IAM

Put Video on Specific Websites And Reject Other Video Configuration Guide

Version 12.0.18

Change Log

Date	Change Description
Dec 03, 2019	Version 12.0.18 document release.

CONTENT

1 Application Scenario 1
2 Configuration Step 1
3 Testing Result 5
4 Precautions 6

1 Application Scenario

Allowed internal user to visit to specific video, but rejected to visit other web site video.
Requirement condition:

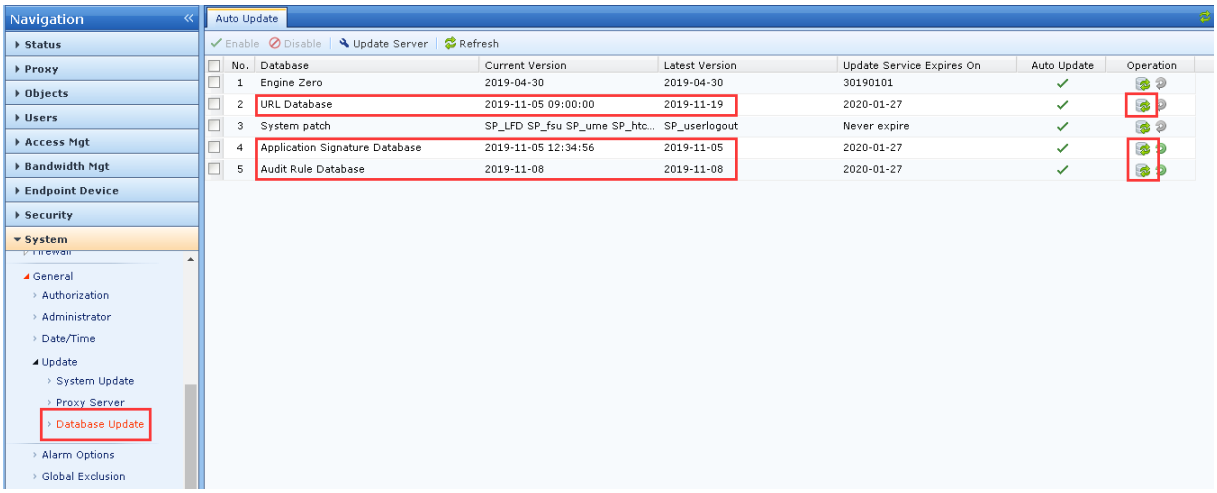
1. Prepare one IAM version 12.0.18 device, with IP address 10.1.3.40.
2. Prepare one PC, with a testing IP address 10.1.3.101.
3. The video browning address https://sangfor.com/source/video-videos.html

2 Configuration Step

First Step: Update database to latest version.

[**System**] – [**General**] – [**Update**] – [**Database Update**] , verify if the current database version is the latest version, please make sure that [**Application Signature Database**] has updated to latest version, else click on [**Update now**] to update to latest version.

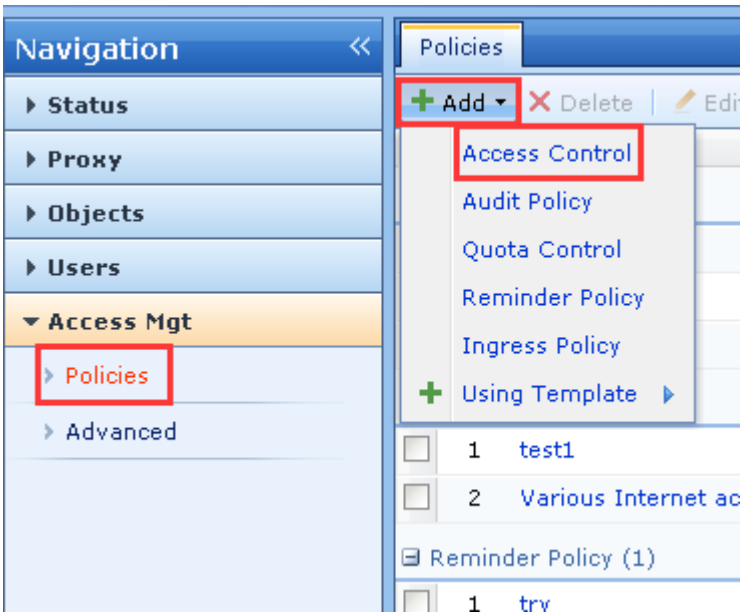
Ensure that [**URL Database**], [**Application Signature Database**] and [**Audit Rule Database**] will have 1 or 2 updates per month.

