qlik server, open the Windows services and stop all Qlik services.
- 10. Go to ProgramData\Qlik\Sense\Repository\PostgreSQL\12.5 (or any version you have) and back up the following files:

pg_hba.conf	
pg_ident.conf	
DG_VERSION	
postgresql.auto.conf	
postgresql.conf	

11. Edit the pg_hba.conf file to allow non-local connections:

# TYPE	DATABAS	E	USER		ADDRESS	METHOD	
# IPv4	local co	nnection	s:	- F		1	
host	all		all		0.0.0.0/0	md5	
# IPv6	local co	nnection	s:				
host	all		all		::0/0	md5	
# Allow replication connections from localhost, by a user with the							
# replication privilege.							
host	replica	tion	all		127.0.0.1/32	md5	
host	replica	tion	all		::1/128	md5	
host	all	all	0.0.0.0	/0	md5		
host	all	all	::/0	md5			

12. Edit the postgresql.conf file to accept more connections from all addresses:





13. 14. 15.	listen_address max_connection Start all Qlik service Run the Qlik install Click the Join a clu	ses = *** ns = 800 es. er as administrator. ister button.
	Qlik	Sense® Enterprise
	Create or jo	Create a cluster Create a single-node deployment or the first node in a cluster. Create a cluster
	<	Join a cluster Create a node to join an existing cluster. Join a cluster

16. Fill in the database credentials (of the existing Qlik server):



	Sense® Enterprise
Enter database	credentials
To connect to an database host na	existing repository database, enter the PostgreSQL me and provide the database user password.
Database host nar	ne 🕜
ben-nginx-03	
Database port)
4432	
Database user	
qliksensereposito	rry
Database user pas	sword

	3
Cancel B	ack

17. Fill in the service account user credentials (the one defined in the new server):

Qlik 🝳	Sense® Enterprise
Provide informa	tion for the Qlik services
Settings and acco installed on the ho	ount information needed for Qlik Sense services ost computer to work properly.
Windows service a	ccount credentials
Username	
ben-nginx-02\bcu	iser
Password	
******	0

- After installing Qlik, install the relevant patch according to the version you are using (May 2022 or Nov 2020).
 Go to the existing Qlik server and open the QMC (https://localhost/qmc).
 Select Nodes.

- Click Create new in the action bar.
 Fill in the parameters as shown in the image below with the Host name field set to the hostname of the newly





IDENTIFICATION Name Host name NODE PURPOSE Node purpose NODE CONFIGURATION	
Host name NODE PURPOSE Node surpose NODE CONFIGURATION	Ben-regire-0.2 If the host name server does not have an authorized certificate, a password will be generated and displayed. Use this password to authorize the certificate on the localitost of the host name server. Both
NODE PURPOSE Node purpose NODE CONFIGURATION	If the host name server does not have an authorized certificate, a password will be generated and displayed. Use this password to authorize the certificate on the localhost of the host name server. Both
NODE PURPOSE Node purpose NODE CONFIGURATION	* Both
Node surpose	* Both
NODE CONFIGURATION	
Failover candidate	0
Node roles	
This node has currently no roles.	
SERVICE ACTIVATION	
Repository	5
Engine	
Printing	
Proxy	0
Scheduler	<u>∿0</u>
CUSTOM PROPERTIES	

- 23. Click Apply and wait several seconds.
 24. If the server cannot reach the remote host, you will see the following 'Node registration' message.

No	ode registration
R	equesting authorization password for he certificate on the node.
	Close
	a. Check the connectivity between the Central node and the Scheduler node.

- b. Using ping, verify that IPV6 as well as the firewall are disabled on both nodes.
- 25. Click Apply again. Wait until you get an authorization password and a URL. The connectivity is done via port 4444.





26. Go to the new Qlik server, open the URL from the previous step: http://localhost:4570/certificateSetup and enter the password from the previous step:

2

Install certificates

Certificates have been distributed to this machine. Use the password provided in the management console to install the certificates.

Submit

Password:	
-----------	--

@ Help



- 27. On the original Qlik server (not the new cluster), restart all Qlik services.
- 28. Make sure you get the following result on the QMC's **Nodes** screen:

∯ Start ▼					
Nodes >					
Nodes Showing: 2 Selected: 1					
Name A G	Host name 🕞	Status	1		
Central	ben-nginx-03	5 of 5 services are running	0		
Scheduler	ben-ngira-02	3 of 3 services are running	0		

This means that there are now two Qlik servers (multi-node) – Central and Scheduler.

29. In the QMC'sSchedulers section, edit the Central node and set the Type field to Manager:



A Schedulers	🛅 Edit scheduler	
Cartoni		
	10EMTIFICATION	
	Node	Central
	LOGGINS	
	Audit activity log level	Basic w
	Sienvice log level	310 W
	TRACING	
	Application log level	346 W
	Audit tog level	Into w
	Performance log level	Into w
	Gecurity log level	into w
	System log level	300 W
	Task execution log level	340 W
	ADVANCED	*(Manazi w)
	Max concurrent reloads	a a a a a a a a a a a a a a a a a a a
	Engine timesul (inimulae)	
	CUETLAN PROPERTIES	
	Apple: Cancel	

30. In the QMC's Schedulers section, edit the Scheduler node and set the Type field to Worker:

Note Schedular coolins Salic valit activity tog level Salic isrice log level Salic valit activity tog level Salic valit Salic valit activity tog level Salic v	DENTIFICATION				
Locativa Audit activity hog level Service log level Service log level Audit log level Audit log level Servity hog level <th>io de</th> <th>Scheduler</th> <th></th> <th></th> <th></th>	io de	Scheduler			
Audit activity top lavel Basic Gervice top lavel Into Audit top lavel Into Audit top lavel Into Performance top lavel Into Security top lavel Into Audit top lavel Into Audit top lavel Into Performance iop lavel Into Security top lavel Into Audit top lavel Into Aud	COGENG			N	
Service log level Into V Application log level Into V Audit log level Into V Performance log level Into V Security log level Into V Spatem log level Into V Task execution log level Into V ADVANCED Type Vorker Apple tineout (minutes) Into V Engine timeout (minutes) Into V Custom PROPERTIES	udit activity log level	Basic	~	Leg.	
RACINO Application log lavel Audit log level Audit log level Performance log level Security log level Into Cystem log level Into Verformance log level	ervice log level	Info	~		
kapication log laval Into v kudit log laval Into v Performance log laval Into v Security log laval Into v Apatem log laval Into v Apatem log laval Into v Task execution log laval Into v Task	RACING				
Audit log level Info V Performance log level Info V Security log level Info V Security log level Info V Task execution log level Info V ADVANCED Type Worker As concurrent reloads. 4 Engine timeout (minutes) 50	polication log level	Info	v		
Performance log level Security log level Security log level Task execution log level Task execution log level Type Worker ADXANCED Type Worker Engine timeout (minutes) DO CUSTOM PROPERTIES	udit log level	Info	¥		
Security log level Into v Spatient top level Into v Task execution tog level Into v ADVANCED Type Worker Max concurrent reloads. 4 Engine timeout (minutes) 50 CUSTOM PROPERTIES	erformance log level	Info	v		
Spatien top level Info	ecurity log level	Into	v		
Task execution tog level ADVANCED Type Worker Max concurrent reloads Engine timeout (minutes) CUSTOM PROPERTIES	ystem log level	Info	~		
ADVANCED Type Worker Max concurrent reloads Engine timeout (minutes) 50 CUSTOM PROPERTIES	ask execution log level	Into	v		
ADVANCED Type Worker Max concurrent reloads Engine timeout (minutes) 50 Custom PROPERTIES					
Type Worker Anton Concurrent reloads 4 50 50 50 50 50 50 50 50 50 50 50 50 50	DVANCED				
Max concurrent reloads 4 Engine timeout (minutes) CUSTOM PROPERTIES	ype	Worker			
Engine Einreout (minutes) 00 CUSTOM PROPERTIES	fax concurrent reloads	4			
CUSTOM PROPERTIES	ngine timeout (minutes)	30			
CUSTOM PROPERTIES					
	USTOM PROPERTIES				

31. In the QMC's **Data Connections** screen, edit the following three connections:



L

Name	Owner
ArchivedLogsFolder	sa_repository (INTERNAL\sa_repository)
AttachedFiles	sa_repository (INTERNAL\sa_repository)
DataPrepAppCache	sa_api (INTERNAL\sa_api)
ExternalData	bcuser (BEN-NGINX-03\bcuser)
monitor_apps_REST_app	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_appobject	sa_repository (INTERNAL\sa_repository)
monitor_apps_REST_event	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_license	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_license_analyzer	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_license_login	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_license_overview	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_license_professional	sa_repository (INTERNAL\sa_repository)
monitor_apps_REST_license_user	sa_repository (INTERNAL\sa_repository)
monitor_apps_REST_task	sa_repository (INTERNAL\sa_repository)
monitor_apps_REST_user	sa_repository (INTERNAL\sa_repository)
monitor_apps_REST_user_condensed	sa_repository (INTERNAL\sa_repository)
Research	bcuser (BEN-NGINX-03\bcuser)
ResearchPostgreSQL	bcuser (BEN-NGINX-03\bcuser)
ResearchQvd	bcuser (BEN-NGINX-03\bcuser)
Scripts	bcuser (BEN-NGINX-03\bcuser)
ServerLogFolder	sa_repository (INTERNAL\sa_repository)

32. For each of the three connections, in the **Connection string** field, instead of local path (such as drive c:), change it to work with the network path – the hostname where the **QlikShare** folder exists (the server where RESEARCH was originally installed):

IDENTIFICATION		
Name		Scripts
Owner		bcuser (BEN-NGINX-03\bcuser)
Connection string	lb-	
Туре	4	folder
User ID		
Password		

- 33. On the new server, open the QMC's Tasks section and make sure that both the research_db and Research apps are running successfully.
- In QMC (central node), navigate to the Load balancing rules section.
 Double click on ResourcesOnNonCentralNodes.

