SANGFOR

IAG

Ingress Client SSL Decryption Configuration Guide

Version 13.0.15

Change Log

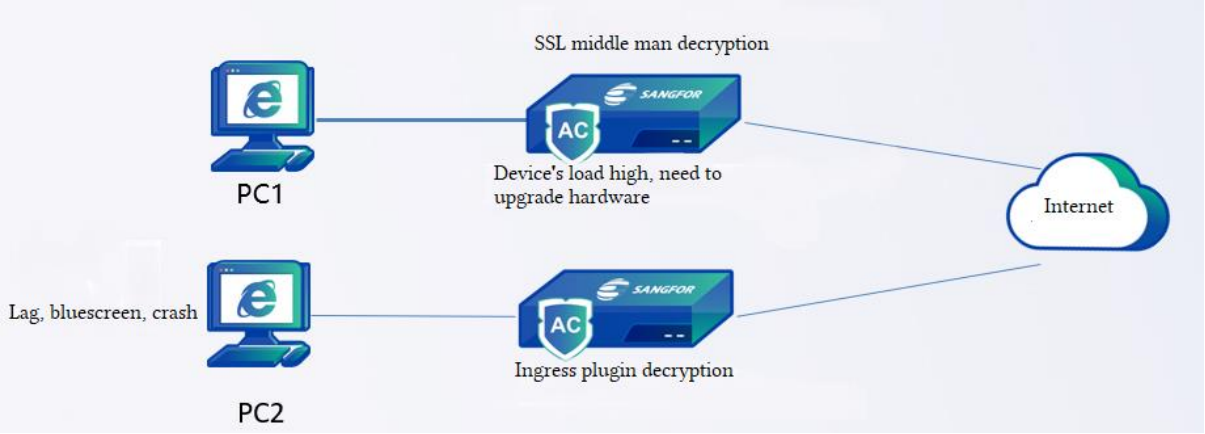
Date	Change Description
September 9, 2020	Version 13.0.15 document release.

CONTENT

Chapter 1 Demand Background

1. The traditional middleman decryption has a great impact on the performance of the device, requiring companies to upgrade and replace IAG hardware, which greatly increases the company's SSL governance costs, but there are many risks of data leakage without decryption.

2. The traditional IAG plugin decryption method is mainly using the global proxy method to audit https. This solution is limited to the version and type of the browser, which may cause compatibility issues such as blue screen and system instability, and it does not support http2 .0.



Chapter 2 Features Explanation

2.1 Introduction

- Ingress client decryption replaces the ingress plug-in decryption method to achieve high-throughput decryption, install the ingress client without perception, and decrypt with higher compatibility.

- Principle: The proxy traffic of PC surfing the Internet interacts with the server through the plug-in, and directly extracts the master session key from the system level for decryption. At present, the terminal proxy is adapted to windows, and the ingress client proxy is used to modify the data packet to simulate the NAT function, so as to achieve the function of proxying all TCP/UDP connections on Windows, and implement SSL middleman proxy, SOCKS proxy and other functions on this basis.

- Note: The proxy program is part of the ingress program and does not support separate uninstallation. It will also be uninstalled when uninstalling ingress.

2.2 Explanation

- If proxied all the SSL traffic may cause the compatibility issue, in this version, the client decryption only focuses on specific process to proxy the traffic.

- Proxy client only do decryption on specific web browser and other application that support the audit.

