IAG
USB Offline Audit Configuration Guide

Version 13.0.15

Change Log

Date	Change Description
Sep 28, 2020	Version 13.0.15 document release.

CONTENT

1 USB Offline Audit Configuration Guide.

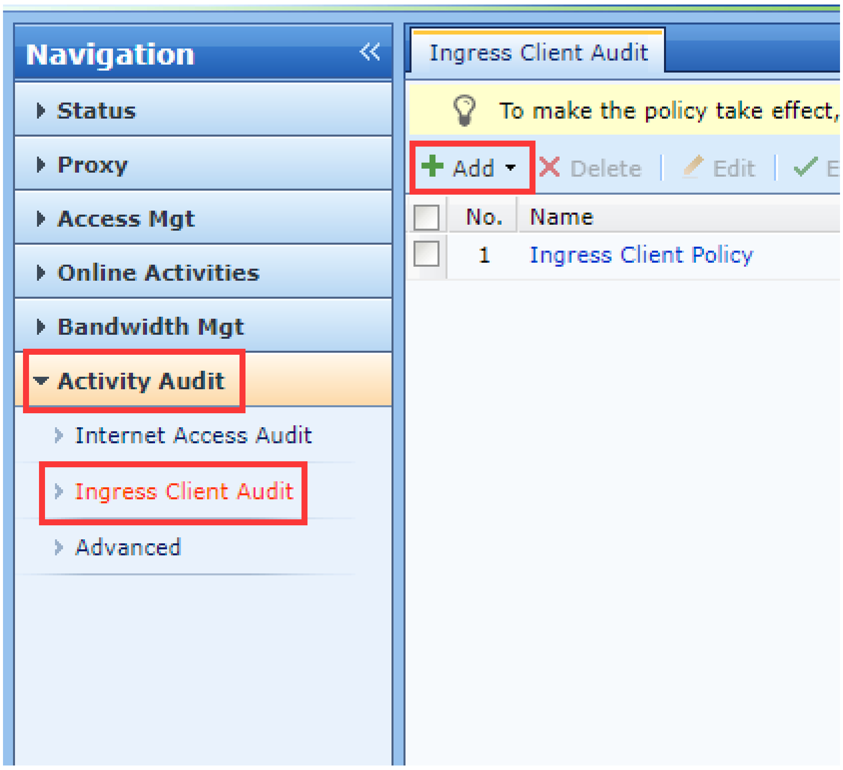
When the company laptop was taken home, it out of control of company's control, user could copy company’s information and sent confidential files through IM chat, which led to problems such as leaks. Support the audit when the ingress client is disconnected from the IAG (typical the case of taking the notebook home), currently supports offline audit of USB, and IM offline audit

2 Product Version

Version 13.0.15

3 Ingress Client Audit Policy Configuration

Go to **Activity Audit** > **Ingress Client Audit**, click **Add** to add a new **Ingress Client Audit Policy.**