Load balancing ru	nes /						
🖅 Load balanc	ing rules Showin	g: 2 Selected: 0					
Name	A 🕞	Description	G	Resource filter	G	Actions	
ResourcesOnCent	tralNode	All resources need to b	e accessibl			Load balancing	
ResourcesOnNon	CentralNodes	All resources need to b	e accessibl	App_*		Load balancing	

36. Remove the marked section shown in the image below.



	g rules	Ø Help
IDENTIFICATION		
Disabled	0	
Name	ResourcesOnNonCentralNodes	
Description	All resources need to be accessible on the non-centra the monitoring apps	al nodes, except
BASIC		
Resource filter	App_*	
Actions	Load balancing	
This condition cann	ot be displayed in the rule editor because it is too complex.	
ADVANCED		
Conditions	((node iscentral="false" and resource stream.id!="a70 b5fa-6e207978dca1))	ca8a5-1d59-4cc9-
		(

Forcing Manual Failover Between the Scheduler and Central Node

To force manual failover between the Scheduler node and the Central node, carry out the following steps:

1. In QMC (central server), select the Schedulers menu.





2. Select the Central scheduler and click the Edit button.

Schedulers Showing: 2 Selected: 1			
Node	Active	🕞 Status	
Central	Yes	running	0
Scheduler La	Yes	running	0
Edit			

3. In the **Advanced** section's **Type** field, select **Manager and worker**. The Central node will return to its initial state (standalone server). The Scheduler node will stop functioning as a cluster member (and eventually will not be in use).



IDENTIFICATION		
Node	Central	
LOGGING		
Audit activity log level	Basic Y	
Service log level	Info 🗸	
TRACING		
Application log level	Info 👻	
Audit log level	Info 💙	
Performance log level	Info 👻	
Security log level	Info 👻	
System log level	Info 👻	
Task execution log level	Info 🗸	
ADVANCED		
Туре	Manager	
Max concurrent reloads	Manager Worker	
Engine timeout (minutes)	Manager and worker	

Editing the Load Balancing Rule Resources on Non-Central Nodes

- From the QMC start page, open Load Balancing Rules.
 Select the ResourcesOnNonCentralNode rule and click Edit.

d Ret +													0 Heb	• •	-	
Lost heleningrates																
The Lond Informing rule	e Stowi												Arlow V			
Hane	* D	Resigner D	Branar or War	D	Artions	Ballol	в	Cantent	D	lpe	э.	Tap				Э.
Resurse/OrkorGettal	-	All records and to be access.	- Aco.*		Lost telening	No.		Soft	-	Read Drip Contorn						
			1440								_					Π

3. In the Advanced section, edit the condition to the following: ((node.iscentral="false"))

4. Click Apply.



g Bat v				
Load belancing rules bo	BT load baancing rules			
👄 Edit load balancing re	des	e Help O	S Audit Restricted bal	incing rules
SDENTSPEATION Disabled Name Description EASSC Resource filter Actions This condition cannot b ADMACED Conditions		_ tqcne	Autit Trepetressure Center Bewinnered But in hub and ONC V Center Define your audit query above and click "Audit" to begin auditing	
Unit to Qilli Sonse help-a	bout rule conventions	Adate rule		

5. Verify that after this change all QMC tasks are running okay including the License and Operations tasks.

Central Node Failover (optional)

To avoid having a single point of failure in a multi-node site, when you add a new node to your deployment you can assign it the role of failover candidate. This means that any server or node in your RESEARCH site can perform the same role as the Central node. The role of the Central node can now be swapped, for example if the central node has been offline for more than 10 minutes.

If you want to back up the Central node:

- 1. Define an additional Central server (a new Central node with the same specifications as the original node).
- 2. In QMC (of the additional Central node), select the Nodes menu and define it as a Failover candidate.

I Edit node		
IDENTIFICATION		
Name		
	This field is mandatory.	
Host name		
	This field is mandatory.	
	If the host name server does not have an authorized certificate, a password will be generated and displayed. Use this password to authorize the certificate on the localhost of the host name server.	
NODE PURPOSE		
Node purpose	Production	×
100		
NODE CONFIGURATION		
Failover candidate		
·	when the node is a failover candidate, the engine, repository, proxy and scheduler services must be active.	

After you have configured a node to become a failover candidate, each node in your site will regularly check the primary node (Central node) to verify that the Central node is active. If there is no communication between the primary node and the other nodes in the site after 10 minutes, then the Primary node will be replaced by the next available node. If more than one node is set as a failover candidate each node will compete to get a lock on a database field and the winner becomes the Central node. There is an additional field in the QMC to show which node is currently the Central node.

Configuring a RESEARCH and Web Services Distributed Environment

If you are working with a distributed environment where the Web Services component and the RESEARCH component are on





separate machines, you either need to do one of the following:

- Use a load balancer (see: Installing and Configuring NGINX)
- Use an FQDN (preferred) or an alias/CNAME If you already use a domain, use a fully qualified name (FQDN). If the servers are not part of a domain (no FQDN), use an alias/CNAME. Details about how to do this are provided below.

You need to make these configurations because BriefCam's web application consumes the RESEARCH component from an IFrame (an HTML element that is used to insert content from another source – a third-party). The newest browsers improved their security and now prevent sending cookies along with cross-site requests.

The solution is to set up the cookies to be first-party (same-site) cookies (when the domain in the browser's URL bar matches your cookie domain).

To achieve this, you need to use the FQDN so the domain suffix will be the same for all the servers as highlighted in yellow in the examples below. If you only use the host name, such as "synopsis" or "research" in the examples below, there is no domain suffix and cookies are not shared between the sites.

For example:

- synopsis.your-domain.com
- research.your-domain.com

If you have a load balancer set up, you will not have this issue. For more information about this, see Installing and Configuring NGINX.

If you are using the FQDN or alias/CNAME option, you need to do the following:

1. If you are using a fully qualified name (**FQDN**), find the FQDN of your server, by clicking on the **System** menu in the Control Panel. You'll see the FQDN of your machine (if one exists).

1	System		
÷		I > System and Security > Sy	stem
	Control Panel Home	View basic information	about your computer
•	Device Manager	Windows edition	
•	Remote settings	Windows Server 2016 Stan	dard
ę	Advanced system settings	© 2016 Microsoft Corporat	tion. All rights reserved.
		System	
		Processor:	Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz 2.30 GHz (4 processors)
		Installed memory (RAM):	16.0 GB
		System type:	64-bit Operating System, x64-based processor
		Pen and Touch:	No Pen or Touch Input is available for this Display
		Computer name, domain, and	workgroup settings
		Computer name:	BC-AD
	FQDN COM	Full computer name:	BC-AD.BriefCam.Local
		Computer description:	
		Domain	BriefCam Local

- 2. From the BriefCam Administrator Console's **Environment Settings** section, edit the **QlikServer** setting and change it to the FQDN or alias/CNAME. For example, if your domain name is: www.test.com, use: research.test.com.
- 3. On the Web Services machine, edit the ProWebClient's webConfig.js file (located at: C:\Program Files\ BriefCam\WebServices\ProWebClient\webConfig.js) and replace the hostname with the FQDN or alias/ CNAME. For example:

const endPointApi = "//www.test.com/prowebapi"; const matomoSiteID = 10; const reCaptchaKey = "";

4. On the Web Services machine, edit the ProWebAdminClient's web.config.js file (located at: C:\Program Files\BriefCam\WebServices\ProWebAdminClient\web.config.js and replace the hostname with the FQDN or alias/CNAME. For example: const endPointApi = "//www.test.com/AdminApi/";



- 5. Enter **Qlik QMC > Virtual proxies** (https://localhost/qmc/virtualproxies) and edit the bc proxy.
- 6. Open the Advanced tab and add the new hostname of the RESEARCH machine (the FQDN or alias/CNAME) into the Host allow list. For example:

ef start v			
Writad previous Edit Writad proxy			
Virtual protes	X full virtual proxy		
R.	Anonymous access mode	No anonymous user	v
_	Authentication method	Tchet	100
	Windows authentication pattern	Windows	
	Authentication module redirect URI		
	LOAD BALANCING		
	Lead balancing nodes		
	Berver node		
		Add new server node	
	Central	(
	ADVANCED		
	Extended secol by environment	0	
		Select the checkbox to send extended information about the client environment to the engine. OS, device, browser, and IP Using extended client information will prevent shared app usage between devices and different browser types.	
	Session cookle domain		
	Has secure attribute (https)	0	
	SameSite attribute (https)	Les	<u>م</u>
	Has secure attribute (MI(p)	0	
	Samellite attribute (http)	No attribute	¥
	Additional response headers		
	Hest allow list *:		
		Add new value	
	besearch text cam		0
			-

- Click Apply.
 Navigate back to Virtual proxies and edit the Central Proxy (Default).
 Open the Advanced tab and add the new hostname of the RESEARCH machine (the FQDN or alias/CNAME) into the Host allow list. For example:





10. Click Apply.

11. When opening the Web Client or the BriefCam Administrator Console, make sure to use the new host name in the URL. For example:

http://www.test.com/app http://www.test.com/admin

Adding a New Cluster in the RESEARCH Module

This how-to provides a step-by-step description on how to build and configure a RESEARCH cluster environment. This includes a failover option between the Scheduler node and the Central and/or failover between two Central nodes to achieve high availability.