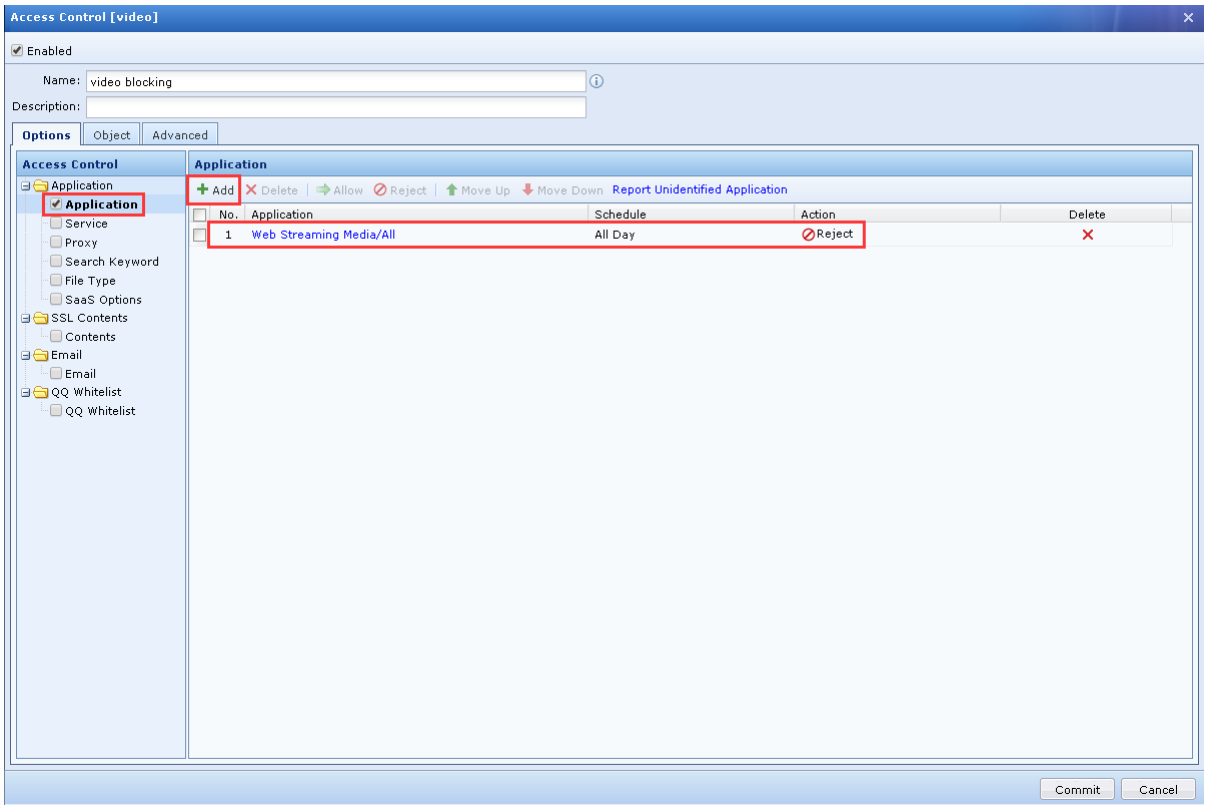


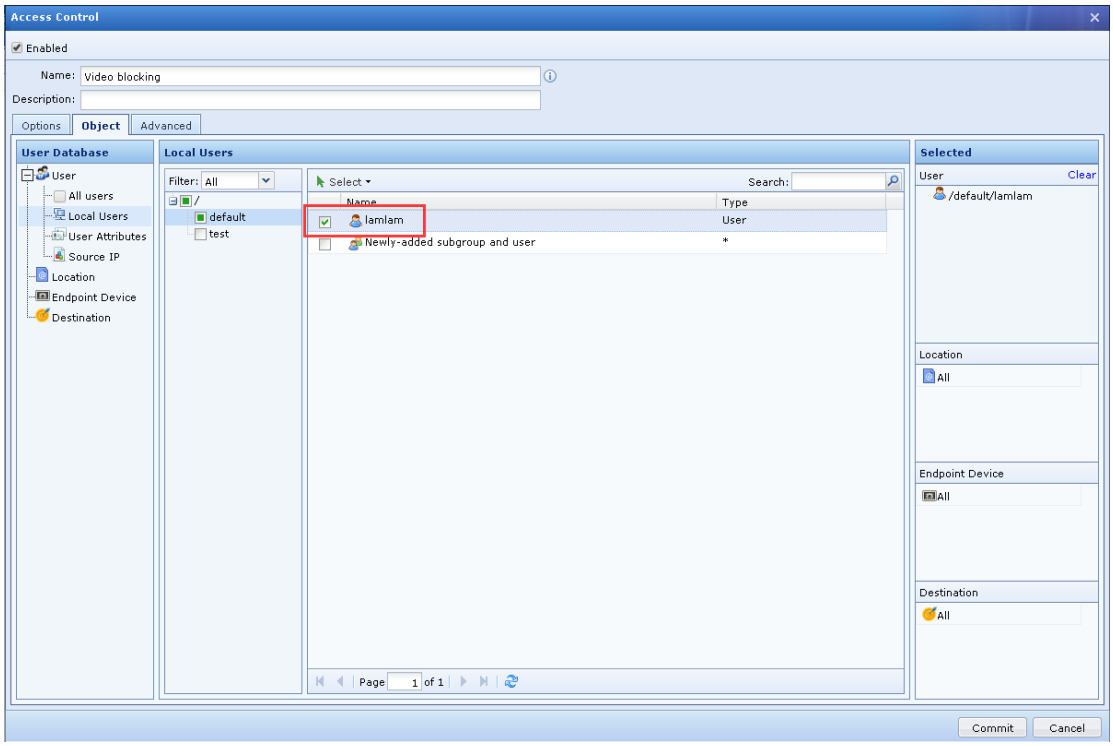
When update the database, please ensure that the license is within the validity period, as well as the device is able to visit website and resolve the domain name normally.