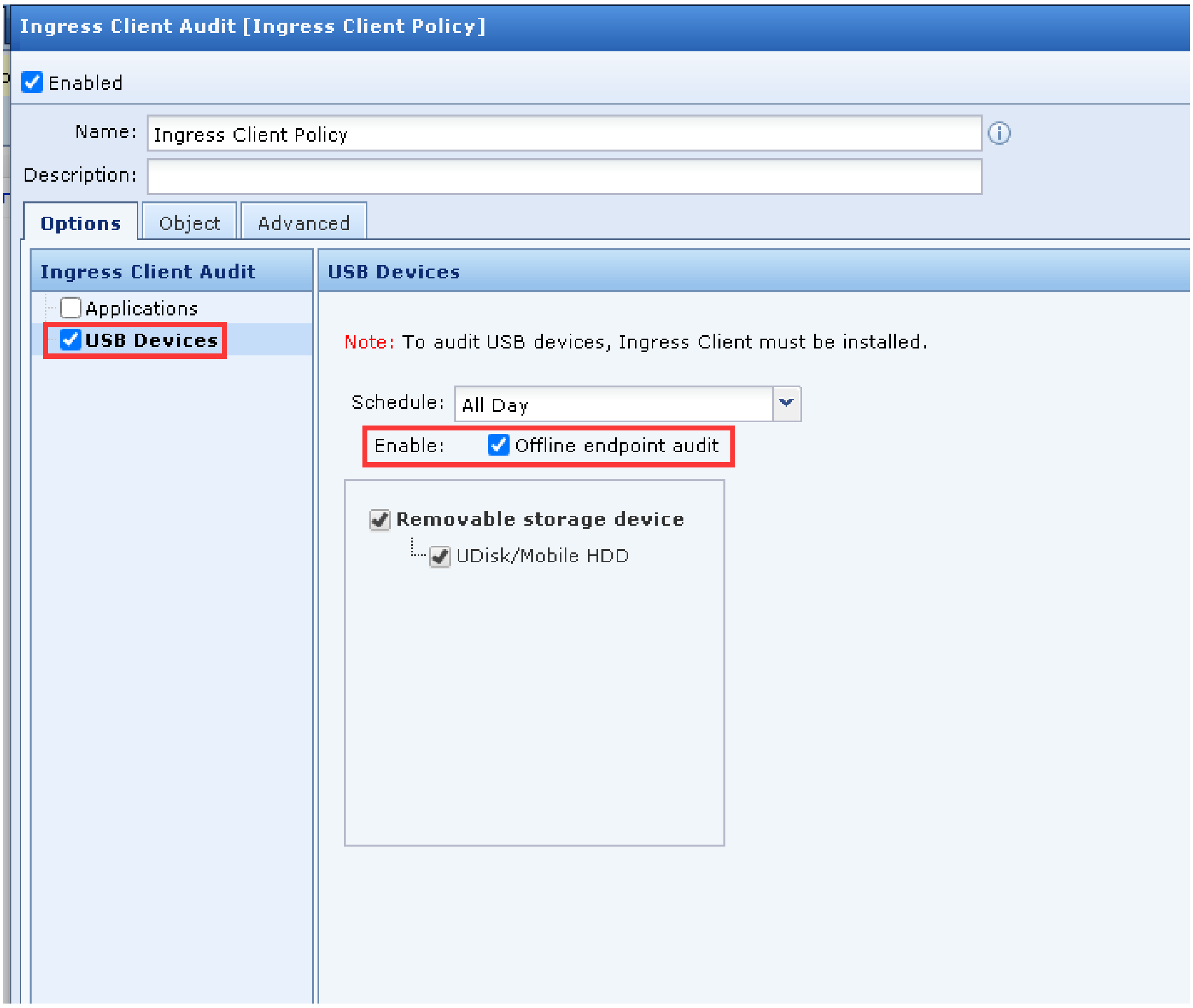


To make the policy take effect,

□	No.	Name
□	1	Ingress Client Policy

Enter the name of the policy, check the option USB Devices. Select the schedule to All Day. Check the option **Removable storage device**, Check the **offline endpoint audit** to enable the USB offline audit feature.

Note: To audit USB Devices, Ingress Client must be installed. You can click the option **Ingress Client Settings** to configure the ingress client.



Ingress Client Audit [Ingress Client Policy]

☑ Enabled

Name: Ingress Client Policy

Description:

Note: To audit USB devices, Ingress Client must be installed.