Introduction

As the amount of data grows and the business logic becomes more complex, additional resources are necessary to calculate the results and deliver them to users. If a Single Node (small) site is used, its performance may deteriorate over time, which could compromise the credibility and quality of BriefCam's RESEARCH module.

To address this issue, a RESEARCH module cluster is employed as a distributed architecture to alleviate the data and application loads from the main RESEARCH server that controls the entire RESEARCH site. The Central node, also known as the "manager", delegates some of its tasks to a secondary machine, referred to as the Scheduler node or the "worker." When receiving a task ID from the manager, the worker reads the task from the local repository database and performs the necessary computations. Once the task is completed, the worker returns the task state (successful or failed) to the manager.

Hardware Specification for the Scheduler Node

The following are the minimum requirements for the Scheduler node:



CPU	2 x Intel(R) Xeon(R) Gold 6234 CPU @ 3.30 GHz (32 vCPU)
Memory	512 GB
Storage	2 x 100 GB SSD 1 x 25.5 TB SSD capacity drives

Implementation Steps

Adding a New Cluster in the RESEARCH Module

To add a new cluster in the RESEARCH module:

- 1. Verify that the existing Qlik server is reachable from the new server by opening the following path on both the file explorer and in a browser: \\[QlikServer]\qlikshare.
- 2. Make sure that the firewall and antivirus are disabled on the new server.
- 3. Make sure that a PostgreSQL Unicode (x64) driver is installed. You will need this to create the two ODBC connections in the next step.
- 4. Add two ODBC connections RESEARCH and RESEARCHPostgreSQL.

r DSN System	DSN File	e DSN	Drivers	Tracing	Connection Pooling	About	
ystem Data Sou	rces:						
Name	F	Platform	Driver				Add
pgBriefCam	6	64-bit	Postgre	SQL Unio	ode(x64)		Permana
RESEARCHPos	tareSQL 6	54-bit	Postgre	SQL Unio		Nemove	
							Configure

ODBC connection, map the database to the BriefCam database server.

Data Source	RESEARCH	Description		
Database	briefcam	SSL Mode	prefer	~
Server	BEN-NGINX-01	Port	5432	
User Name	brief	Password	•••	
Intions				

b. For the RESEARCHPostgreSQL ODBC connection, map the database to the RESEARCH database server.

-BriefCam

PostgreSQL Ur	nicode ODBC Driver (pso	IODBC) Setup		×
Data Source Database Server User Name	SEARCHPostgreSQL QSR BEN-NGINX-03	Description SSL Mode Port	prefer 4432	
Options Datasource	Global	Passwoiu		Test Cancel

*Port 4432 is required to be opened inbound on the 1st RESEARCH machine so that the 2nd RESEARCH machine could access its Postgres database.

- 5. Create a service account user (by default, BCUser is the user that runs Qlik services). In the Computer Management, check that the user is in the Administrators group.
- 6. Make sure that the service account user created in the step above is included in the **Log on as a service** local policy:



- 7. Download the Qlik vanilla installer (located in your Git account at: https://github.com/qlik-download/qlik-sense-server/ releases). It is important that the version be the same as the version installed on the existing server.
- 8. If you are installing the Qlik May 2022 version, download and install .NET 4.8 Framework Runtime from this link: https://dotnet.microsoft.com/en-us/download/dotnet-framework/net48.
- 9. On the existing Qlik server, open the Windows services and stop all Qlik services.
- 10. Go to ProgramData\Qlik\Sense\Repository\PostgreSQL\12.5 (or any version you have) and back up the following files:





- pg_hba.conf
 pg_ident.conf
 PG_VERSION
 postgresql.auto.conf
 postgresql.conf
- 11. Edit the $pg_hba.conf$ file to allow non-local connections:

# TYPE	DATABAS	E	USER		ADDRESS			METHOD	
# IPv4 local connections:									
host	all		all		0.0.0.0/	0	md	5	
# IPv6 local connections:									
host	all		all		::0/0		ma	15	
# Allow replication connections from localhost, by a user with the									
<pre># replication privilege.</pre>									
host	replica	tion	all		127.0.0.	1/32		md5	
host	replica	tion	all		::1/128			md5	
host	all	all	0.0.0.0	/0	md5				
host	all	all	::/0	md5					

12. Edit the postgresql.conf file to accept more connections from all addresses:

```
listen_addresses = '*'
max_connections = 800
```

- 13. Start all Qlik services.
- 14. Run the Qlik installer as administrator.
- 15. Click the Join a cluster button.



16. Fill in the database credentials (of the existing Qlik server):


	Sense @ Enterprise
Enter database	credentials
To connect to an database host na	existing repository database, enter the PostgreSQL me and provide the database user password.
Database host nar	ne 🕜
ben-nginx-03	
Database port)
4432	
Database user	
qliksensereposito	ry
Database user pas	sword

17. Fill in the service account user credentials (the one defined in the new server):

Qlik 🝳	Sense® Enterprise
Provide informa	tion for the Qlik services
Settings and acco installed on the h	ount information needed for Qlik Sense services ost computer to work properly.
Windows service a	ccount credentials
Username	
ben-nginx-02\bcu	iser
Password	
******	0

- 18. After installing Qlik, install the relevant patch according to the version you are using (May 2022 or Nov 2020).
- 19. Go to the existing Qlik server and open the QMC (https://localhost/qmc).
- 20. Select Nodes.
- Click Create new in the action bar.
 Fill in the parameters as shown in the image below with the Host name field set to the hostname of the newly





IDENTIFICATION	
Name	* Scheduler
Host name	* Iben-nginx-02
	If the host name server does not have an authorized certificate, a password will be generated and displayed. Use this password to authorize the certificate on the localhost of the host name server.
NODE PURPOSE	
Node purpose	* Both
NODE CONFIGURATION	
Fallover candidate	0
Node roles	
This node has currently no roles.	
SERVICE ACTIVATION	
Repository	5
Engine	
Printing	0
Proxy	
Scheduler	
CUSTOM PROPERTIES	

- 23. Click Apply and wait several seconds.
 24. If the server cannot reach the remote host, you will see the following 'Node registration' message.

Node	registration
Req	uesting authorization password for certificate on the node.
	Close
a.	Check the connectivity between the Central node and the Scheduler node.

- b. Using ping, verify that IPV6 as well as the firewall are disabled on both nodes.
- 25. Click Apply again. Wait until you get an authorization password and a URL. The connectivity is done via port 4444.





26. Go to the new Qlik server, open the URL from the previous step: http://localhost:4570/certificateSetup and enter the password from the previous step:

2

Install certificates

Certificates have been distributed to this machine. Use the password provided in the management console to install the certificates.

Submit

Password:	
-----------	--

@ Help



- 27. On the original Qlik server (not the new cluster), restart all Qlik services.
- 28. Make sure you get the following result on the QMC's Nodes screen:

∯ Start ▼			
Nodes			
Nodes Showing: 2 Selected: 1			
Name A G	Host name 🕞	Status	1
Central	ben-nginx-03	5 of 5 services are running	0
Scheduler	ben-ngira-02	3 of 3 services are running	0

This means that there are now two Qlik servers (multi-node) – Central and Scheduler.

29. In the QMC'sSchedulers section, edit the Central node and set the Type field to Manager:



A Schedulers	🛅 Edit scheduler	
Cartoni		
	10EMTIFICATION	
	Node	Central
	LOGGINS	
	Audit activity log level	Basic w
	Sienvice log level	310 W
	TRACING	
	Application log level	346 W
	Audit tog level	Into w
	Performance log level	Into w
	Gecurity log level	into w
	System log level	300 W
	Task execution log level	340 W
	ADVANCED	*(Manazi w)
	Max concurrent reloads	a a a a a a a a a a a a a a a a a a a
	Engine timesul (inimulae)	
	CUETLAN PROPERTIES	
	Apple: Cancel	

30. In the QMC's **Schedulers** section, edit the **Scheduler** node and set the **Type** field to **Worker**:

DENTIFICATION		
lode	Scheduler	
OBGENG		Ν
udit activity log level	Basic 🖌	64 <u>9</u>
ervice log level	Into 👻	
RACING		
polication log level	Info V	
udit log level	v one	
erformance log level	Info V	
ecurity log level	Info V	
ystem log level	Info 🗸	
ask execution log level	lata Y	
DVANCED		
ype	Worker	
fax concurrent reloads	4	
ngine timeout (minutes)	30	
USTOM PROPERTIES		