Second Step: Configure access control policy

In [**Access Management**] – [**Policies**], click on [**Add**] – [**Access Control**] , insert a name for this policy at "Name" bar, then select [**Application**] , continue click on [**Add**], select the application [**Web Streaming Video/All**], [**Schedule**] as All Day, [**Action**] as Reject, [**Object**] you may choose all or some specified user, you will finish the configuration after click on [**Commit**], the configuration as diagram below.


Navigation
Status
Proxy
Objects
Users
Access Mgt
Policies
Advanced
Policies
Add
Delete
Access Control
Audit Policy
Quota Control
Reminder Policy
Ingress Policy
Using Template
1 test1
2 Various Internet ac
Reminder Policy (1)
1 try

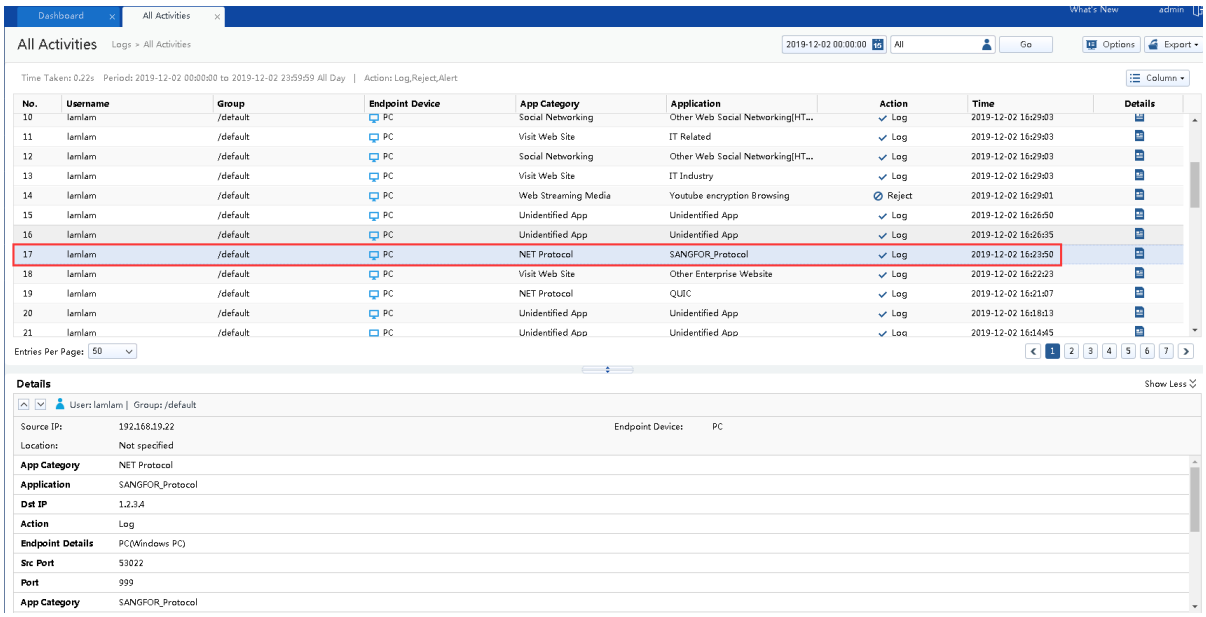

Access Control [video]
Enabled
Name: video blocking
Description:
Options
Object
Advanced
Access Control
Application
Service
Proxy
Search Keyword
File Type
SaaS Options
SSL Contents
Contents
Email
Email
QQ Whitelist
QQ Whitelist
Application
Add
Delete
Allow
Reject
Move Up
Move Down
Report Unidentified Application
No.
Application
Schedule
Action
Delete
1 Web Streaming Media/All All Day Reject
Commit
Cancel



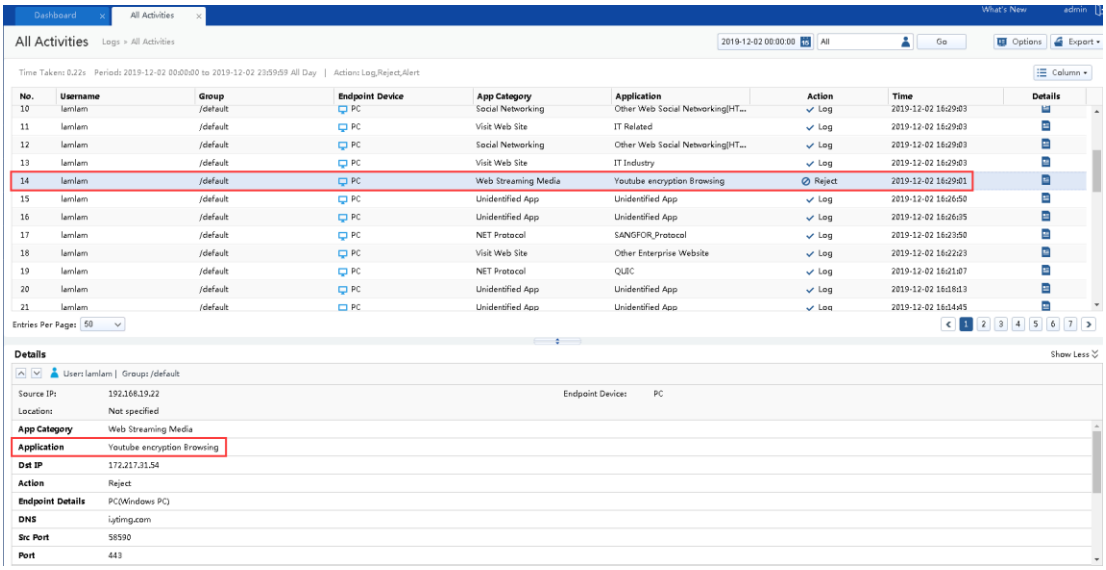
Third Step: Testing for blocking and targeted release.