- Currently only support 34 applications added into the decryption list (21 web browsers, 11 Data leak applications, 2 proxy applications):

Application Type	Application name
Web Browser	Chrome
Web Browser	Firefox
Web Browser	IE 8
Web Browser	IE 9
Web Browser	IE 10
Web Browser	IE 11
Web Browser	Edge
Web Browser	Sogou web browser
Web Browser	360 Web Browser
Web Browser	QQ Web Browser
Web Browser	Maxthon Web browser
Web Browser	CM Browser
Web Browser	Opera Web browser
Web Browser	UC web browser

Application Type	Application Name
Web Browser	Chromium
Web Browser	Brave
Web Browser	Maxthon Cloud Browser
Web Browser	Torch
Web Browser	Vivaldi
Web Browser	Tor Browser
Web Browser	Epic Privacy Browser

Application Type	Application Name
Data Leak risk	Baidu Wangpan
Data Leak risk	Evernote
Data Leak risk	Youdao Note
Data Leak risk	YunZhiJia
Data Leak risk	NetEase Tunder mail
Data Leak risk	QQ – WeiYun
Data Leak risk	115
Data Leak risk	DingPan
Data Leak risk	DingDing Mail
Data Leak risk	Microsoft-onedrive
Data Leak risk	Itunes

Application Type	Application Name
Proxy Software	CC proxy
Antivirus	Rising Antivirus

- **Added support for HTTP 2.0 protocol (traditional ingress client decryption only supports HTTP 1.0 and HTTP 1.1 protocols).**

1. The proxy program downgrades the HTTP 2.0 protocol to HTTP 1.1 protocol data.

2. According to the current TLS 1.3 protocol, it will be used in conjunction with HTTP 2.0, so TLS 1.3 will also be downgraded.

3. If the downgrade fails, the server will reconnect. After the reconnection is successful, it will perform an SSL handshake with the server again and set the same as the original client hello

package to achieve a true transparent proxy, that is, the proxy program does not modify the data packets, ensuring that the PC network is not interfered.

- **Added process decryption list function.**

1. Add a process decryption list to facilitate users to specify applications for decryption.

2. The custom process exclusion is currently only valid for applications that require proxy decryption. (For example, adding the chrome browser to the list of custom excluded processes will not decrypt the chrome data).

3. The process decryption list needs to be customized in the backend (that is, add processes/applications that require proxy decryption, otherwise only the default 34 applications will be decrypted).

2.3 Comparison of Three Decryption Methods

	Ingress Client	Decryption Method	Pros and cons	Application Scenarios
Ingress client decryption	Needed	Ingress client Transparent proxy Replace certificate	Good compatibility. The decryption throughput rate is high. Richer audit content. Low consumption of IAM performance, support http2.0. Can do decryption for specified software applications. Currently only supports WINDOWS system.	Applied to routing/bridge/by pass mode, IAM audits SSL protocol data through the client.
Ingress plugin decryption	Needed	Ingress client Intercept certificate	Low consumption of IAM performance. Poor compatibility, http2.0 is not supported. Only supports WINDOWS system. Does not support the specified process for decryption.	Mainly used in bypass mode, IAM audits SSL protocol data through the client.
SSL middleman decryption	Not needed	Proxy access Replace certificate	No restrictions on the operating system. No compatibility issues. Low decryption throughput rate. High consumption of IAM performance. Does not support the specified process for decryption.	Mainly used in bridge/routing mode, the middleman audits the SSL protocol data between the endpoint and the server.

Chapter 3 Application Scenario

The ingress client is mainly used in enterprises that have many website and application decryption requirements and can accept the installation of ingress software, which can achieve high-throughput decryption and greatly reduce the load on IAG device.