31. In the QMC's **Data Connections** screen, edit the following three connections:



L

Name	Owner
ArchivedLogsFolder	sa_repository (INTERNAL\sa_repository)
AttachedFiles	sa_repository (INTERNAL\sa_repository)
DataPrepAppCache	sa_api (INTERNAL\sa_api)
ExternalData	bcuser (BEN-NGINX-03\bcuser)
monitor_apps_REST_app	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_appobject	sa_repository (INTERNAL\sa_repository)
monitor_apps_REST_event	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_license	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_license_analyzer	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_license_login	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_license_overview	sa_repository (INTERNAL\sa_repository)
nonitor_apps_REST_license_professional	sa_repository (INTERNAL\sa_repository)
monitor_apps_REST_license_user	sa_repository (INTERNAL\sa_repository)
monitor_apps_REST_task	sa_repository (INTERNAL\sa_repository)
monitor_apps_REST_user	sa_repository (INTERNAL\sa_repository)
monitor_apps_REST_user_condensed	sa_repository (INTERNAL\sa_repository)
Research	bcuser (BEN-NGINX-03\bcuser)
ResearchPostgreSQL	bcuser (BEN-NGINX-03\bcuser)
ResearchQvd	bcuser (BEN-NGINX-03\bcuser)
Scripts	bcuser (BEN-NGINX-03\bcuser)
ServerLogFolder	sa_repository (INTERNAL\sa_repository)

32. For each of the three connections, in the **Connection string** field, instead of local path (such as drive c:), change it to work with the network path – the hostname where the **QlikShare** folder exists (the server where RESEARCH was originally installed):

IDENTIFICATION		
Name		Scripts
Owner		bcuser (BEN-NGINX-03\bcuser)
Connection string	lb-	
Туре	4	folder
User ID		
Password		

- 33. On the new server, open the QMC's Tasks section and make sure that both the research_db and Research apps are running successfully.
- In QMC (central node), navigate to the Load balancing rules section.
 Double click on ResourcesOnNonCentralNodes.

Load balancing ru	nes -						
🖅 Load balanc	ing rules Showin	g: 2 Selected: 0					
Name	A 🕞	Description	G	Resource filter	G	Actions	
ResourcesOnCent	tralNode	All resources need to b	e accessibl			Load balancing	
ResourcesOnNon	CentralNodes	All resources need to b	e accessibl	App_*		Load balancing	

36. Remove the marked section shown in the image below.



	grules Ø Help
IDENTIFICATION	
Disabled	0
Name	ResourcesOnNonCentralNodes
Description	All resources need to be accessible on the non-central nodes, except the monitoring apps
BASIC	
Resource filter	App_*
Actions	Load balancing
This condition canno	ot be displayed in the rule editor because it is too complex.
ADVANCED	
ADVANCED	((node.iscentral="false" and resource.stream.id!="a70ca8a5-1d59-4cc9- b5fa-6e207978dcat]))

Forcing Manual Failover Between the Scheduler and Central Node

To force manual failover between the Scheduler node and the Central node, carry out the following steps:

1. In QMC (central server), select the Schedulers menu.





2. Select the Central scheduler and click the Edit button.

Schedulers Showing: 2 Selected: 1			
Node	Active	🕞 Status	
Central	Yes	running	0
Scheduler La	Yes	running	0
Edit			

3. In the **Advanced** section's **Type** field, select **Manager and worker**. The Central node will return to its initial state (standalone server). The Scheduler node will stop functioning as a cluster member (and eventually will not be in use).



IDENTIFICATION		
Node	Central	
LOGGING		
Audit activity log level	Basic ¥	
Service log level	Info 👻	
TRACING		
Application log level	Info 🖌	
Audit log level	Info 🗸	
Performance log level	Info 🗸	
Security log level	Info 🗸	
System log level	Info 🗸	
Task execution log level	Info 🗸	
ADVANCED		
Type	Manager	
Max concurrent reloads	Manager	
Engine timeout (minutes)	Manager Nnd worker	

Editing the Load Balancing Rule Resources on Non-Central Nodes

- From the QMC start page, open Load Balancing Rules.
 Select the ResourcesOnNonCentralNode rule and click Edit.

d Ret +													@ 14b	• •	-	
Lost heleningrates																
The Lond Informing rule	e Stowi												Arlow V			
Hane	* D	Resigner D	Branar or War	D	Artions	Ballol	в	Cantent	D	lpe	э.	Tap				Э.
Resurse Or KonGentral	-	All records and to be access.	- Aco.*		Lost telening	No.		Soft	-	Read Drip Contorn						
			1440								_					Π

3. In the Advanced section, edit the condition to the following: ((node.iscentral="false"))

4. Click Apply.



g Bat v										
Load belancing rules bo	Load belancing rules Edit load belancing rules									
👄 Edit load balancing re	des	e Help O	S Audit Recticuted	incing rules						
SDENTSPEATION Disabled Name Description EASSC Resource filter Actions This condition cannot b ADMACED Conditions		_ tqc:se	Autit Trepetressure Center Bewinnered But in hub and ONC V Center Define your audit query above and click "Audit" to begin auditing							
Unit to Qilli Sonse help-a	bout rule conventions	Adate rule								

5. Verify that after this change all QMC tasks are running okay including the License and Operations tasks.

Central Node Failover (optional)

To avoid having a single point of failure in a multi-node site, when you add a new node to your deployment you can assign it the role of failover candidate. This means that any server or node in your RESEARCH site can perform the same role as the Central node. The role of the Central node can now be swapped, for example if the central node has been offline for more than 10 minutes.

If you want to back up the Central node:

- 1. Define an additional Central server (a new Central node with the same specifications as the original node).
- 2. In QMC (of the additional Central node), select the Nodes menu and define it as a Failover candidate.

Edit node		
IDENTIFICATION		
Name		
	This field is mandatory.	
Host name		
	This field is mandetory.	
	If the host name server does not have an authorized certificate, a password will be generated and displayed. Use this password to authorize the certificate on the localhost of the host name server.	
NODE PURPOSE		
Node purpose	Production	¥
NODE CONFIGURATION		
Failover candidate		
L	when the node is a failover candidate, the engine, repository, proxy and scheduler services must be active.	

After you have configured a node to become a failover candidate, each node in your site will regularly check the primary node (Central node) to verify that the Central node is active. If there is no communication between the primary node and the other nodes in the site after 10 minutes, then the Primary node will be replaced by the next available node. If more than one node is set as a failover candidate each node will compete to get a lock on a database field and the winner becomes the Central node. There is an additional field in the QMC to show which node is currently the Central node.

Replicating the BriefCam PostgreSQL Database

This section details how to streamline the replication of the PostgreSQL database.



Prerequisites, Notes, and Conventions



Use Windows PowerShell and not Command Prompt (cmd) while pasting commands from the samples in this document.

- 1. If the primary server space is sufficient, perform a full backup of the database (using the pg_dump tool) before attempting to create the replica.
- 2. Make a note of the primary server's IP address. Later in this document it will be referred to as <primaryIP>.
- 3. Make a note of the secondary server's IP address. Later in this document it will be referred to as <secondaryIP>.
- 4. In the PGSQL server, the following three BriefCam installation components need to all be set to either the hostname or the IP address. Make sure that they are all using the same method (to ensure consistency). You do this by looking for the PostgreSQL connectionString in the following files or settings:
 - VS Server: C:\Program Files\BriefCam\BriefCam Server\VSServer.exe.config
 - Web Services: C:\Program Files\BriefCam\WebServices\ProWebApi\Web.config
 - Qlik (RESEARCH): ODBC 64-bit entries (Server field)

ODBC Data Source Adm	ninistrato	or (64-bit	t)					\times		
User DSN System DSN F	ile DSN	Drivers	Tracing	Connection	Pooling	About				
System Data Sources:										
Name	Platform	Driver					Add			
pgBriefCam RESEARCH	64-bit 64-bit	Postgre Postgre	SQL Unic SQL Unic	ode(x64) ode(x64)			Remove			
RESEARCHPORGRESGE	64-Dit	Postgre	SUL UNIC	ode(x64)			Configure			
			P	ostgreSQL Ur	nicode (DDBC D	river (psqIODBC) Setup			×
				Data Source	pgBrief	Cam	Description			
An ODBC System	m data so	urce store	es info	Database	briefca	m	SSL Mode	disable		~
A System data s	iource is v	risible to a	use	Server	10.30.3	30.22	Port	5432		
			_	User Name			Password			
				Options		C1-1-1	Marca DOM			Test
				Datasource		uiobal	Manage DSN	S	ave	Cancel

- 5. It is recommended to test the full functionality of the systems before creating the secondary server. Make sure to take note of all of the original values of the parameters you change.
- 6. On all of the servers where the BriefCam Server components are deployed, set the hosts file to point to the primary PostgreSQL database server this will override the DNS.
- 7. In the BriefCam Administrator Console, open the **Environment Settings** section and set the **DB.LocalStorageAddress** and **VideoProductsPath** settings to use hostnames and not IP addresses.
- The speed of PostgreSQL base_backup significantly varies depending on the environment setup (SSD/HDD/NIC speed). As a rule of thumb, on ISCSI storage (10 Gbps links HDD array) and 1 Gbps network NIC (vmxnet3) in a virtual environment, it takes about 40 minutes to perform a base backup of the PostgreSQL database that contains 90 GB of BriefCam data.

Consider testing the speed on the actual environment to be able to estimate how much time the base backup will take to be able to properly set the time slot for the replica creation process.

- 9. Use the actual path of the PostgreSQL_Data directory. The BriefCam default is C:\PostgreSQL_Data. However, this may vary in different setups (later in this document the default BriefCam path will be used).
- 10. Use the actual pgsql.exe path. The BriefCam default is C:\PostgreSQL\bin\psql.exe (later in this document the default BriefCam path with be used).

