SANGFOR

# IAG

## External Device Control Configuration Guide

### Version 13.0.15

# Change Log

| Date | Change Description |
|---|---|
| September 10, 2020 | Version 13.0.15 document release. |
| | |

# CONTENT

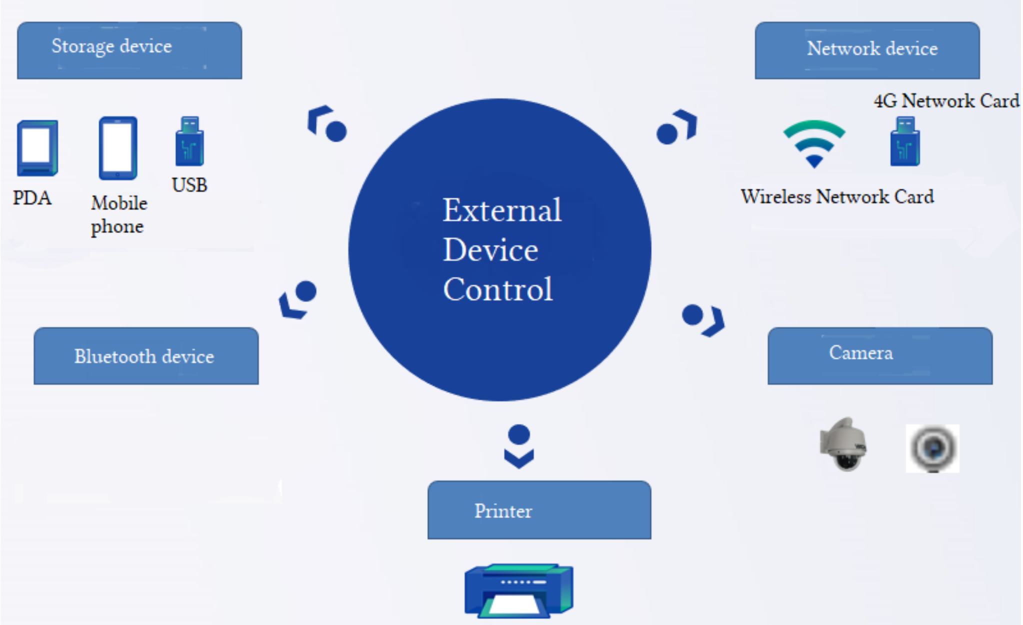
# Chapter 1 Demand Background

Intranet endpoints are arbitrarily connected to peripheral devices that cannot be controlled, such as connected with USB flash drives to spread viruses, and connected to wireless 4G network cards to open up the internal and external networks, resulting in data leakage.

# Chapter 2 Features Explanation

## 2.1 Explanation

- Support the disabling of storage devices, network devices, Bluetooth devices, cameras and printers.



- Support refined control of USB and portable devices (mobile phones, tablets, etc.).

    - **Refined control of USB:**

        1. Reject - USB is not allowed.

        2. Read - USB is allowed, but content cannot be written to the USB (you can copy the file and open the file in the USB).

        3. Read/write - Equivalent to no control.

        4. Alert – Send alarm when the USB is inserted, the event alarm function of the device needs to be enabled.

    - **Refined control of portable devices:**

        1. Allow - Equivalent to not control.

        2. Disable - Prohibit access.

        3. Alert - Send alarm when inserted, the event alarm function of the device needs to be enabled.

## 2.2 Implementation steps

1. Install the ingress client on the endpoint (currently only supports Windows).

2. The ingress client connects to the IAG device and distribute the policy to the local (users are required to be online on IAG).

3. Two control methods:

    - By using the system group policy to prohibit the installation of drivers for peripheral devices, so as to achieve the purpose of controlling peripherals (Windows XP system and the home version systems do not have group policies so they do not support external device control).

