MAKE THE
WORLD SEE

Milestone Systems

XProtect® Rapid REVIEW

Installation and deployment guide

milestone

Contents

Copyright, trademarks, and disclaimer

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

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.

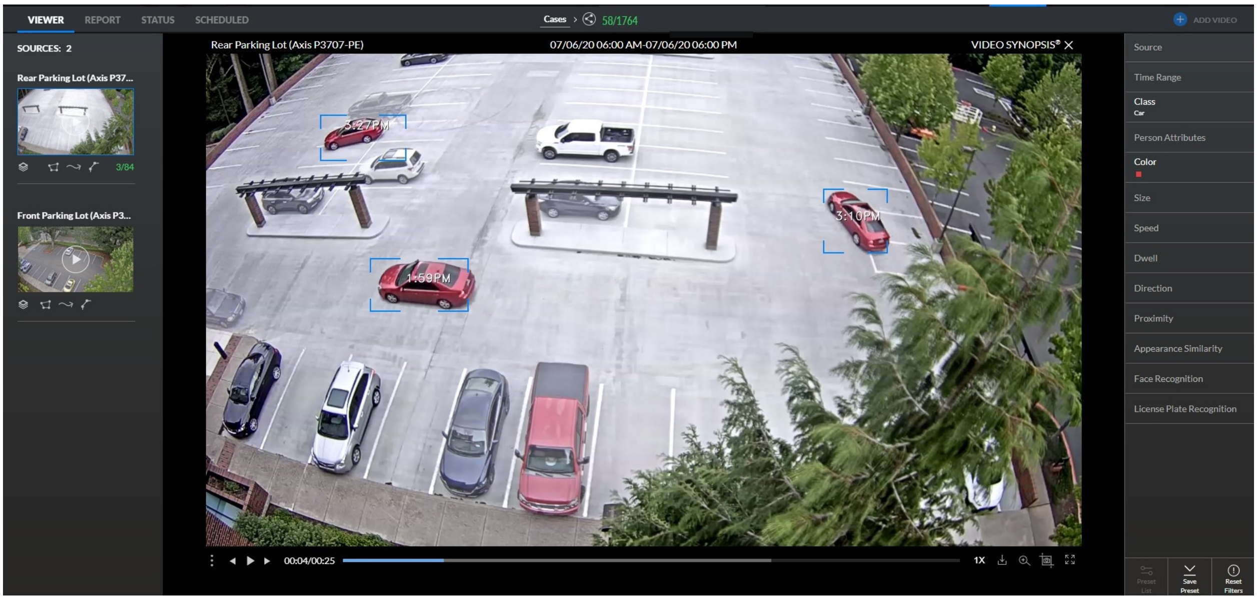
This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file 3rd_party_software_terms_and_conditions.txt located in your Milestone system installation folder.

XProtect Rapid REVIEW

This Installation and deployment guide outlines the installation and deployment of XProtect Rapid REVIEW for rapid time-to-value.

Get started and accelerate investigations with XProtect Rapid REVIEW

- Review hours of video in minutes with VIDEO SYNOPSIS®
- Pinpoint objects of interest with robust multi-camera search capabilities supporting 29 classes and attributes, face recognition, appearance similarity, color, size, speed, path, direction, and dwell time
- Quickly and effectively organize all video assets of an investigation with collaborative case management
- Rapidly visualize activity level, dwell time, common paths and background changes with powerful visual layers



Installation and deployment steps

1. Installation prerequisites
2. Run the installation script
3. Activate the BriefCam license
4. Set up the deployment
5. Define and activate the cameras
6. Disable face recognition and license plate recognition (optional)
7. Update the SSO address
8. Install BriefCam Embedded Client for Milestone XProtect plug-in
9. Using an HTTPS host (optional)

STEP 1 - Installation prerequisites

1. Download a supported version of the NVIDIA driver (461.72 or higher). For the Tesla family of cards, the supported versions are 461.33 or higher.
2. If the computer is running Windows 10 or Windows Server 2016, download and install .NET Framework 4.7.2 Runtime or higher. Lastly, another thing that came up in the Tech Training that ought to be mentioned is that the installation may error out if the default system language is not set to English. I'd include this as an Installation prerequisite in section 1. Users can set this back to their preferred system language after installation.
3. Set the default system language to English during the installation. If the language is a language other than English, the installation may end with an error. The system language can be set to any preferred language after the installation.
4. Disable antivirus scans from all BriefCam folders. For more information, see the Antivirus guidelines from BriefCam.
5. Restart the computer.

STEP 2 - Run the installation script

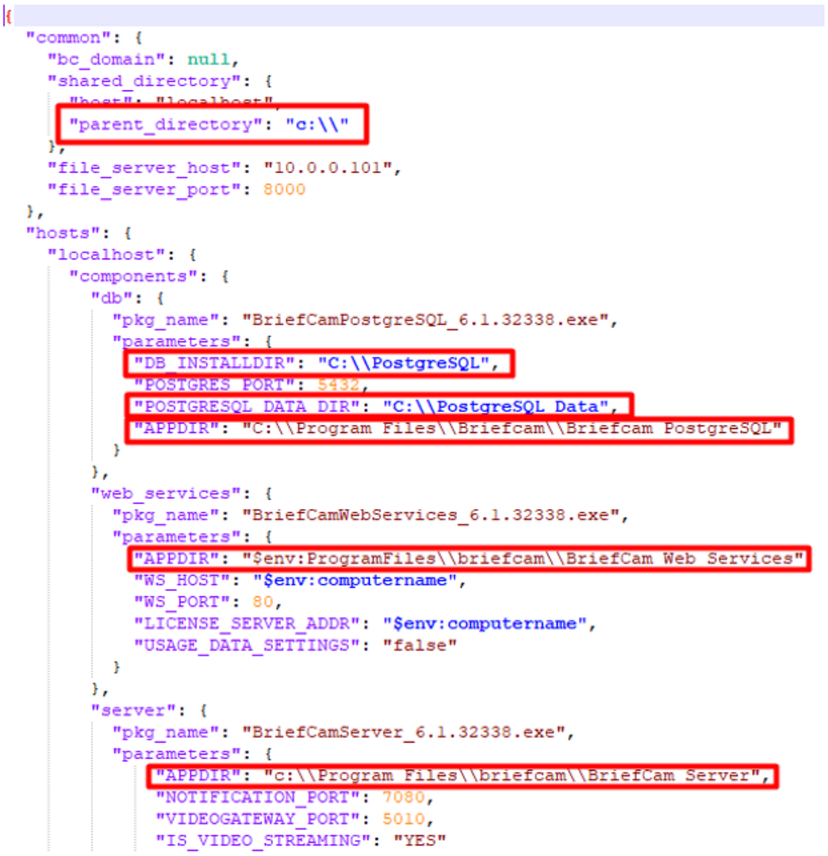
1. Extract the XProtect Rapid REVIEW package (RapidREVIEW_v6.1.xxxxx.zip)

   The extracted folder includes a main folder called **deploy** with the installation script and multiple installer files:

   - BriefCam Milestone plug-in
   - BriefCam PostgreSQL
   - BriefCam Server
   - BriefCam Web Services

> Note: You do not need to run any of the installers. The installation script automatically installs XProtect Rapid REVIEW for you.

2. If you want to change the target directory for a server application or its associated data from C:// to a different location, open the **config.json** file (located in the **deploy** folder) and change the paths that are highlighted in the illustration below.