-BriefCam

Steps on the Primary Server

1. Connect to the primary PostgreSQL server sql shell and verify the location of the config and hba files by executing the following commands:

C:\PostgreSQL\bin\psql.exe -U dbadmin postgres

SHOW config_file;

SHOW hba_file;

Here is an example of the expected output (based on the location of the PostgreSQL Data folder):

C:/PostgreSQL_Data/postgresql.conf

C:/PostgreSQL_Data/pg_hba.conf

2. Back up the original config and hba files by executing the following commands in PowerShell:

copy C:/PostgreSQL_Data/postgresql.conf C:/PostgreSQL_Data/postgresql.conf.\$(((get-date).ToUniversalTime()).ToString("yyyyMMddTHHmmssZ"))

copy C:/PostgreSQL_Data/pg_hba.conf C:/PostgreSQL_Data/pg_hba.conf.\$(((get-date).ToUniversalTime()).ToString("yyyyMMddTHHmmssZ"))

3. Verify that the backup files were created by executing the following command:

dir C:/PostgreSQL_Data/*.conf.*

The expected output is:

PS C:\Users\Administrator> dir C:/PostgreSQL_Data/*.conf.*

Directory: C:\PostgreSQL_Data

Mode LastWriteTime Length Name

-a---- 11/10/2021 11:22 AM 4374 pg_hba.conf.20211117T100109Z

- -a---- 11/10/2021 11:25 AM 23798 postgresql.conf.20211117T100344Z
- 4. Add parameters to the postgres.conf file. You do this by opening the file in a text editor and adding the following lines to the end of the file (just below the Customized Options section):

wal_level = replica

hot_standby = on

hot_standby_feedback = on

full_page_writes = on

max wal senders = 6

max_replication_slots = 6

- 5. Create a role/user for replication and set its password (do not use the password specified in the sample commands).
 - a. Connect to the primary PostgreSQL server's SQL shell via PowerShell console using the command:

C:\PostgreSQL\bin\psql.exe -U dbadmin postgres

b. Execute the following command (in the SQL shell opened in the previous step):

CREATE ROLE repl_user LOGIN REPLICATION PASSWORD 'replQwerty123';



6. Add parameters to the pg_hba.conf file. You do this by opening the file in a text editor and adding the following lines to the file (under the #replication privilege line):

replication privilege.

host replication repl_user <secondaryIP>/32 md5

7. Restart the **BriefCamPostgreSQL** service on the primary PostgreSQL server by opening PowerShell as an administrator and running the following commands:

net stop "BriefCamPostgreSQL - PostgreSQL Server 10" net start "BriefCamPostgreSQL - PostgreSQL Server 10"

- 8. Verify that the config files contain the changes that you made to the postgres.conf file as follows:
 - a. Connect to the primary PostgreSQL server's SQL shell via PowerShell console using the command:

C:\PostgreSQL\bin\psql.exe -U dbadmin postgres

b. Print out the custom configs added to the PostgreSQL conf file using the commands below via SQL shell:

\pset pager off

SELECT pg_read_file('postgresql.conf');

c. Verify that you can now see the lines added to the postgresql.conf file at the bottom of the output.

\r		
wal	_level = replica\r	
hot	_standby = on\r	÷
hot	_standby_feedback = on\r	÷
ful	l_page_writes = on\r	÷
c max	_wal_senders = 6\r	
max	_replication_slots = 6	
(1)	ow)	
post	gres##	

- 9. Verify that the config files contain the changes that you made to the pg hba.conf file as follows:
 - a. Connect to the primary PostgreSQL server's SQL Shell by executing the following commands:

C:\PostgreSQL\bin\psql.exe -U dbadmin postgres

\pset pager off
SELECT pg_read_file('pg_hba.conf');

b. Verify that you can now see the lines added to the pg hba.conf file at the bottom of the output.

host replication all 127.0.0.1/32 host replication all ::1/128 host replication repl_user	md5\r md5\r 10.30.30/32	md5\r+				
host all all 0.0.0.0/0 host all all ::0/0	md5\r md5\r	* + +				
1 row)						

Steps on the Secondary Server

- 1. Install BriefCamPostgreSQL.
- 2. On the secondary PostgreSQL server, stop the **BriefCamPostgreSQL** service by running the following in PowerShell as an administrator:

net stop "BriefCamPostgreSQL - PostgreSQL Server 10"

- 3. Clean the data directory as follows:
 - a. Rename the PostgreSQL_Data folder.
 - b. Create a new folder named PostgreSQL_Data and in the folder's **Permissions** tab, add **Full control** to **Everyone**.

-BriefCam



- 4. Perform a PostgreSQL basebackup from the primary to the secondary server as follows:
 - a. Execute the following command in PowerShell as an administrator:

c:\PostgreSQL\bin\pg_basebackup -h <primaryIP> -U repl_user --checkpoint=fast -D C:\PostgreSQL_Data -R

TBD #--slot=standby1

- b. It is recommended to stop all the BriefCam services on all the servers during the potentially long database backup. It's possible to perform this step without stopping all services, depending on the dataset size.
- 5. On the secondary PostgreSQL server, start the BriefCamPostgreSQL service by executing the following commands in PowerShell as an administrator:

net start "BriefCamPostgreSQL - PostgreSQL Server 10"

Verify the Replication Operation

1. Connect to the primary PostgreSQL server's SQL shell via PowerShell console using the command:

C:\PostgreSQL\bin\psql.exe -U dbadmin postgres

2. Check the lag value by running the following command in SQL shell (the write_lag value must begin with 00:00:00):

SELECT write_lag,client_addr FROM pg_stat_replication ;

This is an example of the expected output:





postgres=# SELECT write_lag,client_addr FROM pg_stat_replication ; write_lag | client_addr

00:00:00.003972 | 10.30.30.30 (1 row)

postgres=#



This check needs to be performed at least once per day.

Activate the Secondary Server to Act as Primary Server

This section describes the procedure of activating the secondary server as the primary instance of the PostgreSQL database, in cases where the primary is at fault and recovery/migration is needed.

- 1. Change the hosts file in all BC servers to reflect the <secondaryIP> instead of <primaryIP>.
- 2. Check the status and promote the secondary server PGSQL to become the primary server by running the following commands in PowerShell console (make sure to run PowerShell in administrator, and to edit the paths to the pg_ctl.exe file and the PostgreSQL_Data folder accordingly):
 - c:\PostgreSQL\bin\pg_ctl.exe status -D "C:\PostgreSQL_Data"

Sample output:

pg_ctl: server is running (PID: 5672)

C:\PostgreSQL\bin\postgres.exe "-D" "C:\PostgreSQL_Data"

c:\PostgreSQL\bin\pg_ctl.exe promote -D "C:\PostgreSQL_Data"

Sample output:

waiting for server to promote.... done server promoted

Create Periodic Backup on the Secondary Server

PG_DUMP Scripts in Windows Task Scheduler

 Create the %APPDATA%\postgresql\pgpass.conf file containing the db credentials (that is: *:5432:*:dbadmin:Qwerty123). For details, refer to: https://www.postgresql.org/docs/10/libpq-pgpass.html and https://www.postgresql.org/docs/10/libpq-envars.html (external links).

If the above does not work, the password of the scripts can be specified on the execution line:

\$env:PGPASSWORD='Qwerty123';& c:\PostgreSQL\bin\pg_dump.exe -F t -U dbadmin -d briefcam -f e:\PostgresB
ackups\db_briefcam-\$(((get-date).ToUniversalTime()).ToString("yyyyMMddTHHmmssZ")).tar

- 2. Create a folder for backup files, for example: E: \PostgresBackups \.
- 3. Create a folder for the backup script files, for example: E:\PostgresBackupScripts\.
- 4. Create the backup script at: E:\PostgresBackupScripts\backup.ps1 with the three commands as shown below:
 - c:\PostgreSQL\bin\pg_dump.exe -F t -U dbadmin -d postgres -f e:\PostgresBackups\db_postgres-\$(((getdate).ToUniversalTime()).ToString("yyyyMMddTHHmmssZ")).tar
 - c:\PostgreSQL\bin\pg_dump.exe -F t -U dbadmin -d briefcam -f e:\PostgresBackups\db_briefcam-\$(((getdate).ToUniversalTime()).ToString("yyyyMMddTHHmmssZ")).tar
 - #ls -file E:\PostgresBackups\db*.tar | where {(get-date) \$_.creationtime -gt 15.} | Remove-Item –Verbose



*The 3rd command above should be adjusted according to the required backup retention period by removing the "#" sign at the start of the line and modifying the number 15 as it represents the number of days backwards. For example, if you wish to configure the script to delete all files older than 7 days, you would have to change the number 15 to 7.