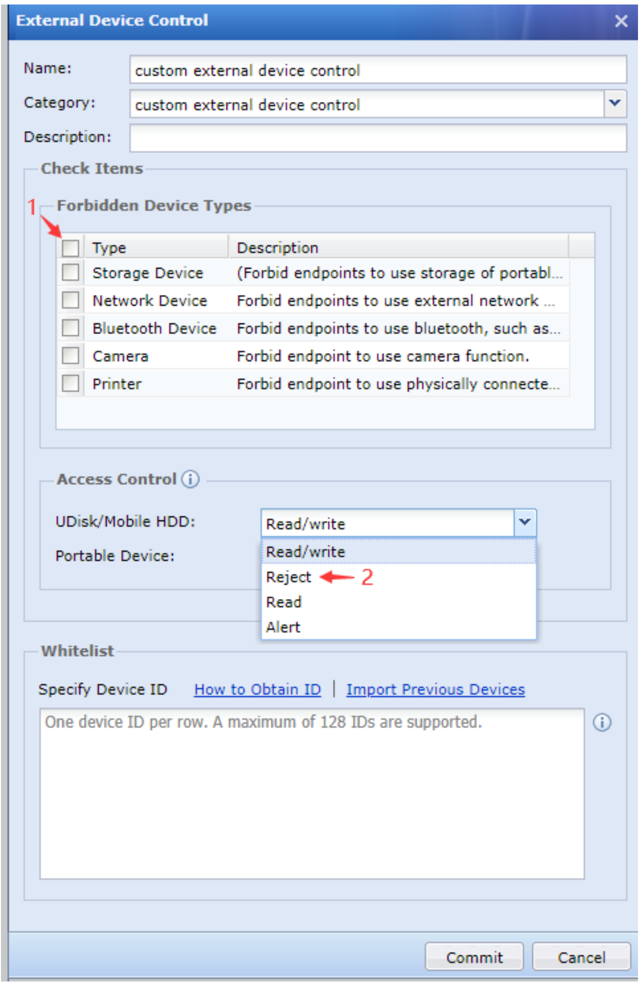
    - Refined control, use the system's device manager function and process injection method to achieve the refined control of USB and portable devices (only support Win7 and above OS, regardless of whether it is home version).

4. When the ingress client and IAG cannot communicate with each other, the group policy control method still takes effect, and the control function can continue to be implemented (refined control does not take effect).

Two ways to disable:

1. The group policy method: use the system group policy to implement, control the enabling and disable function, controlled by 1 in the picture below.

2. Implementation of refined management and control: use the system's device manager function to enable and disable it, configuration as shown in 2 in the picture below.



External Device Control

Name: custom external device control

Category: custom external device control

Description:

Check Items

Forbidden Device Types

| □ Type | Description |
|---|---|
| □ Storage Device | (Forbid endpoints to use storage of portabl... |
| □ Network Device | Forbid endpoints to use external network ... |
| □ Bluetooth Device | Forbid endpoints to use bluetooth, such as... |
| □ Camera | Forbid endpoint to use camera function. |
| □ Printer | Forbid endpoint to use physically connecte... |

Access Control

UDisk/Mobile HDD: Read/write

Portable Device:

Whitelist

Specify Device ID

One device ID per row. A maximum of 128 IDs are supported.

If you selected 1, the two disabling methods will take effect at the same time, and the group policy will be used first to disable. In disabling failure scenario (domain user scenario, home version does not have a group policy scenario), use the device disable method to prohibit; if you select 2 to reject, it uses the device manager to disable method.

Whitelist setting:

1. The whitelist needs to fill in the hardware ID of the peripheral device, you can refer to the device ID obtain guide, there are tools to get the hardware ID.

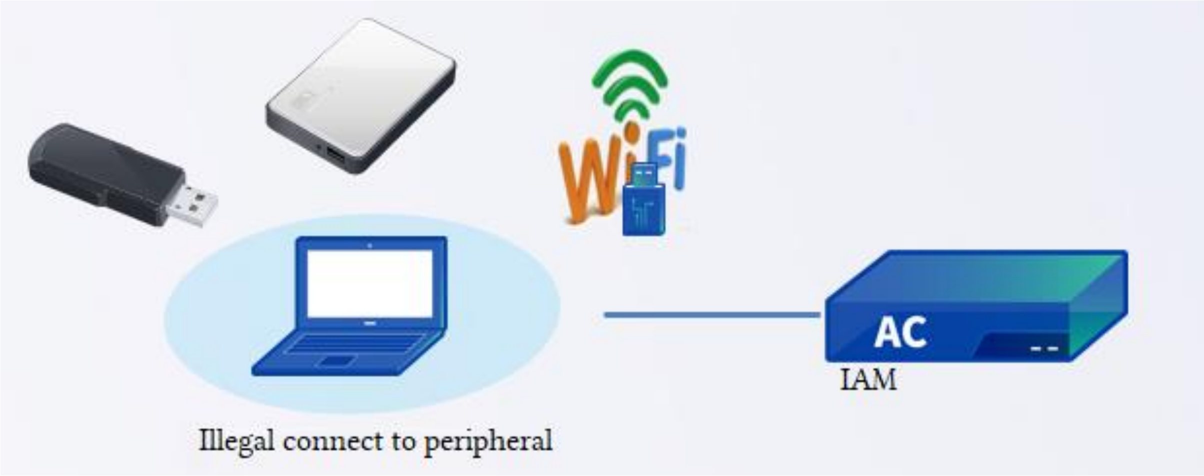
2. The hardware ID is composed of the hardware ID of each device and the patriline of the computer, therefore the hardware ID of each peripheral device on each computer is different.

3. The quick import function of previous device is only effective for USB and portable hard disk. Others such as network devices, Bluetooth devices, etc. do not support quick import and need to use tools.