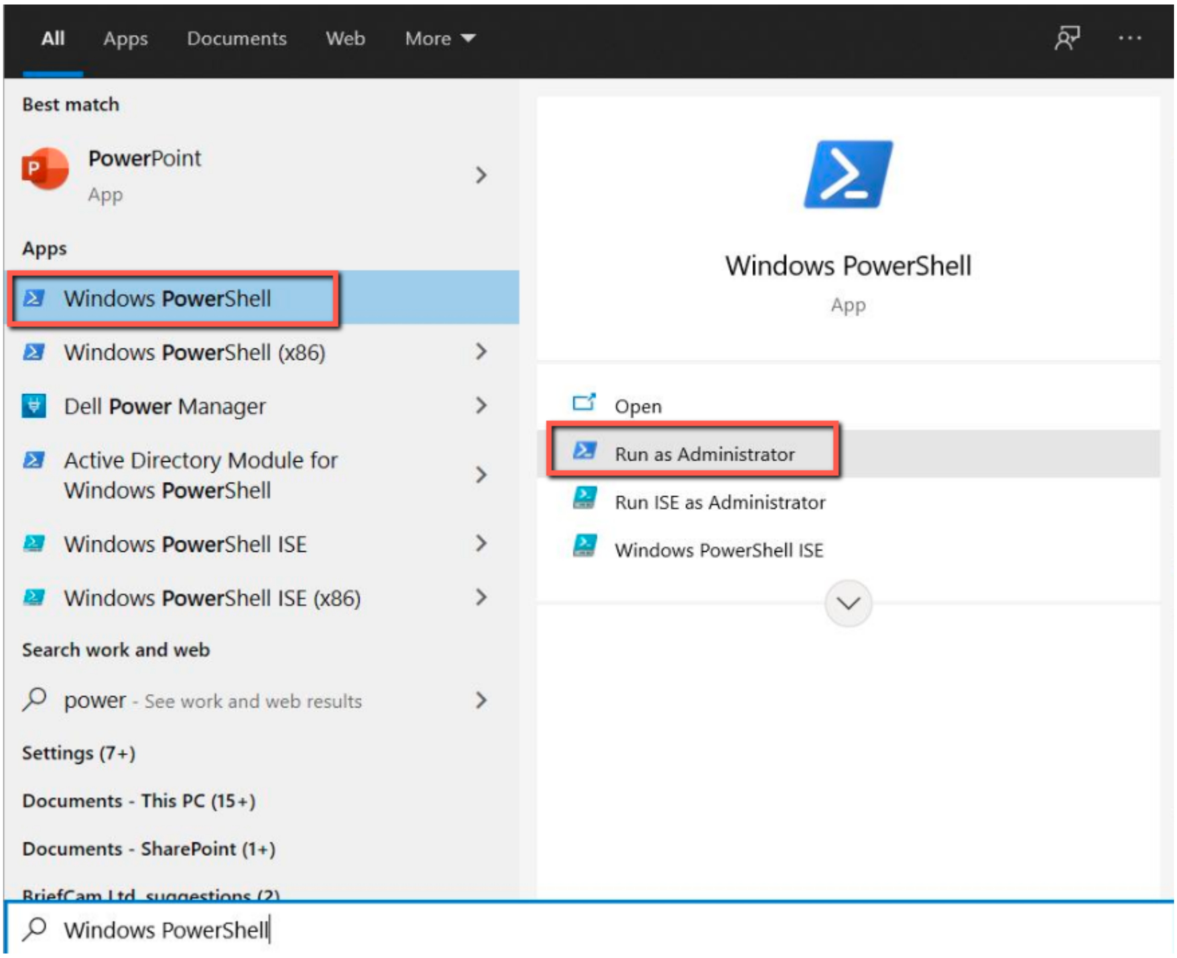
```
{
  "common": {
    "bc_domain": null,
    "shared_directory": {
      "host": "localhost",
      "parent_directory": "c:\\"
    },
    "file_server_host": "10.0.0.101",
    "file_server_port": 8000
  },
  "hosts": {
    "localhost": {
      "components": {
        "db": {
          "pkg_name": "BriefCamPostgreSQL_6.1.32338.exe",
          "parameters": {
            "DB_INSTALLDIR": "C:\\PostgreSQL",
            "POSTGRES_PORT": 5432,
            "POSTGRESQL_DATA_DIR": "C:\\PostgreSQL Data",
            "APPDIR": "C:\\Program Files\\Briefcam\\Briefcam PostgreSQL"
          }
        },
        "web_services": {
          "pkg_name": "BriefCamWebServices_6.1.32338.exe",
          "parameters": {
            "APPDIR": "$env:ProgramFiles\\briefcam\\BriefCam Web Services"
            "WS_HOST": "$env:computername",
            "WS_PORT": 80,
            "LICENSE_SERVER_ADDR": "$env:computername",
            "USAGE_DATA_SETTINGS": "false"
          }
        },
        "server": {
          "pkg_name": "BriefCamServer_6.1.32338.exe",
          "parameters": {
            "APPDIR": "c:\\Program Files\\briefcam\\BriefCam Server",
            "NOTIFICATION_PORT": 7080,
            "VIDEOGATEWAY_PORT": 5010,
            "IS_VIDEO_STREAMING": "YES"
```

Parameter	Description
“parent_directory”	Location where video files and processing artifacts will be stored.
“DB_INSTALLDIR”	Location where the Postgres SQL database will be installed.
“POSTGRESQL_DATA_DIR”	Location where Postgres SQL data and scripts are stored.
“APPDIR”	Location where the application files will be installed.

3. If a domain user is required, set the domain name itself in the config file (config.json):

   "bc_domain:"user-domain-name"

4. Open Windows PowerShell 64 bit as an Administrator.



5. Run the following PowerShell command to enable running remote signed scripts:

```
Set-ExecutionPolicy RemoteSigned
```

6. When asked if you want to change the execution policy, type in **a** and press **Enter**.

7. Open the **deploy** installation folder:

```
cd [your extracted folder]\deploy
```

8. Set seven variables by running each of the below commands separately. Replace the text in quotation marks (" ") with your values. Note that all of the strings should only have whole numbers and/or English letters:

Command	Description
$env:BC_USR="USER_NAME"	The user that runs BriefCam services.
$env:BC_PWD="USER_PASSWORD"	The user’s password.
$env:PG_BC_USR="PG_BC_USR"	The BriefCam application user for the PostgreSQL database. This cannot be the same as the PG_BC_ ADMIN_USR mentioned below.
$env:PG_BC_PWD="PG_BC_PWD"	The password of the user above (PostgreSQL user).
$env:PG_BC_ADMIN_USR="PG_BC_ADMIN_USR"	The root admin user for the PostgreSQL datbase. This cannot be the same as the PG_BC_USR mentioned above.

$env:PG_BC_ADMIN_PWD="PG_BC_ADMIN_PWD"	The password of the user above (PostgreSQL root admin user).
$env:BC_PASS_PHRASE = "Welcome1"	This pass phrase will be used to generate an encryption key to secure connection strings and other sensitive data.

> For the most reliable performance, the user that runs BriefCam services, the **BC_USR**, should be part of the **Administrators** role in XProtect Management Client and additionally, this user should have local administrator rights on the server where the deployment is performed.
>
> If a user that runs BriefCam services logs on using the **Windows authentication (current user)** option and this user is not part of the **Administrators** role in XProtect Management Client, authentication in BriefCam via the Briefcam Milestone SSO provider might fail. The failure to authenticate will have the effect that the **BriefCam** tab in XProtect® Smart Client will load without content.

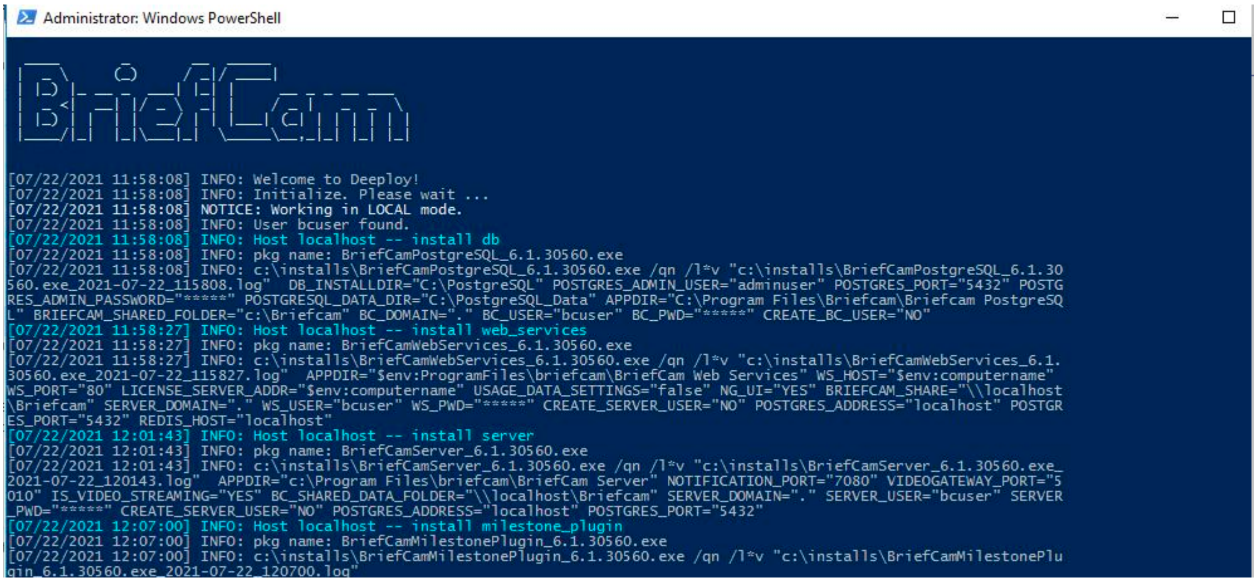
9. Run the following command to start the installation:

```
.\deploy.ps1 -local
```

For example:

```
C:\RapidReview\deeploy> .\deeploy.ps1 -local
```

The installation may take 10-25 minutes.