5. Test the backup creation and the removal of the old files by setting the -gt to 0 and run the following command in Windows cmd:

powershell.exe e:\PostgresBackupScripts\backup.ps1

```
C:\Users\Administrator>powershell.exe e:\PostgresBackupScripts\backup.ps1
VERBOSE: Performing the operation "Remove File" on target "E:\PostgresBackups\db_briefcam-20211122T1157392.tar".
VERBOSE: Performing the operation "Remove File" on target "E:\PostgresBackups\db_briefcam-20211122T1157422.tar".
VERBOSE: Performing the operation "Remove File" on target "E:\PostgresBackups\db_briefcam-20211122T11570422.tar".
VERBOSE: Performing the operation "Remove File" on target "E:\PostgresBackups\db_priefcam-20211122T1157042.tar".
VERBOSE: Performing the operation "Remove File" on target "E:\PostgresBackups\db_postgres-20211122T1157092.tar".
VERBOSE: Performing the operation "Remove File" on target "E:\PostgresBackups\db_postgres-20211122T1157422.tar".
VERBOSE: Performing the operation "Remove File" on target "E:\PostgresBackups\db_postgres-20211122T1157422.tar".
VERBOSE: Performing the operation "Remove File" on target "E:\PostgresBackups\db_postgres-20211122T1157422.tar".
```

This will remove all the files created.

- 6. Adjust the retention period of the backups as mentioned at the bottom of step 4 above.
- 7. Add the backup script to the Windows task scheduler as follows:
 - a. Set the **Program/script** field to the following path:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

b. In the Add arguments field set the following: E:\PostgresBackupScripts\backup.ps1

Edit Actio	n	×
You mus	t specify what action this task will perform.	
Action:	Start a program	~
Settings	;	
Progra	m/script:	
dows\?	System32\WindowsPowerShell\v1.0\powers	hell.exe Browse
Add ar	guments (optional):	3ckupScripts\backup.ps1
Start in	n (optional):	

8. Set the triggers and timing accordingly.



the second se			×
Task Scheduler L	Library		× Run Time
	General Triggers	Actions Conditions Settings	2022 11:33:3
	When you create	New Trigger	×
	Tringer	Begin the task: On a schedule ~	
	ingger	Settings	
		One time Start: 2/23/2022 419:18 PM Start: 5 Oneily Weekly Monthly	ynchronize across time zones
	New	Advanced settings Delay task for up to (random delay): 1 hour Repeat task every: 1 hour Stop all running tasks at end of repetition duration Stop task if it runs longer than: 3 days Expire: 2/23/2023 4:19:18 PM Synchr	on of: 1 day v
t the task to postgres-bac	Security options- When running the run regardless if the ckup Properties (Local Cor	user is logged in and save the password.	OK Cancel
t the task to postgres-bac General Trigg	run regardless if the ckup Properties (Local Cor gers Actions Conditions	user is logged in and save the password.	OK Cancel
t the task to postgres-bac General Trigg Name:	Security options- When summing the run regardless if the ckup Properties (Local Cor pers Actions Conditions postgres-backup	user is logged in and save the password. nputer) Settings History	OK Cancel
t the task to postgres-bac General Trigg Name: Location:	Security options- When running the run regardless if the ckup Properties (Local Cor gers Actions Conditions postgres-backup	user is logged in and save the password.	OK Cancel
t the task to postgres-bac General Trigg Name: Location: Author:	PAUL-BC1-DB-02\Admin	user is logged in and save the password.	OK Cancel
t the task to postgres-bac General Trigg Name: Location: Author: Description:	Security options- When nunning the run regardless if the ckup Properties (Local Cor gers Actions Conditions postgres-backup AUL-BC1-DB-02\Admin	user is logged in and save the password.	OK Cancel
t the task to postgres-bac General Trigg Name: Location: Author: Description:	PAUL-BC1-DB-02\Admin	user is logged in and save the password.	OK Cancel
t the task to postgres-back General Trigg Name: Location: Author: Description: Security opting	Security options- When running the ckup Properties (Local Cor gers Actions Conditions postgres-backup N PAUL-BC1-DB-02\Admin	user is logged in and save the password. Settings History strator Task Scheduler Enter user account information for runn User name: GBC1-08-02V	OK Cancel
et the task to postgres-bac General Trigg Name: Location: Author: Description: Security opti When runnin PALL PC 1	PAUL-BC1-DB-02\Admin Administrations PAUL-BC1-DB-02\Admin PAUL-BC1-DB-02\Admin	user is logged in and save the password. Settings History strator Task Scheduler Enter user account information for runn User name: @ -BC1-DB-02V Password:	OK Cancel
et the task to postgres-bac General Trigg Name: Location: Author: Description: Security opti When runnin PAUL-BC1-D	Security options- When experies the ckup Properties (Local Cor gers Actions Conditions postgres-backup N PAUL-BC1-DB-02\Admin ons ing the task, use the follow DB-02\Administrator	user is logged in and save the password. Settings History strator Task Scheduler Enter user account information for runn User name: Basword:	OK Cancel
t the task to postgres-bac General Trigg Name: Location: Author: Description: Security opti When runnin PAUL-BC1-E O Run only	PAUL-BC1-DB-02\Admin Tun regardless if the Ckup Properties (Local Cor pers Actions Conditions postgres-backup A PAUL-BC1-DB-02\Admin ions Ing the task, use the follow DB-02\Administrator I when user is logged on	user is logged in and save the password. Settings History strator Task Scheduler Enter user account information for runn user name: Benter user account information for runn User name: Benter user account information for runn Compared Benter user account information for runn Compared Benter user account information for runn Setting user account: Setting User name: Setting Benter user account information for runn Setting User name: Setting Benter user account information for runn Setting User name: Setting Benter user account information for runn Setting User name: Setting Benter user account information for runn Setting User name: Setting Benter user account information for runn Setting User name: Setting Benter user account information for runn Setting User name: Setting Benter user account information for runn Setting User name: Setting Benter user account information for runn Setting User name: Setting Benter user account information for runn Setting User name: Setting Benter user account information for runn Setting Benter user account informati	OK Cancel
t the task to postgres-back General Trigg Name: Location: Author: Description: Security opti When running PAUL-BC1-E O Run only Run when Do no	Security options- When running the ckup Properties (Local Cor- gers Actions Conditions postgres-backup N PAUL-BC1-DB-02\Admin M PAUL-BC1-DB-02\Admin M M PAUL-BC1-DB-02\Admin M M PAUL-BC1-DB-02 M M M M M M M M M M M M M M M M M M M	user is logged in and save the password. Settings History strator Task Scheduler Enter user account information for runni ing user account: User name: @ -BC1-DB-02\ Password: OK	OK Cancel
the task to postgres-bac General Trigg Name: Location: Author: Description: Security opti When runnin PAUL-BC1-D Run only Run when Do no Run with	PAUL-BC1-DB-02\Admin PAUL-BC1-DB-02\Admin run regardless if the ckup Properties (Local Cor pers Actions Conditions postgres-backup Actions Conditions PAUL-BC1-DB-02\Admin ions ing the task, use the follow DB-02\Administrator rwhen user is logged on or n ther user is logged on or n	user is logged in and save the password.	OK Cancel

10. On a test server, check if the files are restorable. This test should be part of your ongoing routine.

Here is an example of the restore command:

C:\PostgreSQL\bin\pg_restore.exe -c -v -U dbadmin -d briefcam -F t e:\PostgresBackups\db_briefcam-20211122T122052Z.tar

The parameter -c performs drop and create. For additional options see:





"C:\PostgreSQL\bin\pg_restore.exe --help"

Revert to Primary Server After It Is Fixed

If you were using a secondary server because there was an issue with the primary server, this section describes how to revert to the primary server once the issue is fixed.

Ø

The details of the process below may vary depending on what kind of failure the primary server suffered. To consider the most severe case (an absolute crash of the primary server), the steps below include a fresh installation.

- 1. Install the operating system from scratch.
- 2. Perform the steps from the Steps on the Primary Server section on the current primary server.
- 3. Perform all the actions described in the sections below on the servers, considering that the server that was reinstalled is now technically the "secondary" instance:
 - Steps on the Secondary Server
 - Verify the Replication Operation
 - Activate the Secondary Server to Act as Primary Server
- 4. Stop the PostgreSQL service on the server that was used as the primary server.
- 5. Verify that the BriefCam system works properly.
- 6. Perform steps for creating a replica on the server that was used as the primary server.

Installation and Troubleshooting Tools

Check Prerequisites Tool Move Storage Tool Server Hostname Change Tool Configure Server Logging Tool

Log Collector Tool

Installation Troubleshooter

Check Prerequisites Tool

The Check Prerequisites tool checks that the hardware and operating system parameters on a machine meet the BriefCam's prerequisites before running the BriefCam installers.

The Check Prerequisites tool (BriefCamCheckPrerequisites) is available for download from BriefCam's Installation Downloads page. From the Select Product list, select Additional Tools and then select the relevant BriefCam version.

Run the .exe file, select the components that you will be installing on the machine, and click Run.

The tool presents you with a list of the minimum prerequisites checked and you whether your machine meets the minimum prerequisites.

Move Storage Tool

The Move Storage tool updates the BriefCam shared directory to another location and a different name (when required).

The tool can be found at: {BriefCam Server installation folder}\tools\move_storage_tool.

-=BriefCam



The config file is available by contacting BriefCam's support.



The tool assumes that all data is saved in one location.

Prerequisites

Before execution it is highly recommended to:

- Back up the Postgres database.
- Remove previous shared folder mapping (if you want to use the same shared folder name).