Chapter 4 Configuration

4.1 Configuration Steps:

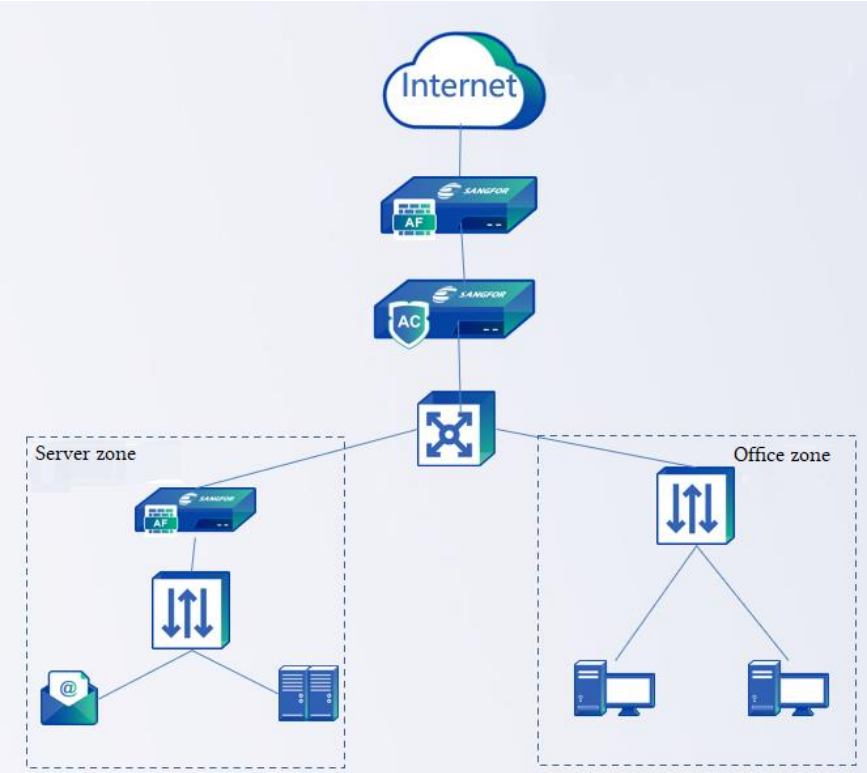
1. The ingress installation reminder function is enabled on the IAG (enabled by default).

2. The endpoint PC installs the ingress client, goes online on the IAG, and maintains network connectivity with the IAG.

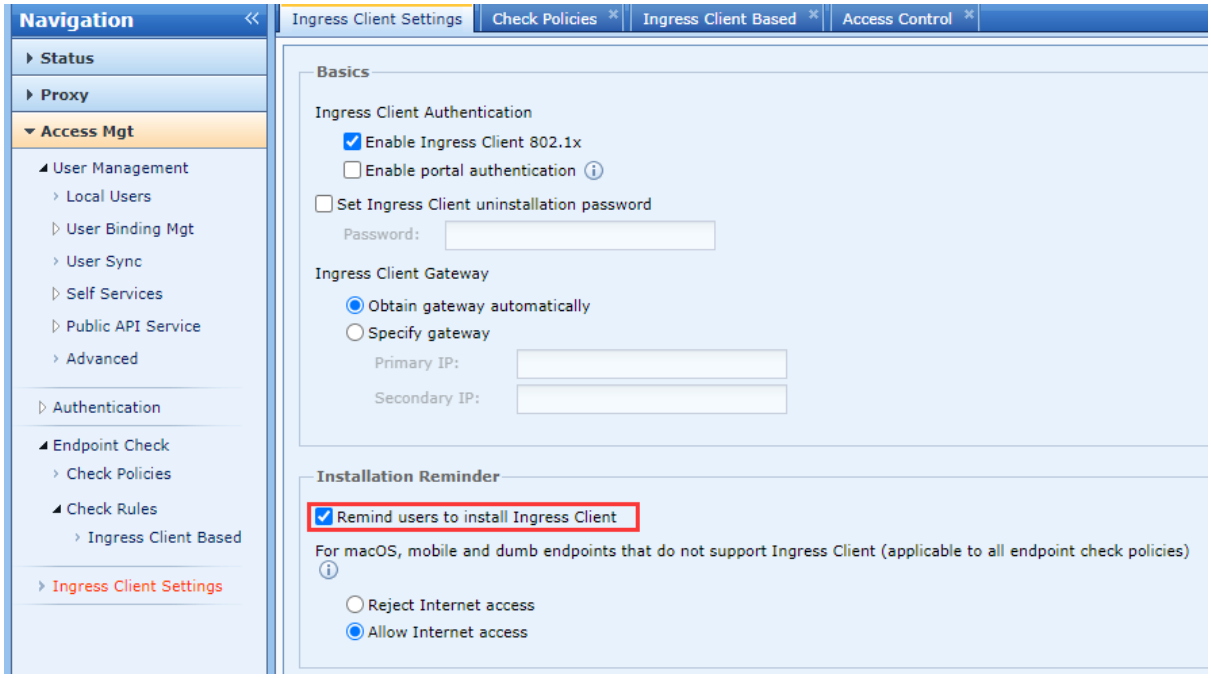
3. Enable the ingress client decryption function on the IAG **[Access Control] - [SSL Decryption] - [Ingress Client Decryption]**.