By using a PC to watch the video in Sangfor.com , if the video browsing is rejected, checked on the related log in Report Center, determine the causes of video rejected and perform targeted release.

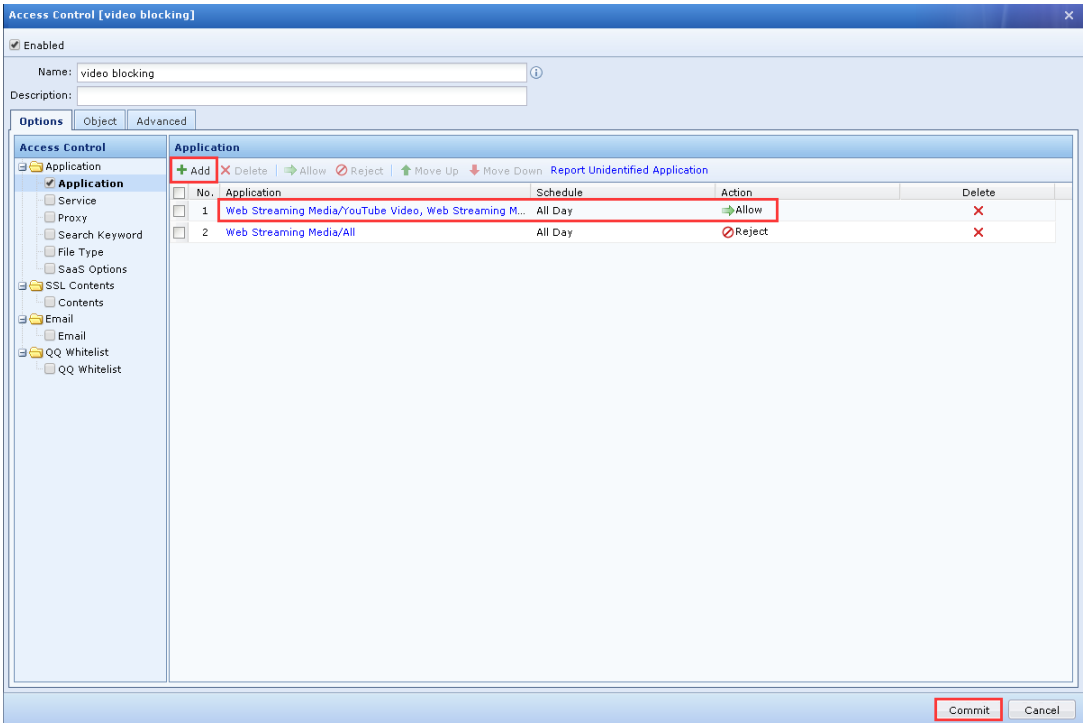
1. Checked the activity log that recorded in Internal Record Center, as we can see the user has enter Sangfor.com to get view on the video. The diagram as below.



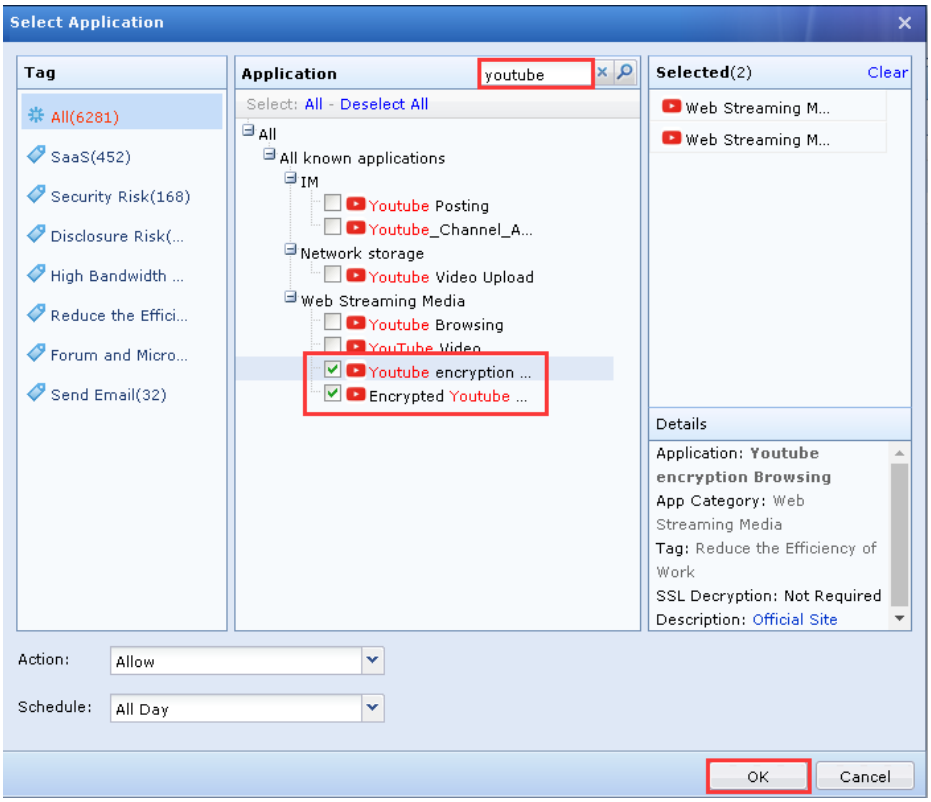
2. In between the time user access Sangfor.com, it has recorded a video rejected record. As the diagram below, it has been identify as [**Web Streaming Media**] – [**Youtube encryption Browsing**] has been rejected.