Parameters

The following are the parameters that can be used:

Deremeter	Description			
Parameter	Description	Optional		
-share-path {SHARE_PATH}	Path to new share. SHARE_PATH can be a regular path, such as: "c:\path\to\my\new\share" or a network path, such as: "\\host-name\share-name". If it is a regular path, a new shared directory will be created. If it is a network path, it is assumed that this path is already shared under the required permissions and therefore will not be recreated.	required		
-share-name {SHARE_NAME}	New shared folder name	not required if network path is given		
-share-host {SHARE_HOST}	New shared folder host	not required in local execution		
-db-port {DB_PORT}	Database port	required		
-db-user {DB_USER}	Database username	required		
-db-pwd {DB_PWD}	Database user password	required		
-local		required for local operation		



-config {CONFIG} Path to a JSON config file for remote execution. Contains the machines that belong to a certain BriefCam installation.

required for remote operation

Running the Tool

To run the tool from an **all-in-one** machine:

- 1. Extract the move-storage.zip file.
- 2. Open PowerShell as administrator.
- 3. Run the tool from within the directory where you extracted the tool.
- 4. The tool does not move the data. Therefore, after running the tool, you need to move the data to the new location.

To run the tool from a **remote** machine:

- 1. Extract the move-storage.zip file.
- 2. Update the config.json file with your hosts and credentials.
- 3. Enable and allow WINRM and ICMP in the firewall administrator-level credentials of the remote machines.
- 4. On every machine, enable the running of PowerShell remote-signed scripts. For additional information, see High Security Environment with Customized Policy Settings.
- 5. Open PowerShell as administrator.
- 6. Run the tool from within the directory where you extracted the tool.
- 7. The tool does not move the data. Therefore, after running the tool, you need to move the data to the new location. First move the Backups folder (located at: \\server\BriefCam\ServerData\Backups) and the RESEARCH certificates (located at: \\server\BriefCam\certificates). Then move the rest of the data.
- 8. Enable BriefCam's Maintenance service.

The move-storage.log file is available for troubleshooting this tool (located in the directory of the tool).

Examples

Here are a number of examples:

For local execution with a standard path:

PS> ./move-storage.exe -local -share-path 'C:\my\new\share' -share-name 'shary' -db-port 5432 -db-user 'bb' -db-pwd 'king'

For local execution with a network path:

PS> ./move-storage.exe -local -share-path '\\MyMachine\MyShare' -db-port 5432 -db-user 'bb' -db-pwd 'king'

Note that with the network path the share name is not needed and will be ignored even if given explicitly.

Server Hostname Change Tool

This tool makes changes to an all-in-one environment after a server hostname change. Note that this tool does not make changes to the RESEARCH component or to RabbitMQ.

Note: It is highly recommended not to change the server hostname if you are using the RESEARCH component.

The tool (BriefCamUpdateHostname) is available at: {BriefCam Server installation folder}\tools\ change hostname.

To work with the tool:



- 1. Change the machine's host name. (Make a note of the original host name because you will need it in step 4.)
- 2. Restart the machine.
- 3. Reshare the BriefCam share.
- 4. Open PowerShell as admin.
- 5. Run the following command:

.\update_hostname.exe /qn NEW_HOSTNAME="{the new host name}" OLD_HOSTNAME="{the old host name}" P OSTGRES_BC_USER="{the BC application user for connecting to the DB}" POSTGRES_BC_PASSWORD="{the p assword for BC application user}" LOG_NAME="{the file name for the application log}" /L*V "{path for verbose loggin g of the tool}"

The LOG_NAME parameter controls the name of the log the tool generates for tracking what was changed. This log is saved in the %APPDATA%\briefcam folder.

- The machine will be restarted by the installer after the tool has finished running.
- 6. Uninstall RabbitMQ using the Windows Add/Remove Programs option.
- 7. Reinstall the RabbitMQ component.

Configure Server Logging Tool

This tool lets you update the configuration of the BriefCam Server's log files (Logconfig.xml) from one location.

The tool can be found at: {BriefCam Server installation folder}\tools\log configuration tool.

This tool includes a config.json file that lists all the appenders and elements to be updated. When it runs on the target machine it discovers the location where the BriefCam Server was installed and replaces the values according to the config file.

To run this tool:

- 1. Copy both the configure.ps1 and config.json files to the target machine.
- 2. Update the config.json file with the changes that you want to make to the log configuration files.
- 3. Open PowerShell as an administrator.
- 4. Run the configure.ps1 file.

Log Collector Tool

The Log Collector is a tool for collecting relevant logs from a BriefCam deployed system. Once you run the tool, you'll have a compressed file for each machine in an output directory.

Logs related to the following are collected:

- BriefCam services
- IIS
- db-config
- db-tool

The Log Collector tool (collect-logs) can be found at: {BriefCam Server installation folder}\tools\ log collector tool.

To run the tool from an all-in-one machine:

- 1. Extract the collect-logs.zip file.
- 2. Open PowerShell as administrator.
- 3. Run the utility from within the directory where you extracted the tool.

To run the tool from a remote machine:

- 1. Extract the collect-logs.zip file.
- 2. Update the config.json file with your hosts and credentials.
- 3. Enable and allow WINRM and ICMP in the firewall administrator-level credentials of the remote machines.
- 4. On every machine, enable the running of PowerShell remote-signed scripts. For additional information, see High





Security Environment with Customized Policy Settings.

- 5. Open PowerShell as administrator.
- 6. Run the utility from within the directory where you extracted the tool.

The following are the parameters that can be used:

Parameter	Туре	Description	Required/Optional	Comment
-config	string	path to configuration file	required when running from a remote machine	default: './config.json'
-start	string	start date	optional	Format: 'yyyy-MM-dd'. If omitted, no start date is assumed.
-end	string	end date	optional	Format: 'yyyy-MM-dd'. If omitted, today's date is assumed (inclusive).
-local	flag		required in case of local collection only	
-0	string	compressed archived output directory	optional	default: current working directory. If the given path does not exist, it will be created.

Here are a number of examples:

For local collection:

PS> ./collect-logs.ps1 -local -start 2021-08-01 -end 2021-10-23

For remote collection:

PS> ./collect-logs.ps1 -config "./config.json" -start 2022-01-01 -o "c:\path\to\keep\logs"

There are a number of log files available for troubleshooting the Log Collector:

- c:/windows/temp/_collect.log on every remote collected machine
- <UTILITY-DIRECTORY>/_collect.log when running the tool locally
- <UTILITY-DIRECTORY>/deploy.log, <UTILITY-DIRECTORY>/deploy-trace.log on the machine the utility runs from

Installation Troubleshooter

To extract all existing environment properties needed for the successful installation of BriefCam, use the Installation Troubleshooter tool. This tool can be used with the following operating systems: Server 2012, Server 2016, Windows 10, and Windows 11.

- Go to {BriefCam Server installation folder}tools and copy the installation_troubleshooter folder with all its content to a running directory.
- 2. Run the installation_troubleshoot.bat file with administrator privileges.
- 3. For information about the BriefCam Administrator Console settings, open the db_tool_input.txt file.

Local Disk (C:) > Program Files > BriefCam > BriefCam Server > Tools > InstallationTroubleshooter > bin					
	Name	Date modified	Туре	Size	
A A	init .pv	6/29/2020 3:25 AM	PY File	0 KB	
	db_tool_input	6/29/2020 3:25 AM	Text Document	1 KB	
	installation_troubleshoot	6/29/2020 3:25 AM	Windows PowerS	24 KB	

4. Add or remove the settings that you want to retrieve from the BriefCam Administrator Console.





🔚 db_to	ool_input.txt 🔀			
1	DB.LocalStorageAddress			
2	General.AdminWebAPIAddress			
3	ProWebApiAddress			
4	ProWebClientAddress			
5	Product.ResearchReports			
6	QlikApplicationId			
7	QlikCertPath			
8	QlikServer			
9	FrameTimeoutMS			
10	VideoProcessingGateWayUrl			
11	QlikCertPsw			

5. In the running directory, see the <hostname>__out__<date-time>.txt and the installation troubleshoot.log files.

For additional information, see the README file.

Distributed Architecture



All BriefCam components can be installed on one machine (all-in-one) or the components can be distributed across several machines.

In general, to ensure a fast, real-time user experience with high capacity loads, use dedicated machines for the following components: Rendering, RESEARCH, Database, Storage and Processing Servers.

For example, if your deployment is RESEARCH-focused, install the RESEARCH component on a separate machine.

For additional information, see the BriefCam High Availability Deployment white paper.

See also the Required Configuration per Machine Type section.

Required Configuration per Machine Type

The table below details what needs to be installed on an all-in-one machine.



Machine Type	BriefCam Installers	Other Requirements	Services to Enable (BriefCam Administrator Console)	Activate License
All-in-one	 Database Rabbit MQ Server RESEARCH Web Services VMS Integration plugins 	 Compatible NVIDIA GPU VMS SDKs if required 	All	Yes

Below is an example of a distributed environment with six machines.