4. The tool usage method can be obtained from the device ID obtain guide.

# Chapter 3 Application Scenario

The external device control function is mainly used when the endpoint has illegal access to the peripheral, such as inserting a USB to copy data, inserting a wireless network card to access the external network, etc., which can prohibit the endpoint from privately connecting to the peripheral.



# Chapter 4 Configuration

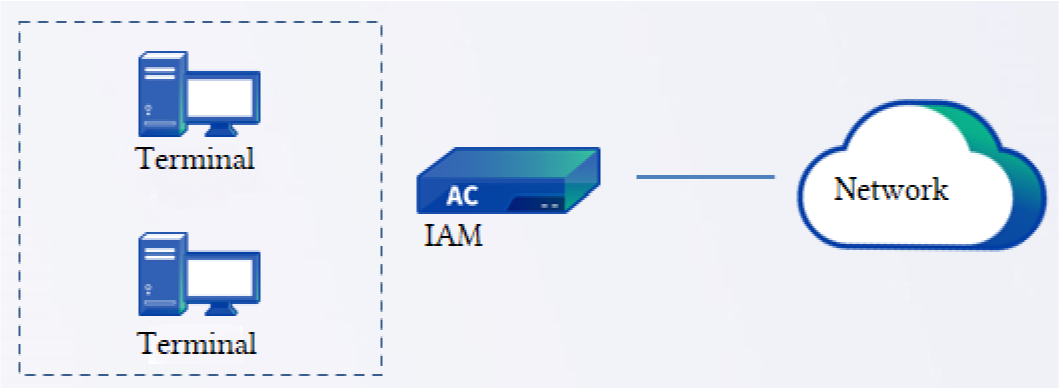
## 4.1 Configuration Steps:

1. Create new external device control policy and configure specific check items or control items.

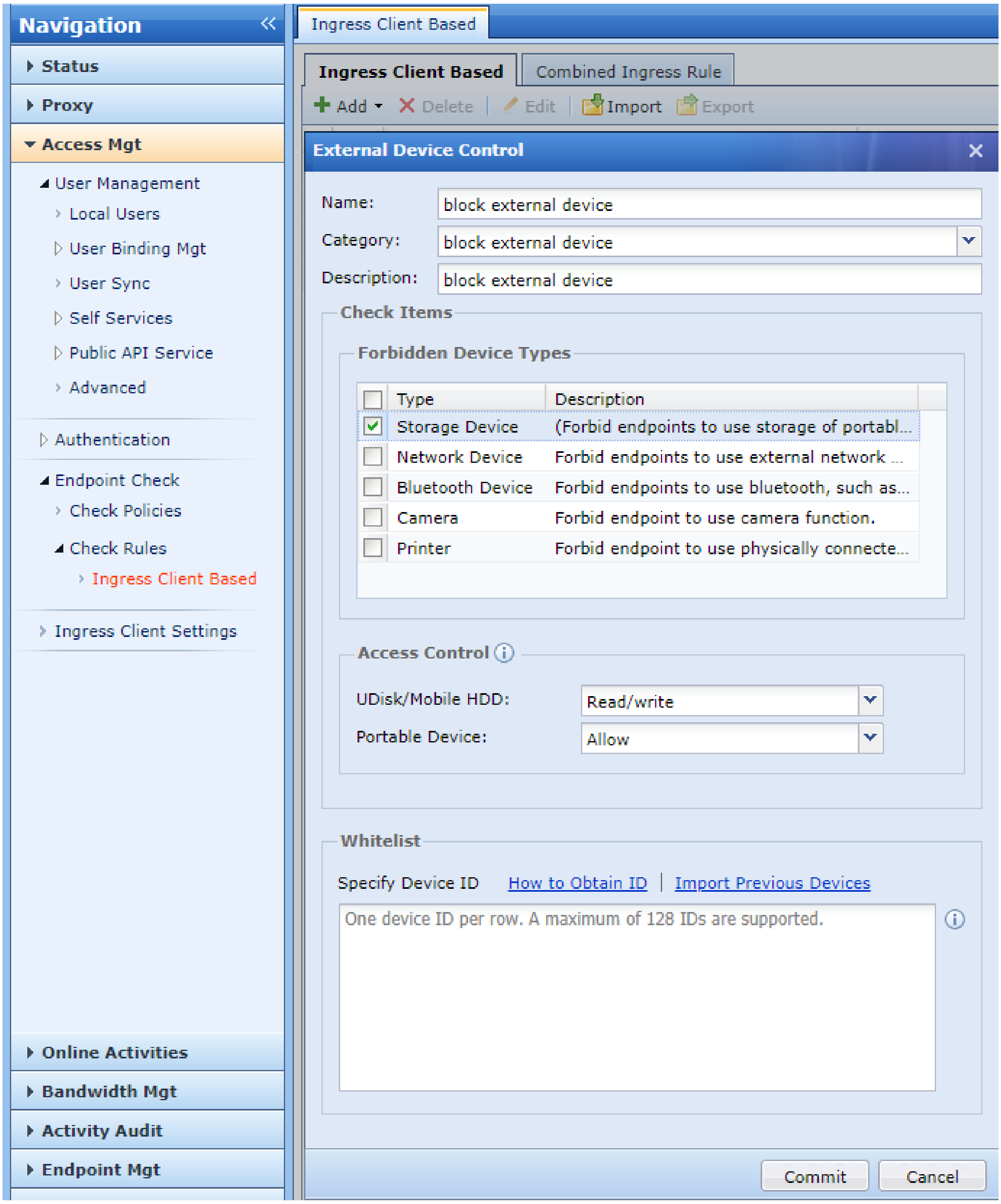
2. Configure endpoint check policy, associate to the previously configured policy, and select the applicable users.

## 4.2 Configuration Case:

The customer's private network deploys an IAG, endpoints are prohibited to access devices such as USB and portable hard drives.



Create a new external device control policy, define the name, category and description, and then tick the storage device.



External Device Control

Name: block external device

Category: block external device

Description: block external device

Check Items

Forbidden Device Types

| ☐ | Type | Description |
|---|---|---|
| ☑ | Storage Device | (Forbid endpoints to use storage of portabl... |
| ☐ | Network Device | Forbid endpoints to use external network ... |
| ☐ | Bluetooth Device | Forbid endpoints to use bluetooth, such as... |
| ☐ | Camera | Forbid endpoint to use camera function. |
| ☐ | Printer | Forbid endpoint to use physically connecte... |

Access Control

UDisk/Mobile HDD: Read/write

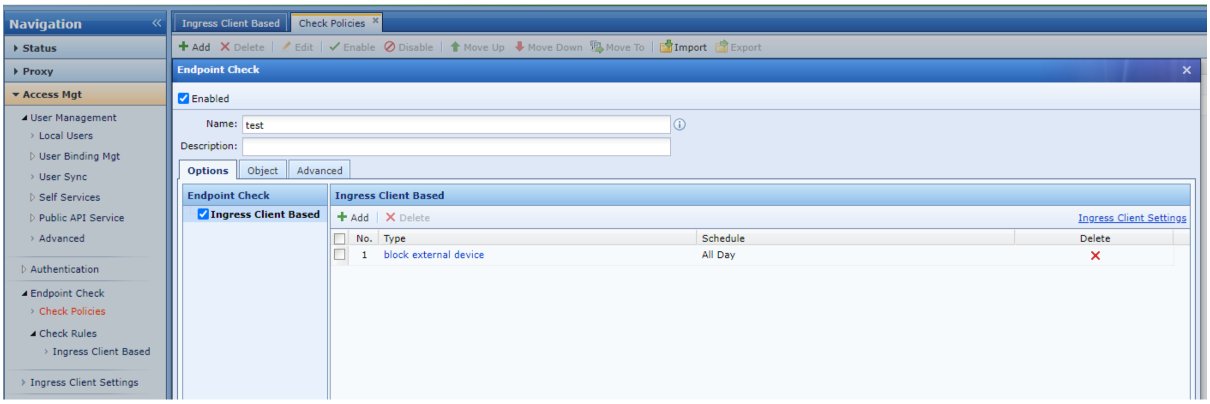
Portable Device: Allow

Whitelist

Specify Device ID How to Obtain ID | Import Previous Devices

One device ID per row. A maximum of 128 IDs are supported.

Create a new endpoint check policy and associate to the previously configured policy and select applicable users.



Endpoint Check

☑ Enabled

Name: test

Description:

Endpoint Check

☑ Ingress Client Based

Ingress Client Based

| □ | No. | Type | Schedule | Delete |
|---|---|---|---|---|
| □ | 1 | block external device | All Day | ✕ |

# Chapter 5 Precautions

1. The terminal can only obtain the policy after passing the authentication, and the ingress client must be installed for the external device control functions.

2. There must be no NAT in the path from the terminal to the IAG device. If there is NAT, the endpoint check function will not take effect.

3. Windows XP system and all family version systems do not have group policies, and do not support group policy control methods.

4. Refined control only supports Win7 and above, regardless of whether it is home version.

5. Use group policy to disable storage devices. If the computer has a second non-USB internal hard disk besides the system disk, it will also be disabled. Need to add whitelist to allow it.

6. Group policy is currently found to be incompatible with 360 Tianqing. Do not use group policy for environmental peripheral control with Tianqing.

7. Refined management and control are only for storage devices with USB interface: USB portable hard disk portable devices.

8. Combined ingress rules do not apply to external device control rules (combined ingress rules are for old ingress rules such as process and file based rule).

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