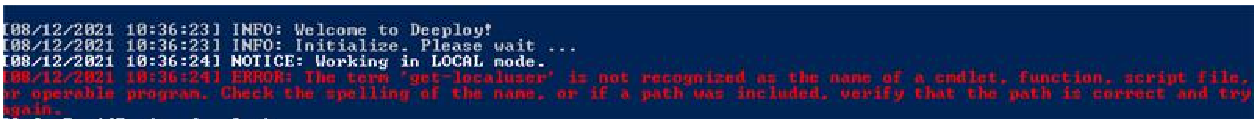
```
[07/22/2021 11:58:08] INFO: Welcome to Deeploy!
[07/22/2021 11:58:08] INFO: Initialize. Please wait ...
[07/22/2021 11:58:08] NOTICE: Working in LOCAL mode.
[07/22/2021 11:58:08] INFO: User bcuser found.
[07/22/2021 11:58:08] INFO: Host localhost -- install db
[07/22/2021 11:58:08] INFO: pkg name: BriefCamPostgreSQL_6.1.30560.exe
[07/22/2021 11:58:08] INFO: c:\installs\BriefCamPostgreSQL_6.1.30560.exe /qn /l*v "c:\installs\BriefCamPostgreSQL_6.1.30
560.exe_2021-07-22_115808.log"  DB_INSTALLDIR="C:\PostgreSQL" POSTGRES_ADMIN_USER="adminuser" POSTGRES_PORT="5432" POSTG
RES_ADMIN_PASSWORD="*****" POSTGRESQL_DATA_DIR="C:\PostgreSQL_Data" APPDIR="C:\Program Files\Briefcam\Briefcam PostgreSQ
L" BRIEFCAM_SHARED_FOLDER="c:\Briefcam" BC_DOMAIN="." BC_USER="bcuser" BC_PWD="*****" CREATE_BC_USER="NO"
[07/22/2021 11:58:27] INFO: Host localhost -- install web_services
[07/22/2021 11:58:27] INFO: pkg name: BriefCamWebServices_6.1.30560.exe
[07/22/2021 11:58:27] INFO: c:\installs\BriefCamWebServices_6.1.30560.exe /qn /l*v "c:\installs\BriefCamWebServices_6.1.
30560.exe_2021-07-22_115827.log"  APPDIR="$env:ProgramFiles\briefcam\BriefCam Web Services" WS_HOST="$env:computername"
WS_PORT="80" LICENSE_SERVER_ADDR="$env:computername" USAGE_DATA_SETTINGS="false" NG_UI="YES" BRIEFCAM_SHARE="\\localhost
\Briefcam" SERVER_DOMAIN="." WS_USER="bcuser" WS_PWD="*****" CREATE_SERVER_USER="NO" POSTGRES_ADDRESS="localhost" POSTGR
ES_PORT="5432" REDIS_HOST="localhost"
[07/22/2021 12:01:43] INFO: Host localhost -- install server
[07/22/2021 12:01:43] INFO: pkg name: BriefCamServer_6.1.30560.exe
[07/22/2021 12:01:43] INFO: c:\installs\BriefCamServer_6.1.30560.exe /qn /l*v "c:\installs\BriefCamServer_6.1.30560.exe_
2021-07-22_120143.log"  APPDIR="c:\Program Files\briefcam\BriefCam Server" NOTIFICATION_PORT="7080" VIDEOGATEWAY_PORT="5
010" IS_VIDEO_STREAMING="YES" BC_SHARED_DATA_FOLDER="\\localhost\Briefcam" SERVER_DOMAIN="." SERVER_USER="bcuser" SERVER
_PWD="*****" CREATE_SERVER_USER="NO" POSTGRES_ADDRESS="localhost" POSTGRES_PORT="5432"
[07/22/2021 12:07:00] INFO: Host localhost -- install milestone_plugin
[07/22/2021 12:07:00] INFO: pkg name: BriefCamMilestonePlugin_6.1.30560.exe
[07/22/2021 12:07:00] INFO: c:\installs\BriefCamMilestonePlugin_6.1.30560.exe /qn /l*v "c:\installs\BriefCamMilestonePlu
gin_6.1.30560.exe_2021-07-22_120700.log"
```

Troubleshooting

If an error occurs, the error appears in the screen above and in the **deploy.log** and **deploy-trace.log** files, which are located in the **deploy** directory.

If you receive the following error, you ran the wrong version of PowerShell:

```
ERROR: The term 'get-localuser' is not recognized as the name of a cmdlet.
function. script file or operable program. Check the spelling of the name, or if a
path was include, verify that the path is correct and try again.
```



```
[08/12/2021 10:36:23] INFO: Welcome to Deeploy!
[08/12/2021 10:36:23] INFO: Initialize. Please wait ...
[08/12/2021 10:36:24] NOTICE: Working in LOCAL mode.
[08/12/2021 10:36:24] ERROR: The term 'get-localuser' is not recognized as the name of a cmdlet, function, script file,
r operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try
again.
```

If the installation failed:

1. Investigate the log files (deploy.log and deploy-trace.log) and fix the issue.
2. Reinstall BriefCam:
   a. Run the following command in PowerShell to remove all installation components:

```
.\deploy.ps1 -uninstall -local -purge
```

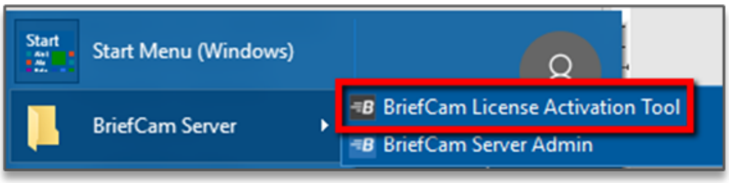
For example:

```
C:\RapidReview\deploy> .\deploy.ps1 -uninstall -local -purge
```

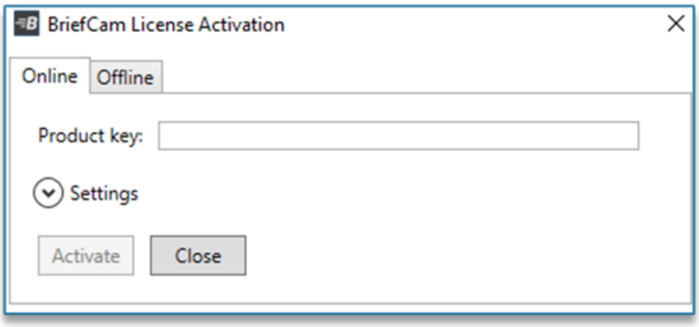
   b. Rerun the installation script.

STEP 3 - Activate the BriefCam license

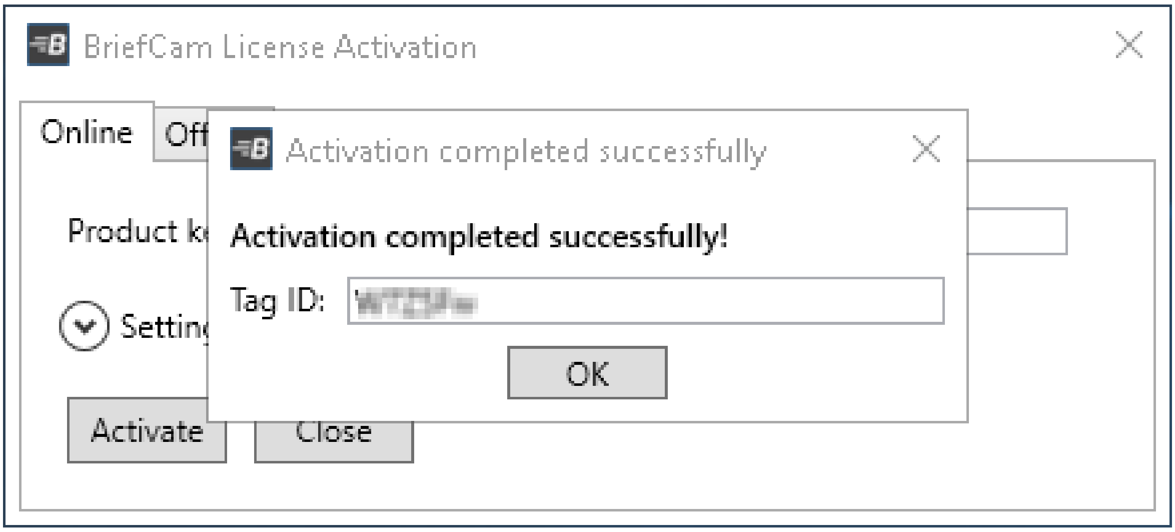
1. On the XProtect Rapid REVIEW computer, launch the BriefCam License Activation application from the **Start** menu.



2. Enter the product key that you received from BriefCam, and click **Activate**.



3. Upon successful activation, the following dialog box will appear.


BriefCam License Activation
Online
Off
Product k
Settin
Activate
Close
Activation completed successfully
OK

Activation completed successfully!

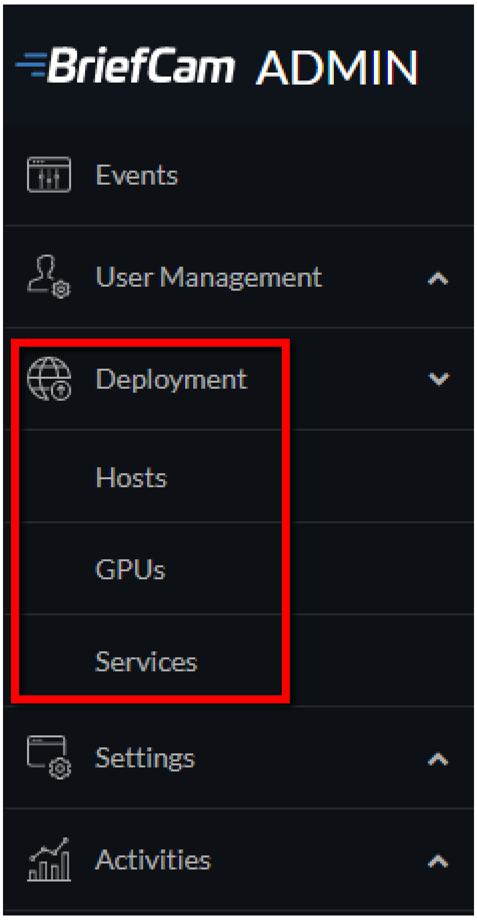
Tag ID: [redacted]

4. Click **OK** to close the dialog box, and then click **Close** in the main application window to close the License Activation application.

STEP 4 - Set up the deployment

1. In a browser, enter the URL of the computer where XProtect Rapid REVIEW was installed followed by slash (/) and the word **admin**, that is: **http://[computer name]/admin**. The BriefCam Administrator Console will open.
2. Log into the console. The user is **Administrator** and the password is **changeit**.
3. Change the password.