3. Currently we need to perform some editing on the policy [**Video blocking**], click on [**Add**] and select the application as [**Web Streaming Video/Youtube encryption Browsing**] and [**Web Streaming Video/Encrypted Youtube Video**], and action as [**Allow**] then click on [**Commit**].

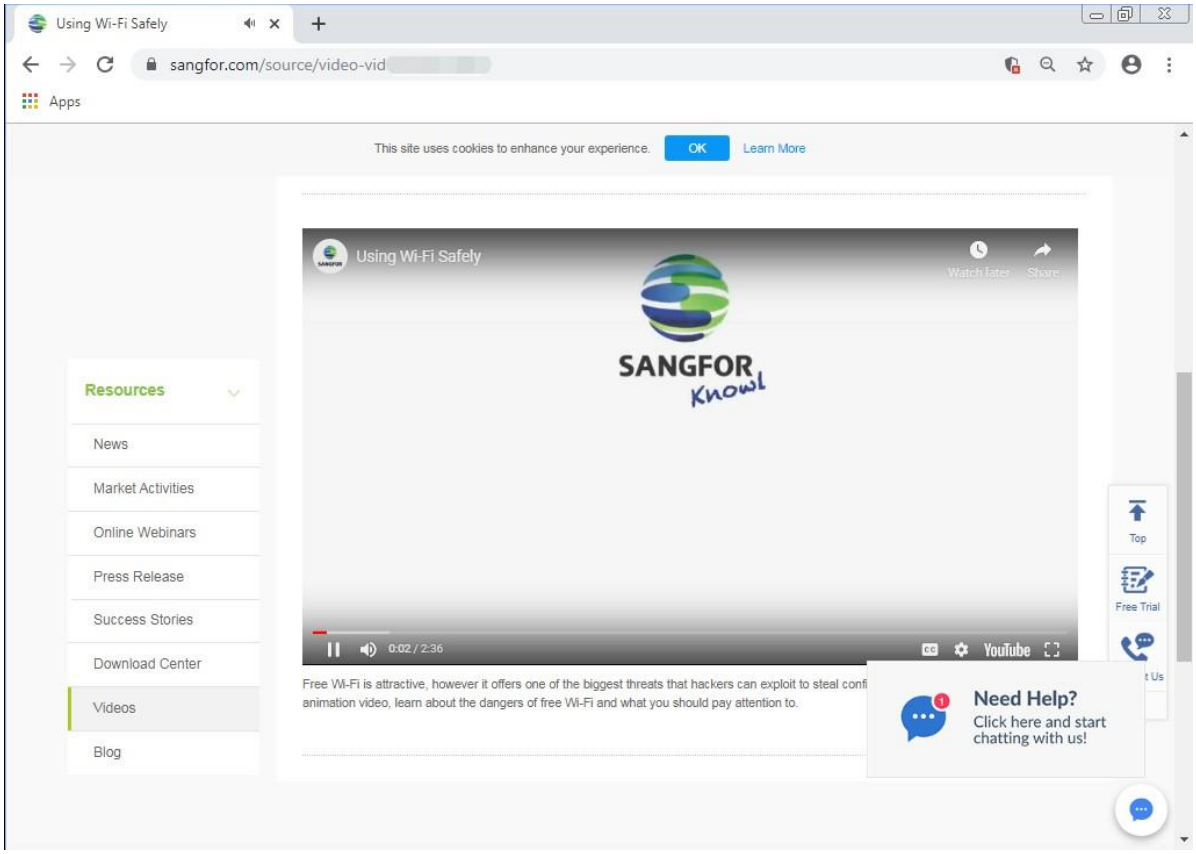


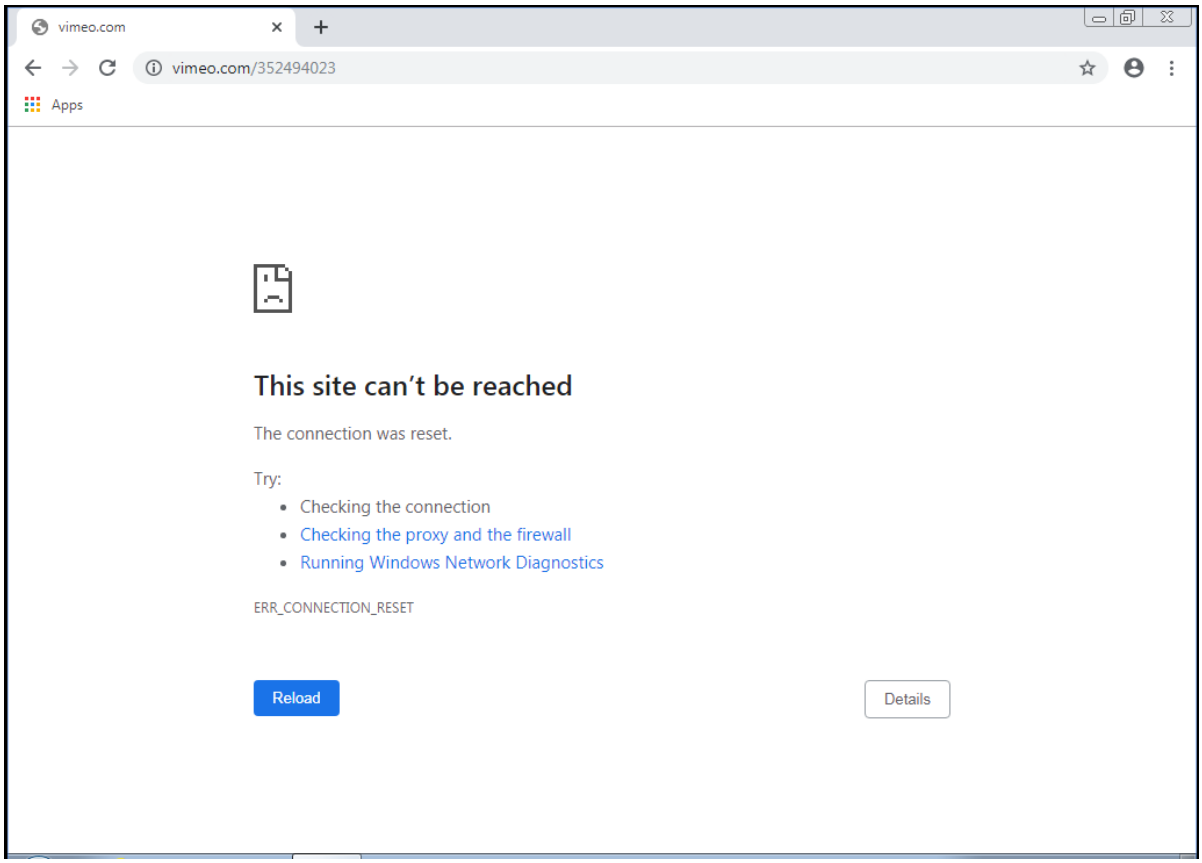
While select a **[Application]**, you may use the search bar to look for the application, for example, with insert the keyword "Youtube", you able to see the related application [**Youtube encryption browsing**] and [**Encrypted Youtube Video**], click on the application [**Youtube encryption Browsing**] you able to see the [**Application Details**] at bottom right corner, the details include the application name, application category, tag, description and the official website.