4.2 Configuration Case:

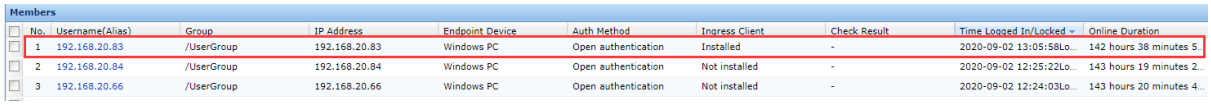
Recently, there has been an incident of data leakage within company B. For the information security of the company, company B requires that it be able to audit the Internet traffic (including https data) of internal endpoints to reduce the risk of internal employees leaking information through the Internet. The IAG hardware is old but currently company B does not want to replace the device.



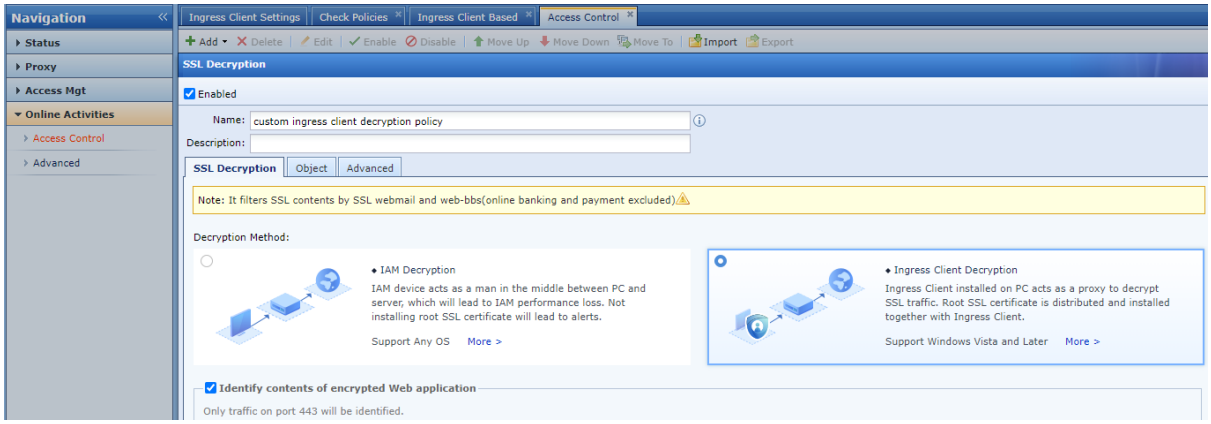
1. Enable the ingress installation reminder function on the IAG (enabled by default).

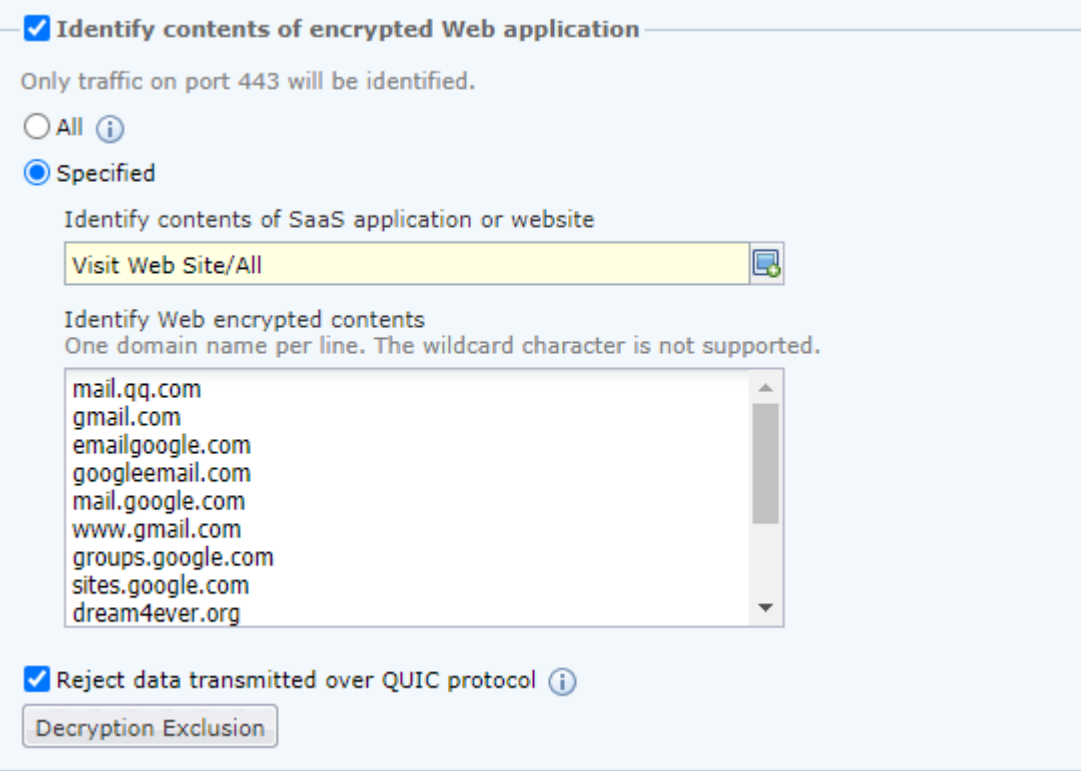


2. Ensure that the user is online on the IAG and installed the ingress client:

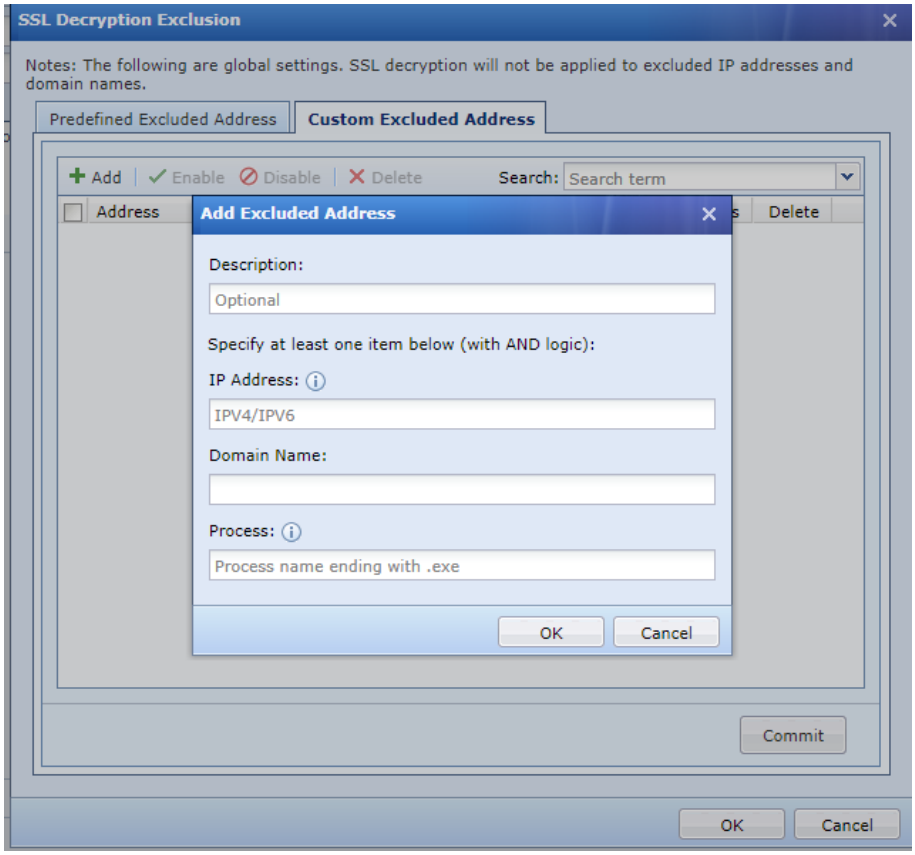


3. On the IAG, select **[Access Control] - [SSL Decryption] - [Ingress Client Decryption]** and select ingress client decryption:

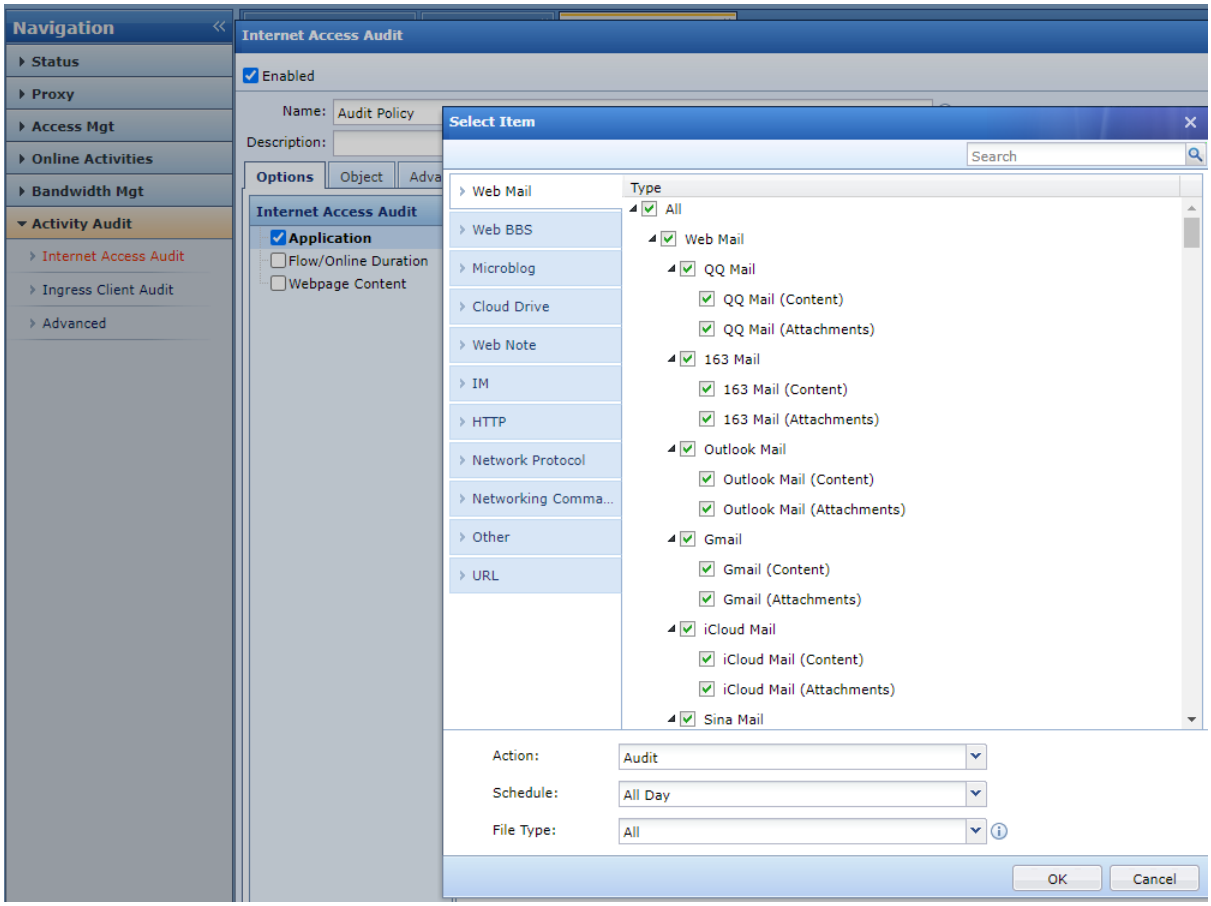




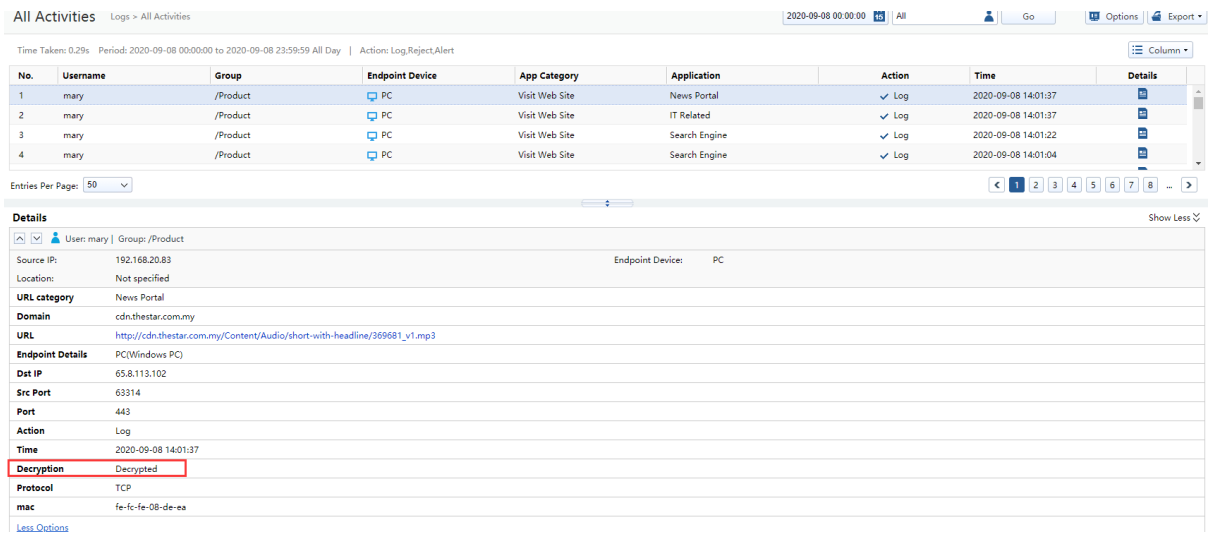
4. Customize the addresses or domain names and processes that need to be excluded on the IAG (that is, the list that does not need to be decrypted):



5. Configure internet access audit policy on IAG:



6. Verification: Enter the report center and query the audited logs:



Chapter 5 Precautions

1. This function requires the PC to install the ingress client. Currently, it only supports Windows system (XP system does not support). MAC system and Linux system can use SSL middleman for decryption.

2. This function needs to enable [Multi-function license] - [SSL content ident].

3. When SSL middleman decryption and ingress client decryption are configured at the same time, the policy list is matched from top to bottom, and only the first one that is matched takes effect.

4. The ingress plug-in decryption function has been cancelled in this version, and replaced by the ingress client decryption.

5. The ingress client only decrypts port 443 by default.

6. The ingress client has a built-in bypass financial domain name, and the bypass type is consistent with the decryption of the middleman [bank website, online banking, foreign exchange, futures market (Web), futures trading (Web)].

7. If the endpoint is a virtual machine, it is not recommended to use an ingress client for decryption. You can use an SSL middleman to decrypt.

8. IAG does not support the proxy decryption function of the ingress client when the proxy function is enabled.

SANGFOR