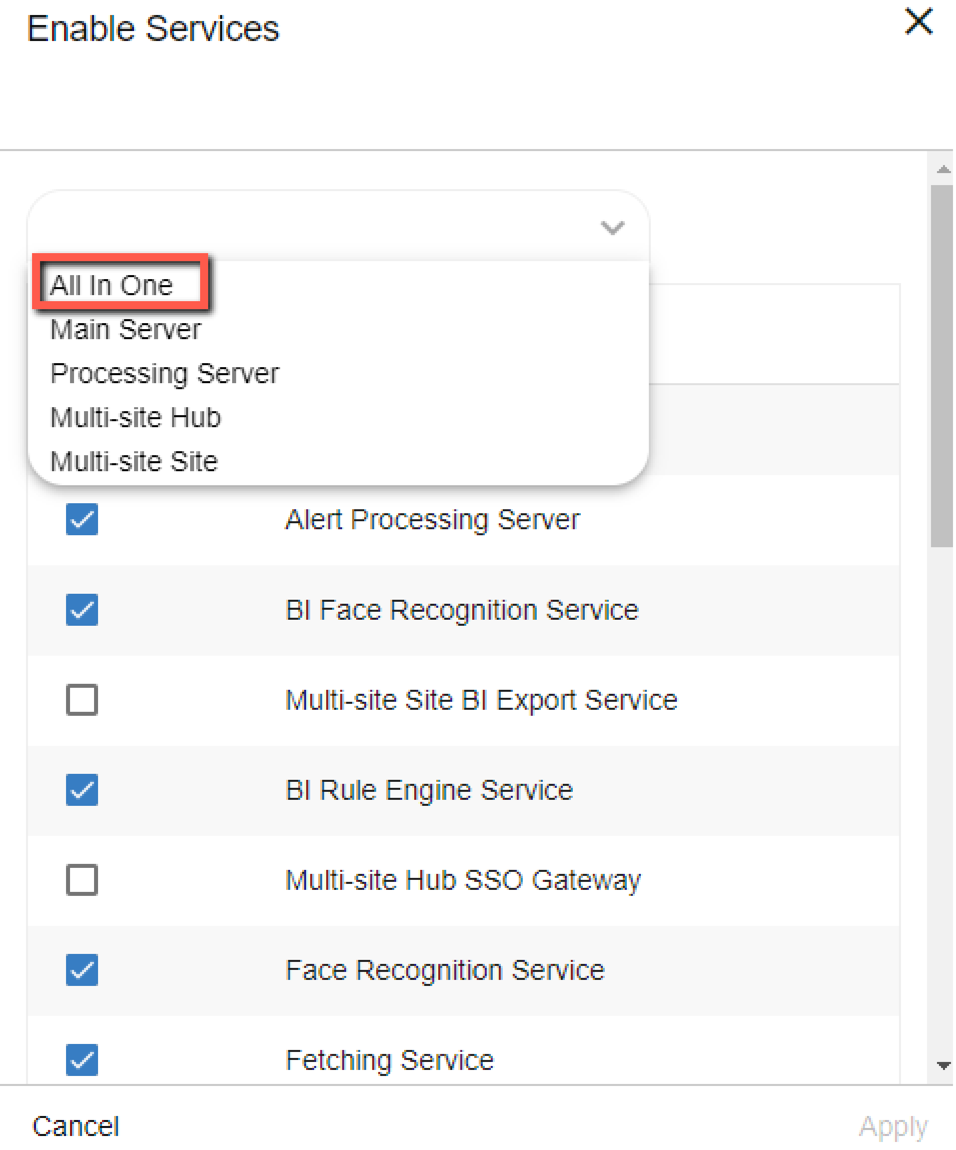
You'll now set up the deployment from the **Deployment** section.



4. From the **Deployment** section, click **Hosts**.

5. Next to the host name, click on the settings icon ⚙.

6. From the **Templates** menu, select **All In One**, and click **Apply**.



☑ Alert Processing Server

☑ BI Face Recognition Service

☐ Multi-site Site BI Export Service

☑ BI Rule Engine Service

☐ Multi-site Hub SSO Gateway

☑ Face Recognition Service

☑ Fetching Service

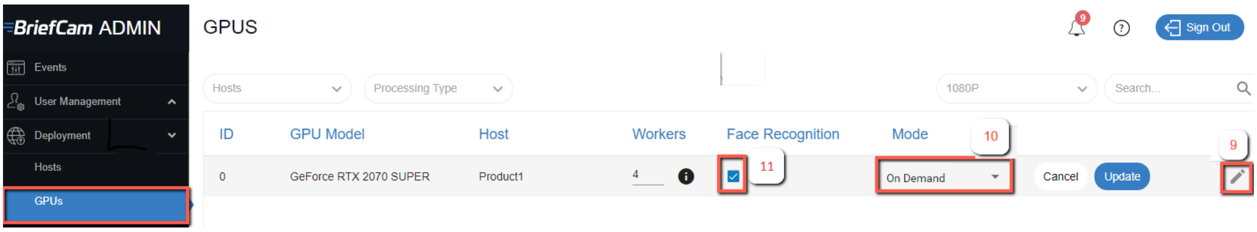
7. Clear the **Alert Processing Server**, **BI Face Recognition Service**, and **BI Rule Engine Service** check boxes.

8. From the **Deployment** section, click **GPUs**.

9. Click on the edit icon (✏).

10. In the **Mode** column, select **On Demand**.

11. If face recognition will be used, select the **Face Recognition** check box.



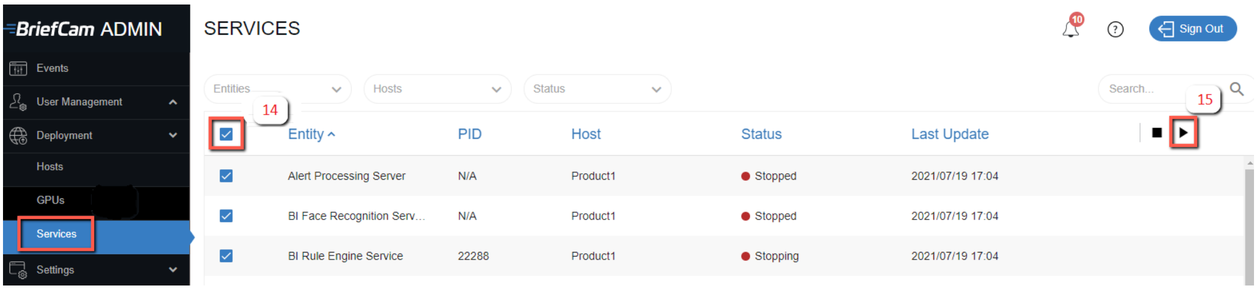
ID	GPU Model	Host	Workers	Face Recognition	Mode
0	GeForce RTX 2070 SUPER	Product1	4	☑	On Demand

12. Verify that the number of workers under **Workers** is set to 4.

13. From the **Deployment** section, click **Services**.

14. Select the check box at the top left of the table.

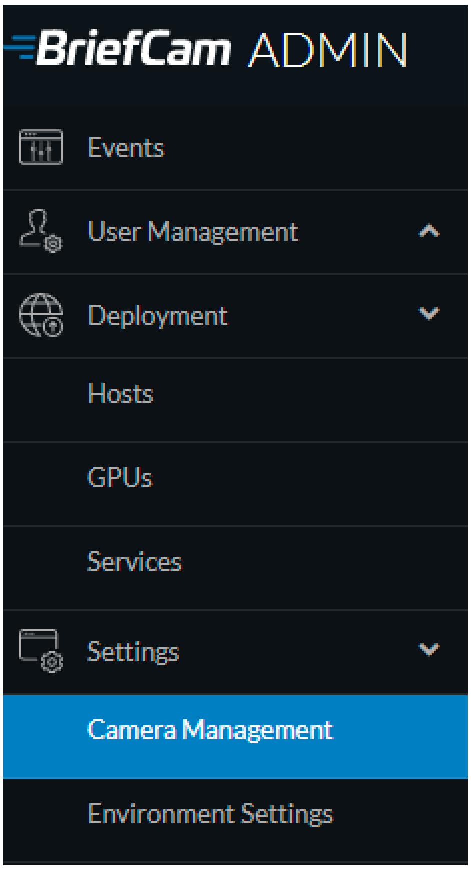
15. Click the start button (as shown in the image below).



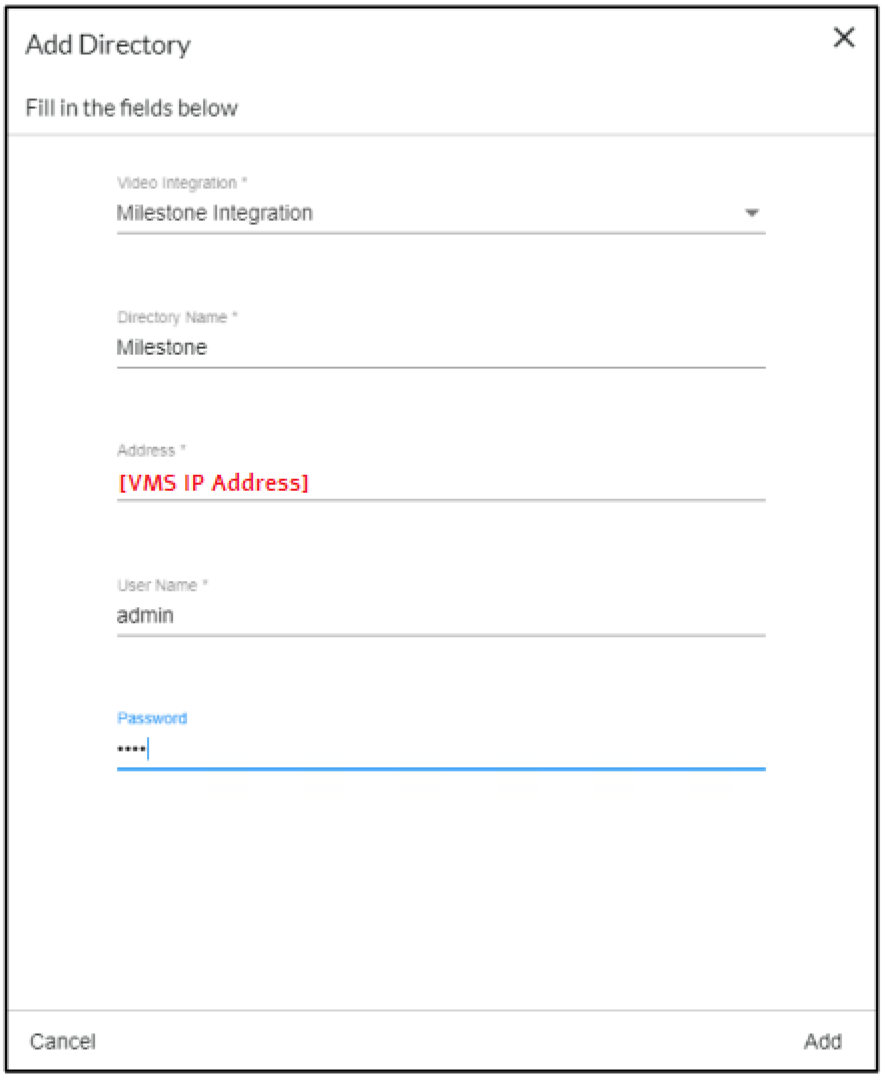
☑	Entity	PID	Host	Status	Last Update
☑	Alert Processing Server	N/A	Product1	● Stopped	2021/07/19 17:04
☑	BI Face Recognition Serv...	N/A	Product1	● Stopped	2021/07/19 17:04
☑	BI Rule Engine Service	22288	Product1	● Stopping	2021/07/19 17:04