#	Machine Type	BriefCam Installers	Other Requirements	Services to Enable (BriefCam Administrator Console)	Activate License
1	VS Server	 Database Rabbit MQ Server Web Services VMS Integration plugins NGINX 	• VMS SDKs if required	 Fetching Service Rendering Service Lighthouse Service Maintenance Service Notification Service Task Management Service Video Streaming Gateway Service VS Server Service VS Server Service VMS Integration services 	Yes
2	RESEARCH	RESEARCH		_	_
3	Processing Servers (x2)	 VMS Integration plugins 	 A single or multiple dedicated NVIDIA GPU for each Processing Server VMS SDKs if required 	 Processing Service VMS Integration services 	_
4	Alert Processing Server	 VMS Integration plugins 	 A single or multiple dedicated NVIDIA GPUs for each Alert Processing Server VMS SDKs if required 	 Alert Processing Service VMS Integration services 	_



Installation Guide: Appendix

Installed Prerequisites

Installed Services

-BriefCam

Installed Prerequisites

The installation checks for the following prerequisites. (BriefCam will install them for you if they do not exist. You do not need to install them manually):

PostgreSQL

- Microsoft Visual C++ 2013 Redistributable Package (x64) 12.0.40649
- Microsoft Visual C++ 2015 2017 2019 Redistributable Package (x64) 14.34.31931
- Microsoft .NET Core Runtime 3.1.0 (x64)
- PostgreSQL 15
- Redis5_Windows64 5.0.10

RabbitMQ

- Microsoft Visual C++ 2013 Redistributable (x64) 12.0.40649
- Erlang/OTP 23
- RabbitMQ Server

BriefCam Server

- Microsoft Visual C++ 2010 SP1 Redistributable Package (x64)
- Microsoft Visual C++ 2012 Redistributable Package (x64)
- Microsoft Visual C++ 2013 Redistributable Package (x64)
- Microsoft Visual C++ 2015 2017 2019 Redistributable Package (x64)
- Microsoft .NET Framework 4.7.2 Full
- Microsoft .NET Core 3.1
- Microsoft ASP .NET Core 3.1

RESEARCH

- BriefcamPostgreSQL_ODBC_Driver
- Qlik Sense May 2022
- Qlik Sense May 2022 Patch 16

-BriefCam



Web Services

- Microsoft Visual C++ 2010 SP1 Redistributable Package (x64)
- Microsoft Visual C++ 2012 Redistributable Package (x64)
- Microsoft Visual C++ 2013 Redistributable Package (x64)
- Microsoft Visual C++ 2015 2017 2019 Redistributable Package (x64)
- Microsoft IIS Installer for BriefCam Web Services
- Microsoft .NET Framework 4.7.2 Full
- Microsoft .NET Core 3.1
- Microsoft ASP .NET Core 3.1
- IIS URL Rewrite

Milestone Embedded Client

- Microsoft .NET Framework 4.7.2 Full
- Microsoft Visual C++ 2010 SP1 Redistributable Package (x64)
- Microsoft Visual C++ 2012 Redistributable Package (x64)
- Microsoft Visual C++ 2013 Redistributable Package (x64)
- Microsoft Visual C++ 2015 2017 2019 Redistributable Package (x64)

Genetec Security Center Embedded Client

- Microsoft .NET Framework 4.7.2 Full
- Microsoft Visual C++ 2010 SP1 Redistributable Package (x64)
- Microsoft Visual C++ 2012 Redistributable Package (x64)
- Microsoft Visual C++ 2013 Redistributable Package (x64)
- Microsoft Visual C++ 2015 2017 2019 Redistributable Package (x64)

Installed Services

When you install the BriefCam Server, the following services and servers are installed on the same machine as the server. These services are centrally managed from the BriefCam Administrator Console's **Hosts** section. For detailed information about these services, see the BriefCam High Availability Deployment white paper.

VSServer Service

The VSServer service is responsible for various maintenance and monitoring-related activities:

- · Watchdogging the RESPOND tasks in case of a task failure
- · Creating new RESPOND tasks when a rule is created or modified by the user
- · Provides live image for the RESPOND task configuration wizard
- · Provides the list of cameras for the Web Admin's Camera Activation dialog
- · Creates the scheduled RESEARCH tasks
- Sends the outbound alerts to the outbound API and also sends alerts to the VMS clients that have real-time alerts integration (level 2a or above)
- · Triggers the data maintenance activity
- Clears inactive sessions

The VSServer service can only run on one host. If you want this service to run on a different host, you need to first stop the service and uncheck the service's checkbox from the host's Enable Services screen.





Fetching Service

The Fetching service is responsible for fetching the videos from the video management system (VMS).

When connecting to VMS systems that license per client concurrent connection, the system integrator must obtain the required number of licenses to support the number of deployed fetching services.

By default, a Fetching service is configured to use two concurrent workers. Regardless of the number of workers, one license is required for each Fetching service.

The fetching request is divided into five-minute tasks. For example, if one-hour of video was requested, the system generates 12 tasks of five minutes each. The two workers will handle the queue until the entire video is fetched.

The number of workers can be modified from the Web Admin's Environment Settings section by modifying the value of the Fetching.NumberOfWorkers setting. This setting can be configured to any number as long you validate that the VMS is capable of serving the necessary number of clients for fetching videos from the archiver.

Filtering Service

The **Filtering** service is responsible for handling in-memory object filtering for various scenarios in all the modules (REVIEW, RESPOND, and RESEARCH). In general, filtering relies heavily on the CPU of the filtering server and on DB read transactions. To define the filtering workers' count, modify the **FilteringDegreeOfParallelism** environment setting.

Task Management Service

The Task Management service is responsible for:

- Sending processing tasks to the processing servers (task management) for the OX6 engine. For the OX5 engine, the VSServer is responsible for task management.
- · Updating case and request task statuses for the REVIEW dashboard.

Face Recognition Service

The Face Recognition service is responsible for the following activities:

- · Monitoring the external watchlist folders for new face images
- Providing the aggregated status of uploaded face images for the web UI

Face Recognition Matching Service

The Face Recognition Matching service is responsible for comparing face queries to watchlists in order to find matches for filtering in the REVIEW module and for RESPOND alerts. This processing is done in-memory.

LPR Matching Service

The License Plate Recognition (LPR) Matching service is responsible for processing license plates to find matches for filtering in the REVIEW module and for RESPOND alerts.

Lighthouse Service

The Lighthouse service is the seed node of BriefCam's Akka cluster. Its main roles are:

- · Registering new services that join the cluster.
- · Providing service-discovery capability for all the other services in the cluster.





BriefCam's Akka cluster consists of the following services:

- LPR Matching
- BI Face Recognition
- Face Recognition Matching
- Filtering

If an Akka service starts while the Lighthouse service is not available, the service will wait for the Lighthouse service and attempt to register to the BriefCam cluster every 10 seconds.

Rendering Service

The Rendering service is responsible for the following:

- Generating visual and video artifacts for the web client, such as rendering the synopsis videos and visual layers, exports and original videos
- Validating uploaded video files before processing

By default, a rendering service is configured to use eight concurrent connections. This default value can be modified in the BriefCam Administrator Console's **Server.VideoRenderServerWorkers** environment setting.

BI Rule Engine Service

The BI Rule engine is responsible for preparing the extracted objects' metadata for the BI engine.

BI Face Recognition Service

The BI Face Recognition service is responsible for advanced face matching functionalities used in RESEARCH. The service monitors faces detected in RESEARCH's camera source groups and combines separate face detections from various cameras and at different times into identities that can be queried effectively to correlate between people appearing in different cameras.

Processing Server Service

The Processing Server service is responsible for on-demand video processing (REVIEW and RESEARCH modules).

Alert Processing Server (APS) Service

The Alert Processing Server service is responsible for real-time video processing (RESPOND and real-time RESEARCH).

Notification Service

The Notification service is responsible for managing all aspects of notification and message delivery between the client application and the server side.

Maintenance Service

The Maintenance service is responsible for running BriefCam's automatic maintenance processes. For more information about maintenance, see the Maintenance and Data Retention section of the **BriefCam Administrator Guide**.

The name of this service in the Task Manager and in the Windows file system is HouseKeepingService.





Storage Gateway Service

The Storage Gateway service is responsible for accessing BriefCam's storage where accessing any storage artifact requires a valid authenticated session.

This service is available when the **UseStorageGateway** environment setting is set to **true**. The default for this setting is **false**. For additional information about using this service, see the <u>Security Settings</u> section in the **BriefCam Administrator Guide**.

Since version: 2023 M1 SP1

Telemetry Agent

This service is for internal use by the Support team.

Since version: 2023 M1 SP1

Services for the Next-Gen Engine

The following services are available for use with the Next-Gen engine:

- OX6.Engine Service
- OX6.Engine Gateway Service
- OX6.Visual Assets Service
- OX.VMS Adaptor
- Task Management

For additional information, see the BriefCam Next-Gen Engine document.

In multi-site deployments, the following services are also available:

Multi-site Site BI Export Service

This Site service transmits RESEARCH data from the sites to the Hub.

The name of this service in the Task Manager and in the Windows file system is BIHubExportService.

Multi-site Hub BI Data Gateway

This Hub service collects RESEARCH data from the sites associated with the Hub.

The name of this service in the Task Manager and in the Windows file system is HubExportGateway.

Multi-site Hub SSO Gateway

This Hub service enables Hub users to play original videos of alerts triggered from the sites.

The name of this service in the Task Manager and in the Windows file system is BriefCam.HubSSOGateway.

Outbound API Gateway

This Hub service collects RESPOND alerts from the sites and if needed, sends them to a third party service.

About BriefCam

BriefCam® is the leading provider of video analytics software that enables people, companies, and communities to unlock the value of video surveillance content. Delivering accurate, flexible, and comprehensive solutions, BriefCam's video analytics platform provides valuable insights for accelerating investigations, increasing situational awareness and enhancing operational intelligence.

For more information about BriefCam's video content analytics solutions, visit https://www.briefcam.com