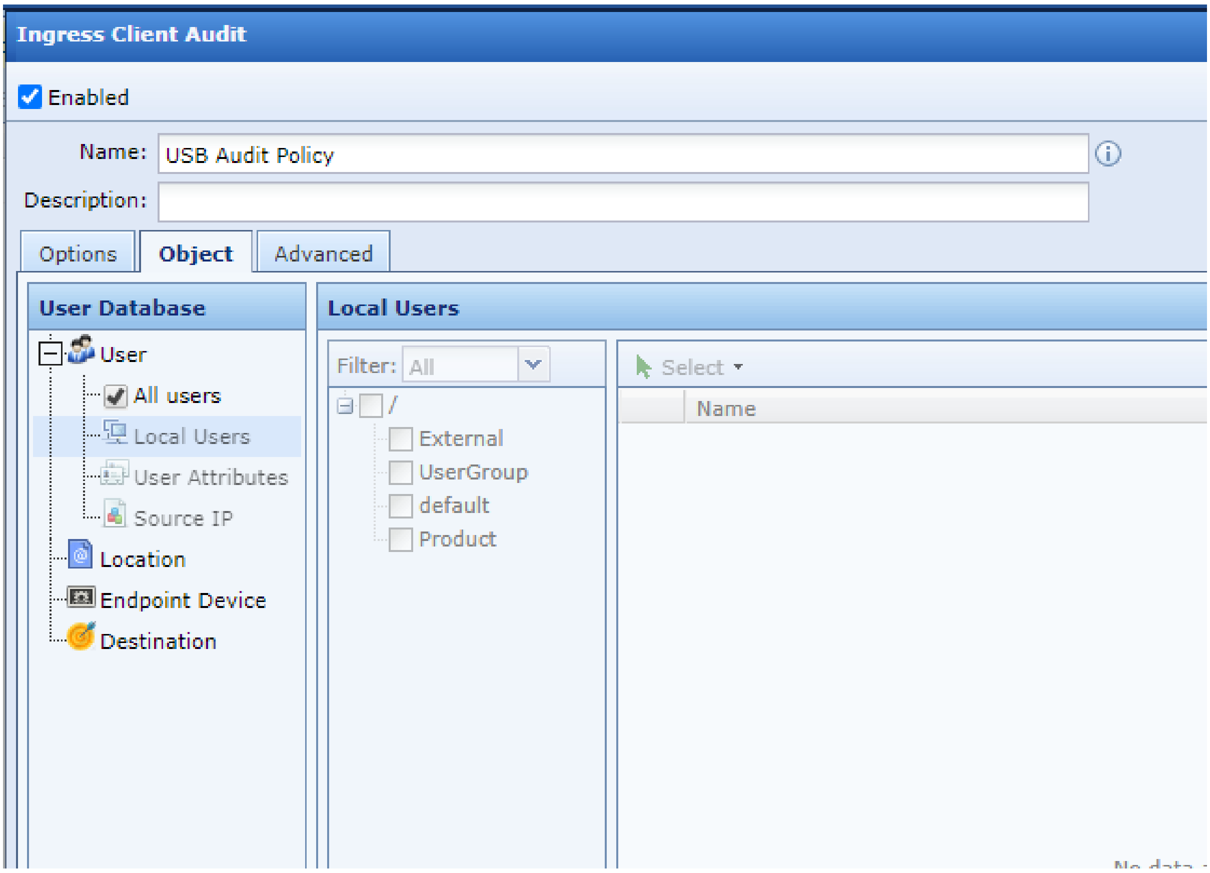
Schedule: All Day

Enable: ☑ Offline endpoint audit

☑ Removable storage device

☑ UDisk/Mobile HDD

Select the users you want to apply this USB audit policy, in this scenario, I will select **All users**.



Ingress Client Audit

☑ Enabled

Name: USB Audit Policy

Description:

4 Precaution

1. Endpoint need to passed authentication in order to let the policy working, ingress client need to installed.
2. Traffic flow from endpoint to NAT cannot be NAT, the policy not working in NAT environment.
3. Offline USB audit Supported windows 7 and above. IM offline audit supported all windows.
4. The TCP port 886 need to open between IAG and endpoint.
5. When the ingress client fails to connect to the gateway or does not receive the heartbeat packet response within 2 minutes, switch to offline mode.