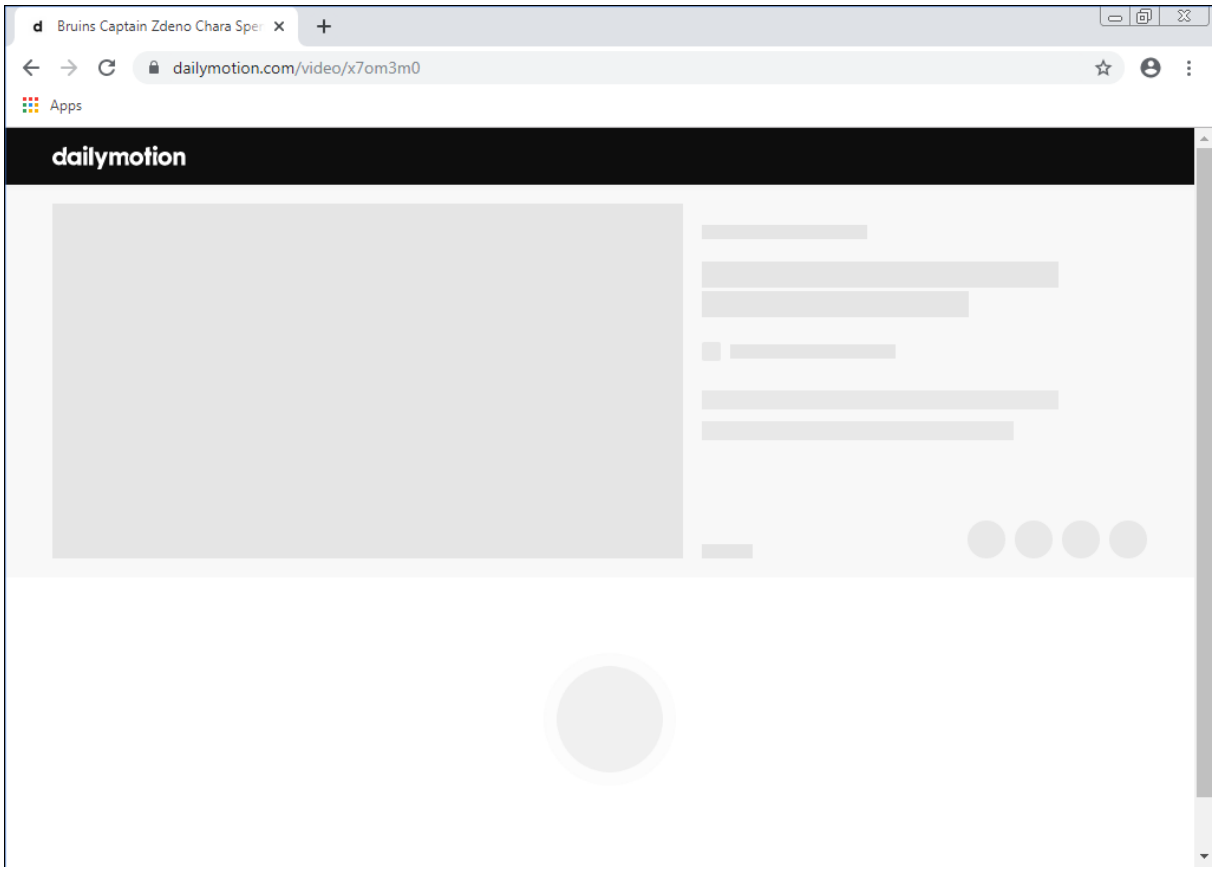


3 Testing Result

PC is able to get watch on the video at Sangfor.com, but other web video is not allowed to access or play, as the diagram below.







4 Precautions

1. If the database cannot be updated, please check on:

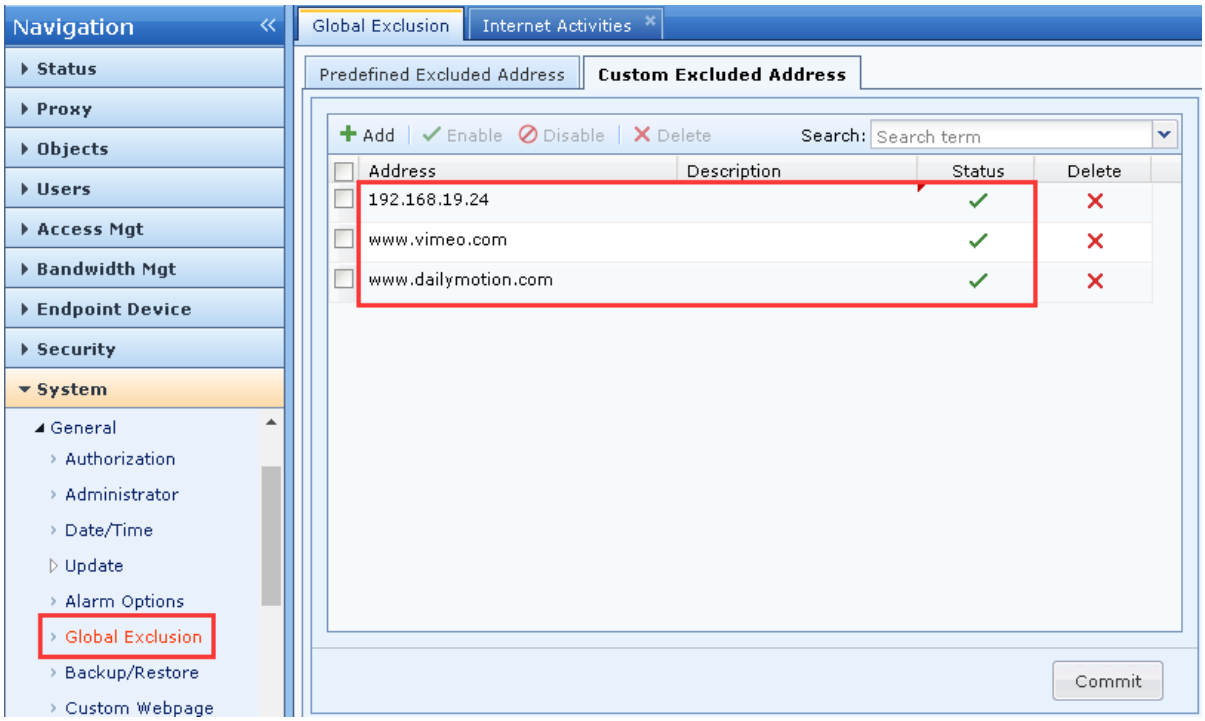
Please ensure that the license is within the validity period .

Please ensure that the device is able to visit website and resolve the domain name normally, since database update is connected to the update server with port 80 to perform updating.

By using the web console at [**System**] – [**Diagnostics**] – [**Web Console**], telnet the domain name with port number, for example : telnet www.baidu.com 80. If the result return "connect OK", means that the device is able to access to internet and resolve domain name correctly. If the connection fails, please check on the devices DNS configuration and whether the configuration of the upper proxy devices is acting as a proxy for IAM device to access the Internet.