STEP 5- Define and activate the cameras

1. Open the **Settings** section and click **Camera Management** (as shown in the image below).



2. Click **Add directory**. The **Add Directory** dialog box opens.



Add Directory

Fill in the fields below

Video Integration *
Milestone Integration

Directory Name *
Milestone

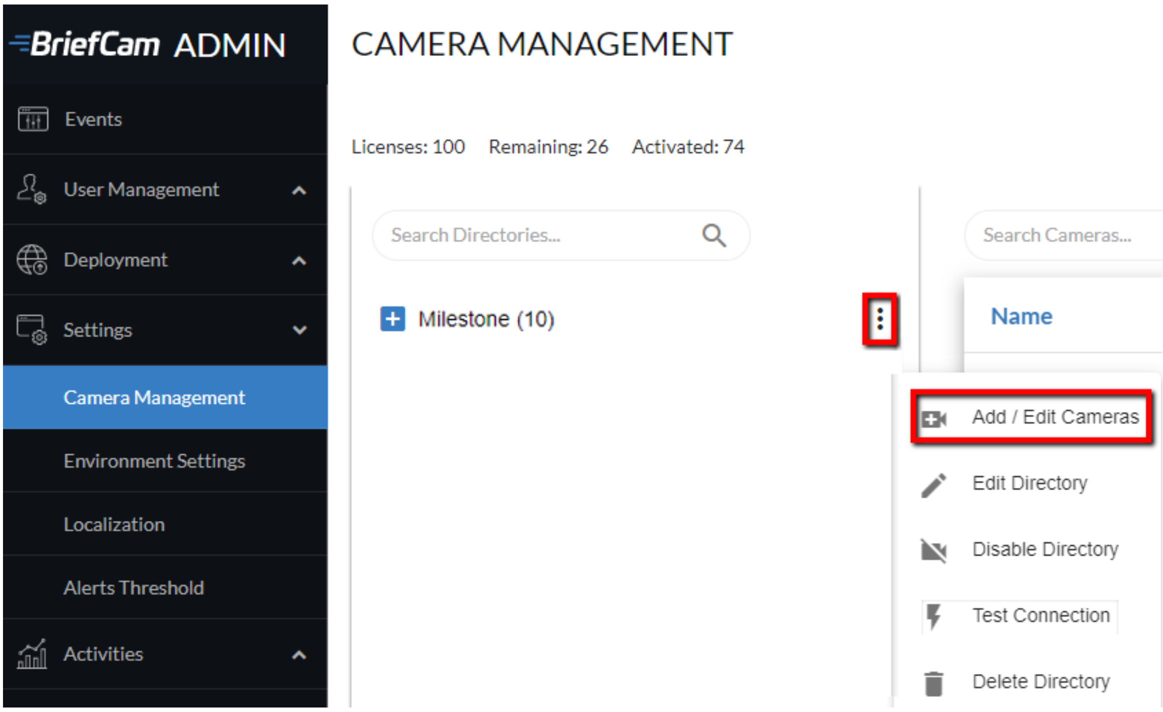
Address *
[VMS IP Address]

User Name *
admin

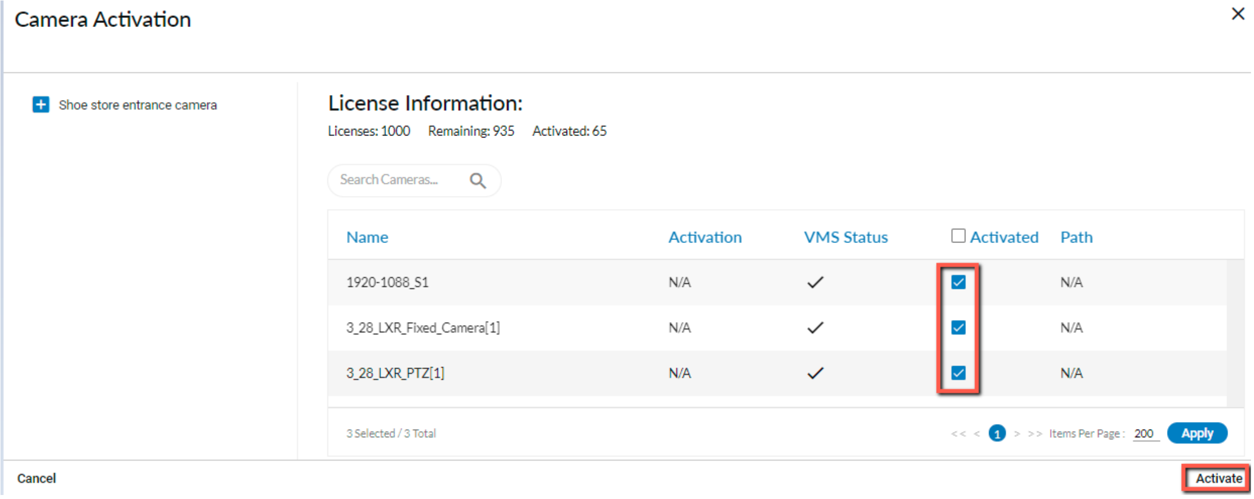
Password
••••

3. From the **Video Integration** field, select **Milestone Integration**.
4. In the **Directory Name** field, enter a display name for the user directory.
5. In the **Address** field, enter the address of the Milestone VMS server.
6. In the **User name** and **Password** fields, enter an administrator user name and password of the VMS server. With an admin user you can make sure that all cameras can be accessed.
7. Click **Add** to add the directory.

8. Click the zoom (⋮) icon to the right of the new directory and select the **Add / Edit Cameras** option.



9. For all of the cameras, select the check box in the camera's **Activated** column and click the **Activate** button (located in the bottom right corner), as shown in the image below.



License Information:

Licenses: 1000 Remaining: 935 Activated: 65

Name	Activation	VMS Status	□ Activated	Path
1920-1088_S1	N/A	✓	☑	N/A
3_28_LXR_Fixed_Camera[1]	N/A	✓	☑	N/A
3_28_LXR_PTZ[1]	N/A	✓	☑	N/A

3 Selected / 3 Total

<< < 1 > >> Items Per Page : 200 Apply

STEP 6 - Disable face recognition and license plate recognition (optional)

If you want to disable face recognition and/or license plate recognition:

1. Set the **clientEnableFaceRecognition** environment setting to **false**. This removes the Face Recognition functionality from the UI.

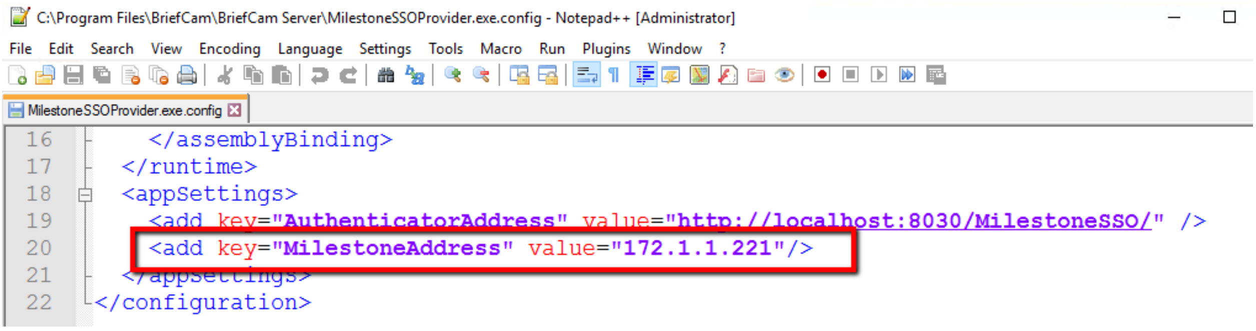
2. Set the **MetaData.EnableFaceRecognition** environment setting to **false**. This disables the Face Recognition engine.

3. Set the **EnableLPR** environment setting to **false**. This removers the License Plate Recognition functionality from the UI.

STEP 7 - Update the SSO address

1. On the XProtect Rapid REVIEW computer, go to C:\Program Files\BriefCam\BriefCam Server and open the MilestoneSSOProvider.exe.config file.

2. Edit the **MilestoneAddress** setting with the IP address of the Milestone VMS server.


C:\Program Files\BriefCam\BriefCam Server\MilestoneSSOProvider.exe.config - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
MilestoneSSOProvider.exe.config

```
      </assemblyBinding>
    </runtime>
    <appSettings>
      <add key="AuthenticatorAddress" value="http://localhost:8030/MilestoneSSO/" />
      <add key="MilestoneAddress" value="172.1.1.221"/>
    </appSettings>
</configuration>
```

Note: If STEP 7 is performed later, you will need to restart the IIS services.

STEP 8 - Install BriefCam Embedded Client for Milestone XProtect plug-in

On each XProtect Rapid REVIEW client computer, install BriefCam's embedded client for Milestone XProtect plugin.

1. Click the **BriefCam Embedded Client for Milestone XProtect** plug-in file to download it and then run it.

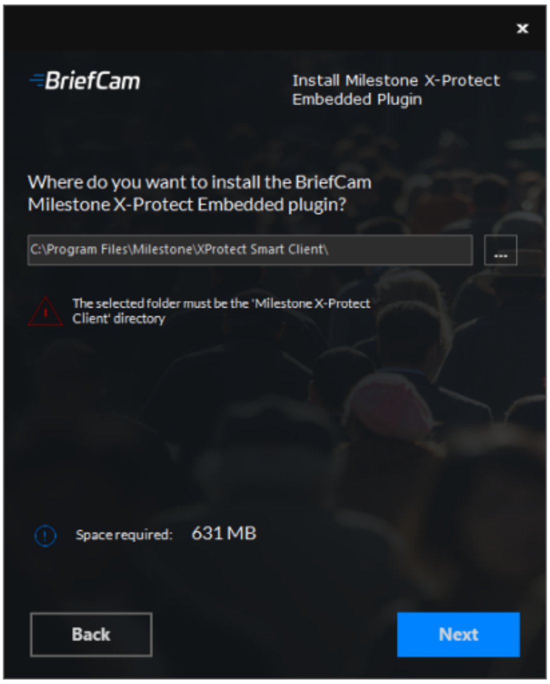
2. The installation checks for prerequisites, such as Microsoft .NET Framework 4.7.2 Full and Microsoft Visual C++ 2015 2017 2019 Redistributable Package (x64).

3. If anything is missing, you will be prompted to install the missing prerequisites and click **Install**.

4. In the Welcome screen, click **Get Started**.

5. Read the license, accept the License Agreement terms and click **Next**.

6. Select the installation destination path and click **Next**.
   Note that the installation path must be the same directory where **Milestone XProtect Smart Client** is installed. (This may vary slightly between client computers and between Milestone versions.)



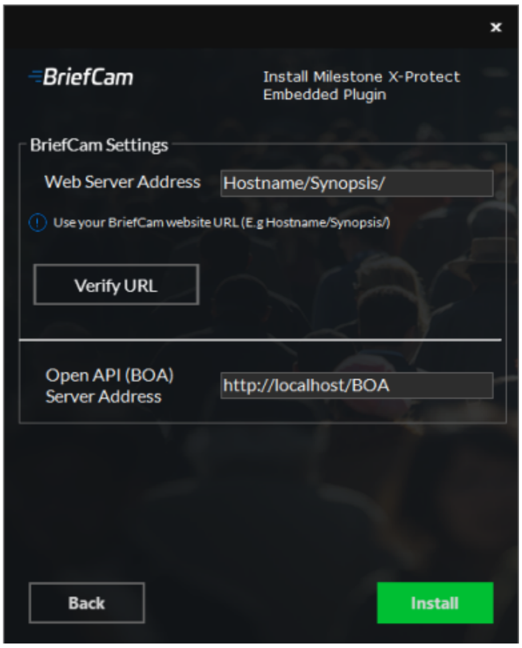
Where do you want to install the BriefCam Milestone X-Protect Embedded plugin?

C:\Program Files\Milestone\XProtect Smart Client\

The selected folder must be the 'Milestone X-Protect Client' directory

Space required: 631 MB

7. Enter the BriefCam Web Application URL (which is the address of the BriefCam computer followed by **/synopsis** and verify that the provided URL is correct by clicking the **Verify URL** button (as shown below).



BriefCam Settings

Web Server Address: Hostname/Synopsis/

Use your BriefCam website URL (E.g Hostname/Synopsis/)

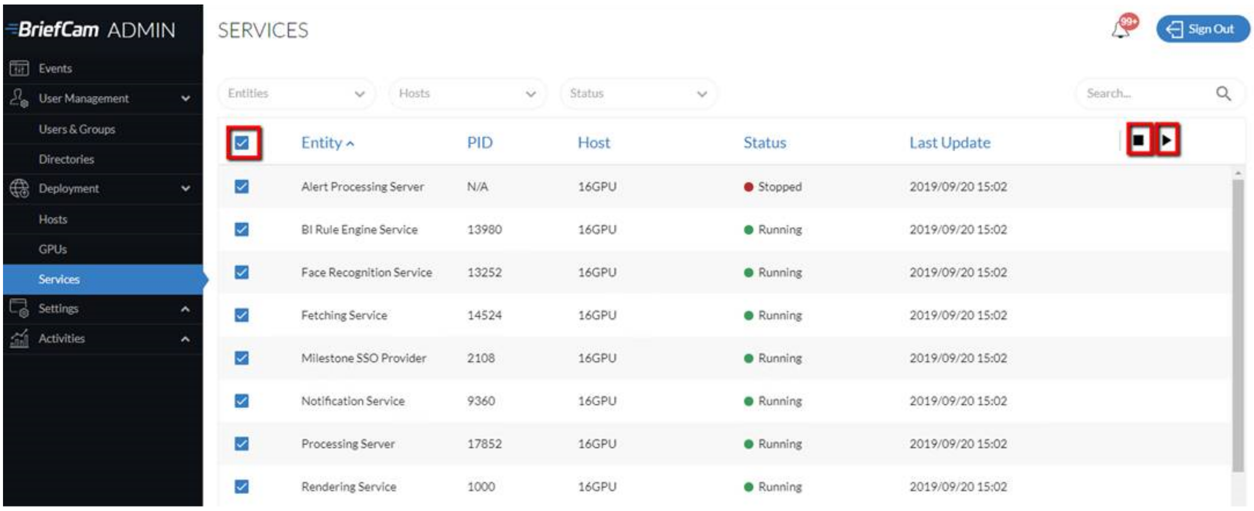
Open API (BOA) Server Address: http://localhost/BOA

8. In the **BriefCam Open API (BOA) Server Address** field, enter the address of the BriefCam computer followed by **/BOA**.

9. Click **Next**.

10. Click **Install** and then click **Finish**.

11. In the BriefCam Administrator Console, restart the services by selecting all of the services, clicking the stop button (■) and then the start button (▶), as shown in the image below.

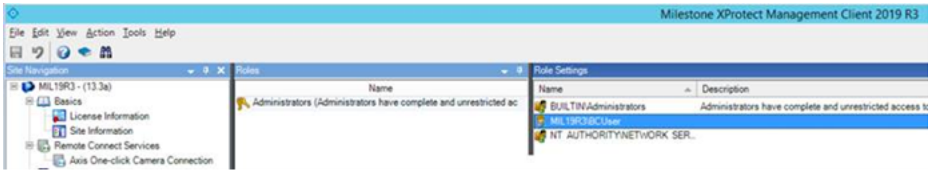


☑	Entity ^	PID	Host	Status	Last Update
☑	Alert Processing Server	N/A	16GPU	● Stopped	2019/09/20 15:02
☑	BI Rule Engine Service	13980	16GPU	● Running	2019/09/20 15:02
☑	Face Recognition Service	13252	16GPU	● Running	2019/09/20 15:02
☑	Fetching Service	14524	16GPU	● Running	2019/09/20 15:02
☑	Milestone SSO Provider	2108	16GPU	● Running	2019/09/20 15:02
☑	Notification Service	9360	16GPU	● Running	2019/09/20 15:02
☑	Processing Server	17852	16GPU	● Running	2019/09/20 15:02
☑	Rendering Service	1000	16GPU	● Running	2019/09/20 15:02

12. Restart IIS by opening the Windows services and right-click the **World Wide Web Publishing Service**. Then click **Restart**.

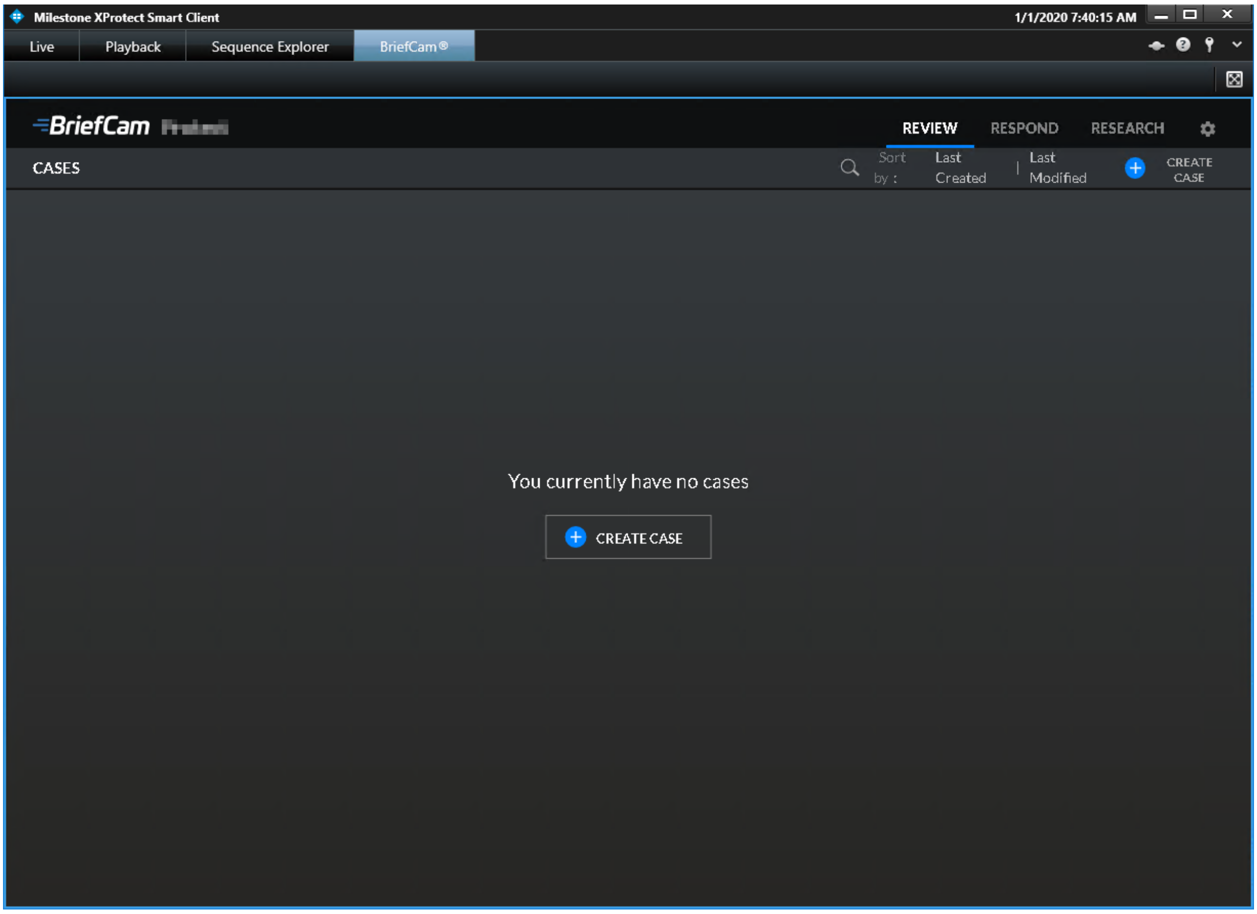
> Note: An admin user is automatically created by the SSO when logging into the Milestone client using the **Basic authentication** or **Windows authentication** method.

If you want to log into the Milestone client using the **Windows authentication (current user)** option, add the **BriefCam user** (by default this is **BCUser**) to the **Administrators** group in Milestone XProtect Management Client.


Milestone XProtect Management Client 2019 R3
File Edit View Action Tools Help
Site Navigation
MIL19R3 - (13.3a)
Basics
License Information
Site Information
Remote Connect Services
Axis One-click Camera Connection
Roles
Name
Administrators (Administrators have complete and unrestricted ac
Role Settings

Name	Description
BUILTIN\Administrators	Administrators have complete and unrestricted access t
MIL19R3\BCUser	
NT AUTHORITY\NETWORK SER...	

When you have completed the steps, a **BriefCam** tab will appear in the Milestone XProtect Smart Client.



You currently have no cases

In BriefCam, for security reasons, users are automatically logged out if no activity is detected for 20 minutes. Therefore, a user may be automatically logged off the BriefCam functionality while the Milestone VMS is still running.

STEP 9 - Using an HTTPS host (optional)

To work with SSL and BriefCam, using a load balancer is required.

This section describes the steps to take to use the NGINX load balancer as an https host for BriefCam services.

Recommendations

BriefCam recommends using NGINX.

It is recommended to install the load balancer on a separate computer.

If you are working in a virtualized environment, the load balancer must be on a separate computer.

If you are working in a non-virtualized (physical servers) environment, you can have the load balancer on the same computer as the Web Services (although it is not recommended). However, if you install the load balancer on the same computer as the Web Services, IIS must be on a different port than port 80, since port 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.

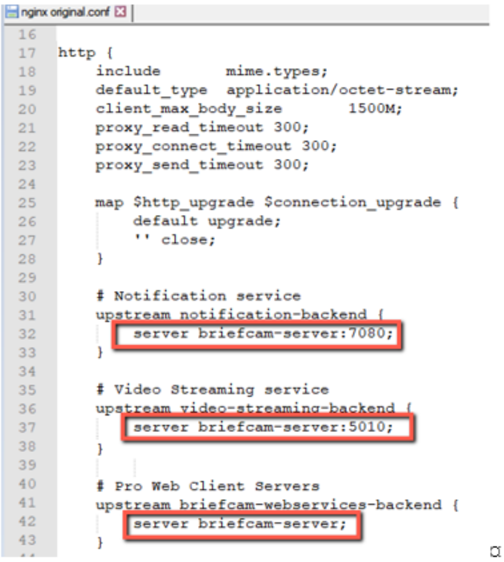
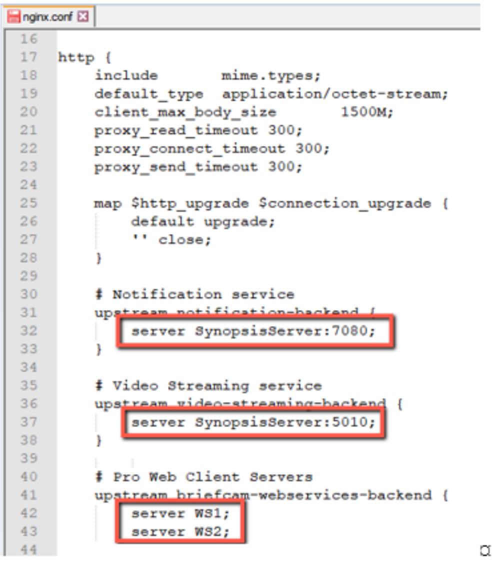
Steps

1. Download NGINX 1.19.x load balancer or later from this link: http://nginx.org/en/download.html.
2. Extract the NGINX zip files to drive C:. It is important to have the NGINX extracted so that the path is: **C:\NGINX**.
3. Create or use an already created self-signed certificate separated into two files: .crt and .key:

   For information about how to create a certificate, see one of these links:

   - https://slproweb.com/products/Win32OpenSSL.html
   - https://helpcenter.gsx.com/hc/en-us/articles/115015960428-How-to-Generate-a-Self-Signed-Certificate-and-Private-Key-using-OpenSSL
   - https://www.akadia.com/services/ssh_test_certificate.html

   To use an already created certificate from the current folder, place both the certificate’s .crt and .key files in the following path: **C:\NGINX\certificates\**.
4. Download the **nginx.conf** file from: https://bcftpuser:BCreleases01!@bcftp.briefcam.com/nginx/nginx.conf and save it to **c:\nginx\conf** (replacing the existing file).
5. In the **nginx.conf** file’s **http** section, modify the server name where the components are running (web services, notification services, and Video Streaming Gateway Services).
6. If you have multiple nodes of a service, add a semicolon (;) after the first node and add a second row with the name of the second node. In the example below, there are two Web Services nodes.

Original¤	Example¤
	

```
http {
    include         mime.types;
    default_type  application/octet-stream;
    client_max_body_size        1500M;
    proxy_read_timeout 300;
    proxy_connect_timeout 300;
    proxy_send_timeout 300;

    map $http_upgrade $connection_upgrade {
        default upgrade;
        '' close;
    }

    # Notification service
    upstream notification-backend {
        server briefcam-server:7080;
    }

    # Video Streaming service
    upstream video-streaming-backend {
        server briefcam-server:5010;
    }

    # Pro Web Client Servers
    upstream briefcam-webservices-backend {
        server briefcam-server;
    }
```

```
http {
    include         mime.types;
    default_type  application/octet-stream;
    client_max_body_size        1500M;
    proxy_read_timeout 300;
    proxy_connect_timeout 300;
    proxy_send_timeout 300;

    map $http_upgrade $connection_upgrade {
        default upgrade;
        '' close;
    }

    # Notification service
    upstream notification-backend {
        server SynopsisServer:7080;
    }

    # Video Streaming service
    upstream video-streaming-backend {
        server SynopsisServer:5010;
    }

    # Pro Web Client Servers
    upstream briefcam-webservices-backend {
        server WS1;
        server WS2;
```

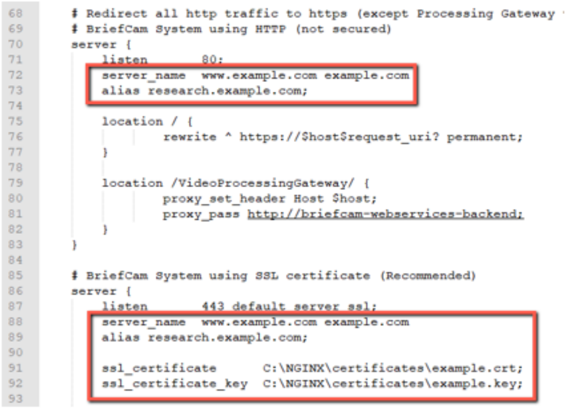
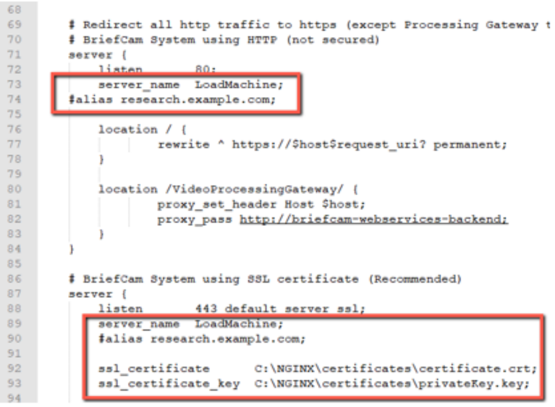
7. In the **nginx.conf** file's **BriefCam System using SSL certificate** section you set up HTTPS as follows:

    a. In the **server_name** node, replace **www.example.com** with the address of the load balancer.

    b. Comment the **alias** node by adding an ampersand (#) at the beginning of the row.

    c. In the **ssl_certificate** row, enter the full path to the .crt file including the file name.

    d. In the **ssl_certificate_key** row, enter the full path to the .key file including the file name.

Original	Example
	

```
# Redirect all http traffic to https (except Processing Gateway
# BriefCam System using HTTP (not secured)
server {
    listen        80;
    server_name  www.example.com example.com
    alias research.example.com;

    location / {
            rewrite ^ https://$host$request_uri? permanent;
    }

    location /VideoProcessingGateway/ {
            proxy_set_header Host $host;
            proxy_pass http://briefcam-webservices-backend;
    }
}

# BriefCam System using SSL certificate (Recommended)
server {
    listen        443 default server ssl;
    server_name  www.example.com example.com
    alias research.example.com;

    ssl_certificate      C:\NGINX\certificates\example.crt;
    ssl_certificate_key  C:\NGINX\certificates\example.key;
```

```

# Redirect all http traffic to https (except Processing Gateway t
# BriefCam System using HTTP (not secured)
server {
    listen        80;
    server_name  LoadMachine;
#alias research.example.com;

    location / {
            rewrite ^ https://$host$request_uri? permanent;
    }

    location /VideoProcessingGateway/ {
            proxy_set_header Host $host;
            proxy_pass http://briefcam-webservices-backend;
    }
}

# BriefCam System using SSL certificate (Recommended)
server {
    listen        443 default server ssl;
    server_name  LoadMachine;
    #alias research.example.com;

    ssl_certificate      C:\NGINX\certificates\certificate.crt;
    ssl_certificate_key  C:\NGINX\certificates\privateKey.key;
```

8. Download the latest release of the NSSM zip files from this link: https://nssm.cc/download and place them on the load balancer computer.

9. Extract the NSSM zip file to a folder, for example: **C:\NSSM\**.

10. Open CMD as **administrator**, navigate to the new **NSSM\win32** folder and run the following commands:

    - nssm install NGINX “C:\nginx\nginx.exe”
    - nssm set NGINX AppDirectory C:\nginx
    - nssm set NGINX DisplayName “NGINX Web Server”
    - nssm set NGINX Description “NGINX Web Server”
    - nssm set NGINX Start SERVICE_AUTO_START

> In the examples below, replace the string **www.example.com** with the address of the load balancer.
> For example: Load balancer = LB01.briefcam.com.

11. 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

    For example: 10.0.0.143 www.example.com

12. Restart the load balancer computer, open **services.msc** and try to start the newly created **NGINX Web Server** service.

    - If the service does not start, there may be an issue with its path. To try and solve this issue, run NSSM install on the same folder as described under step 8 and define the service via the NSSM GUI (making sure to specify the parameters properly).

13. Edit both web config .js files on the BriefCam server (located at C:\Program Files\BriefCam\WebServices\ProWebClient\webConfig.js and C:\Program Files\BriefCam\WebServices\ProWebAdminClient\web.config.js) using the syntax below. This syntax refers to the load balancer address. The endpoints in both files must point to the load balancer.

    • //www.example.com/ProWebApi/

    • //www.example.com/AdminApi/

14. In the BriefCam Administrator Console, set the environment settings with the following values:

    • DB.LocalStorageAddress : “//www.example.com/ProWebApiStorage"

    • BaseVideoUrl: “https://www.example.com/vsg”

    • ClientNotificationEndPoint: “//www.example.com/signalr" (without port 7080)

    > **VideoProcessingGatewayUrl** in https is **not** supported.

> **VideoProcessingGateWayUrl** will use **http** and not **https** because it is communicating between two internal processes (real-time engine and Video Processing gateway web service). This is on purpose to save resources.

15. You now need to update certain parameters, so that the embedded client will reach BriefCam using an HTTPS protocol. In order to do this:

    a. Open the **BriefCam.MilestoneEmbeddedViewer.dll.config** file, which is located at: C:\Program Files\Milestone\XProtect Smart Client\MIPPlugins\BriefCam.

    b. Change the URLs (highlighted below) to include HTTPS:

    ```
    <appSettings>
    <!--Client site address-->
    <add key="serverAddress" value="https://SMB29/Synopsis/" />
    <!--Boa site address-->
    <add key="boaServerAddress" value="https://SMB29/BOA" />
    <!--add key="boaVersion" value="1.0" /-->
    <!--add key="keepAliveIntervalMS" value="60000" /-->
    <!--add key="httpTimeout" value="5000" /-->
    <!--add key="pageLoadTimeoutMS" value="1000" /-->
    <!--add key="BrowserLogLocation" value="c:\DotNetBrowserLog.txt" /-->
    </appSettings>
    ```

16. Browse to the application and make sure that it works with https requests.

    For example:

    - https://www.example.com/synopsis
    - https://www.example.com/admin

Generic configurations

For any other type of load balancer, you need to configure the following redirect rules based on the URL:

1. Notification Service

   Search for: /signalr

   Redirect to: notification-server:7080

2. Video Streaming Gateway

   Search for: /vsg

   Use rewrite rule to remove /vsg from the url

   Redirect to: videostreaming-server:5010

3. Web Services>

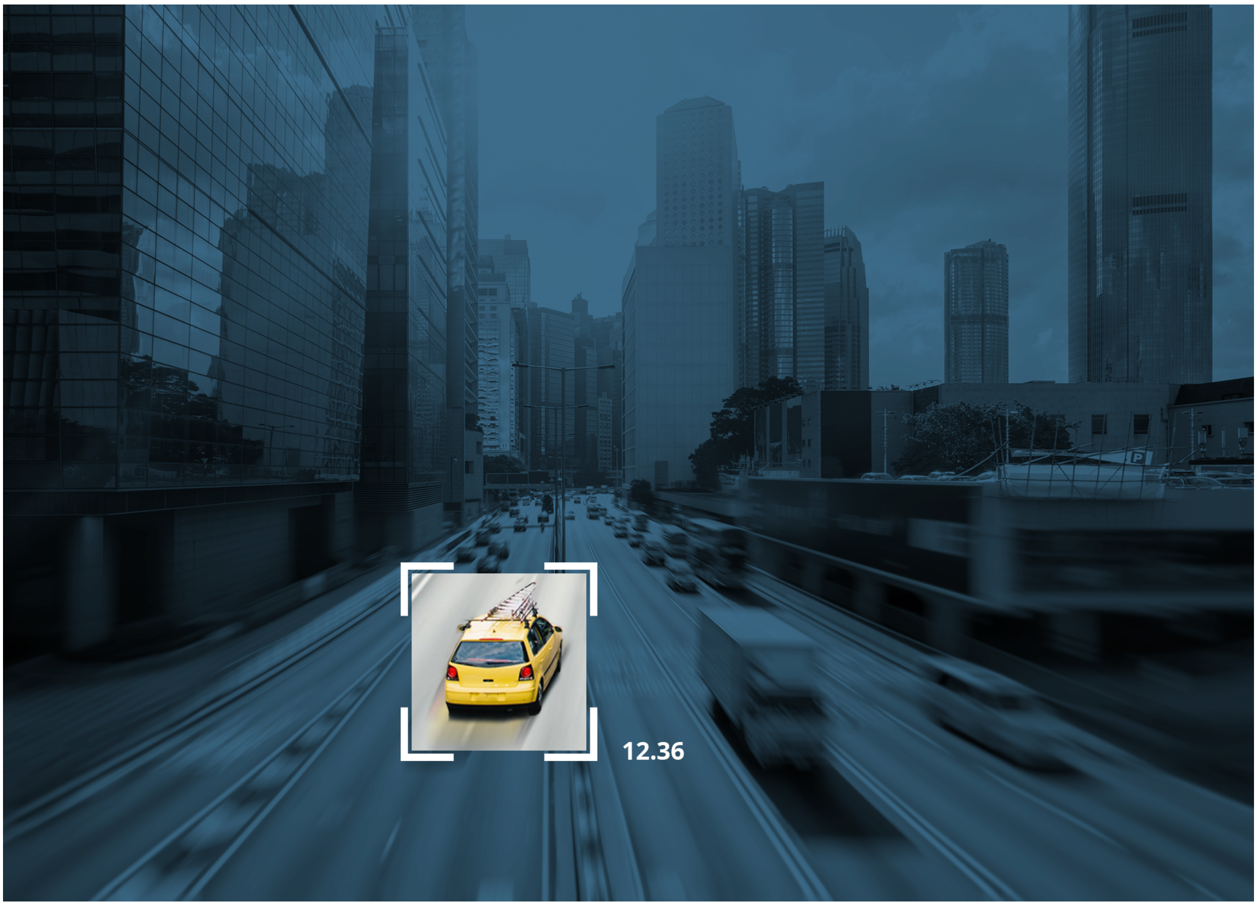
   Search for: /

   Redirect to: briefcam-webserver

Logging

To handle the log rotation:

1. Download the log rotation text from here: Log rotation script and create a bat file:
   a. Copy the text from the link to a .txt file and name it LogRotation.
   b. Change the file extension from .txt to .bat.
2. Save the script (.bat file) 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 assign full control to the user that you created in step 3.
5. Click **Start** (Windows key) and type **secpol.msc** to open the **Local Security Policy** utility.
6. Go to **Security settings** > **Local Policies** > **User Rights Assignment**.
7. Right-click **Log on as a batch job** and add the user.
8. Add a daily scheduled task to run the **C:\NGINX\LogRotation.bat** file. Make sure to select **Run whether user is logged on or not**. By default, the last 10 days will be retained (retention period in days). If you want a different number of days, when running the batch file, enter the required number of days as a command line argument. For example, for 20 days, use: **C:\NGINX\LogRotation.bat 20**.


12.36