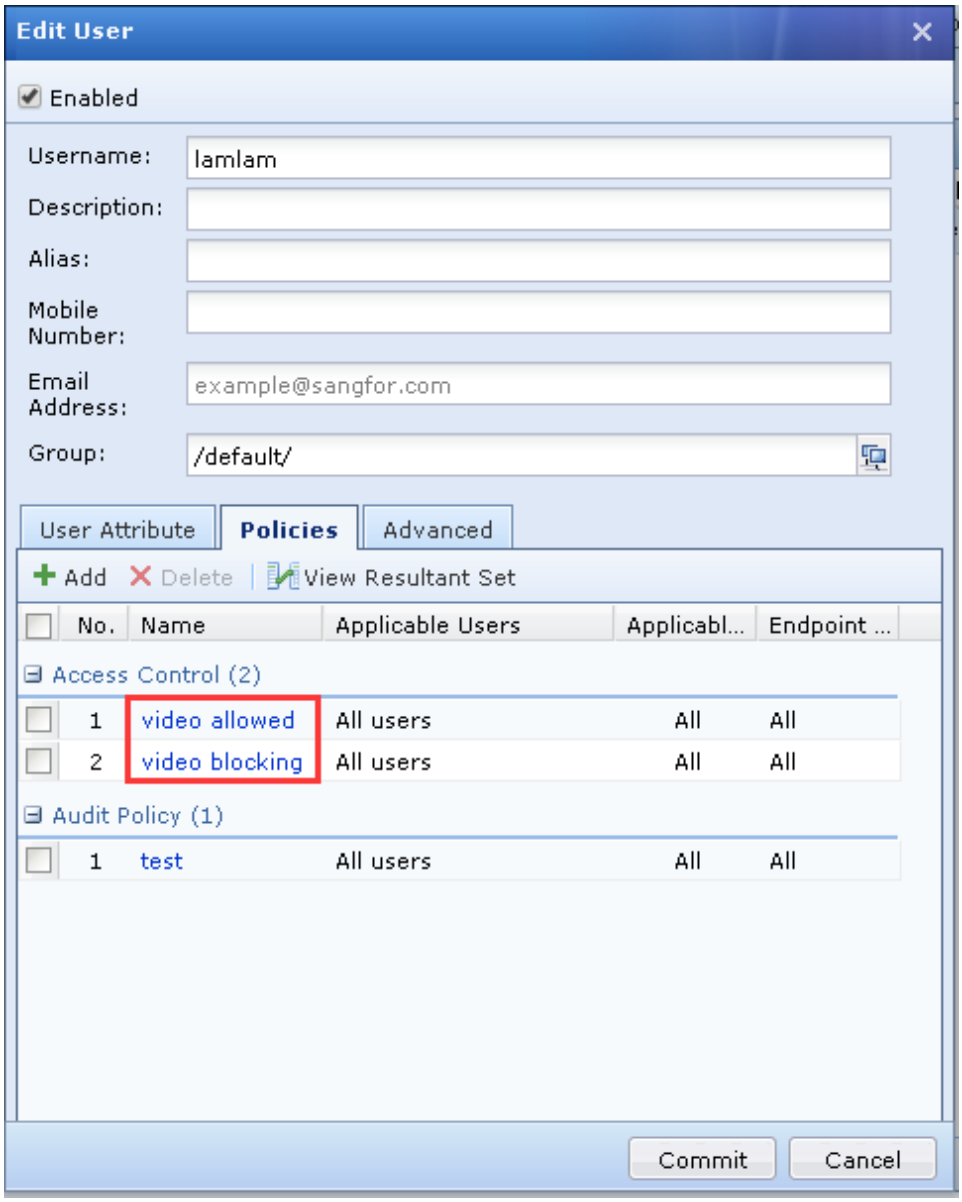
Please ensure that the communicate between IAM and update server is successful. You able to test the update server connectivity at [**System**] – [**General**] – [**Update**] – [**Database Update**] – [**Update server**]. You can test with different server to ensure that the communication is normal, if the connection is normal, try to use different server to update the database.

2. The Policies only will take effect on the user after user authenticate by IAM. If user able to access internet without going through the device, or the user IP address, Vimeo and Dailymotion domain name has added in Global Exclusion, it will not take effect by the Policies.



3. The policies matching rules is from top to bottom, once it match a policy, it will not continue to match the following policies.

For example, the diagram below shows the user has applied with two policies. The first policy is video allowed, and second policy is video blocking. As we can see the first policy on top of the second policy, video browning is allowed. What we need to block the video browsing is to push the second policy to the top, then it will block video browsing follow by allow to watch video.


Edit User
Enabled
Username:
lamlam
Description:
Alias:
Mobile Number:
Email Address:
example@sangfor.com
Group:
/default/
User Attribute
Policies
Advanced
Add
Delete
View Resultant Set
No.
Name
Applicable Users
Applicabl...
Endpoint ...
Access Control (2)
1
video allowed
All users
All
All
2
video blocking
All users
All
All
Audit Policy (1)
1
test
All users
All
All
Commit
Cancel

Copyright © SANGFOR Technologies Inc. All rights reserved.
No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.
SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.
Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc