

How to work with Blacklist feature?

Version: 1.0

Release Date: 30th, Dec, 2021

Catalog

How to work with Blacklist feature?	1
1. Introduction.....	3
1. 1. Overview	3
1. 2. Applicable Model	3
1. 3. Before You Start.....	3
1. 4. Connection Diagram.....	3
2. Operation Guide	4
2. 1. Restrict All IP Calls.....	4
2. 2. Restrict Specified Calls	4

1. Introduction

1.1. Overview

Some customers may get following abnormal phenomenon, like 1) device rings itself but no one calls it; or 2) device doesn't make a call out even when someone presses its DSS key. This may be caused by anonymous calls on device from outside. To avoid anonymous calls, we can work with blacklist feature on devices, this document introduces the configuration steps of blacklist feature.

1.2. Applicable Model

Fanvil PA2, i12, i16V, i18S, i20S, i30, i23S, i31S, i32V and i33V.

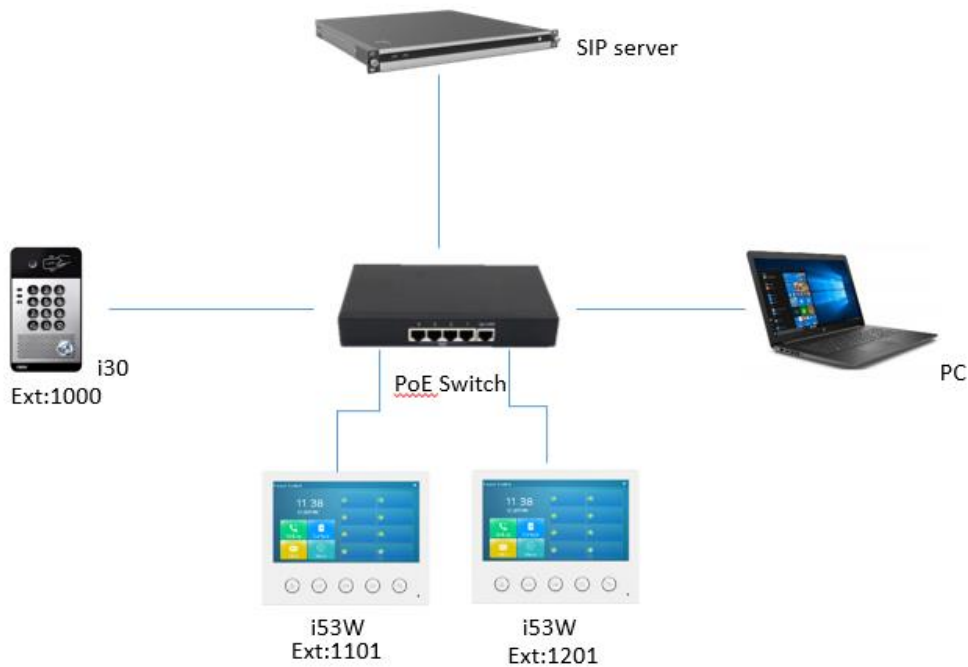
1.3. Before You Start

Step1. Prepare PC, PoE switch, network cable, i30 door phone and at least two IP phones or indoor units;

Step2. Connect PC, IP phones(indoor units) and i30 door phone to the same PoE switch with network cable;

Step3. Make IP phones(indoor units) and i30 door phone register to the same SIP server.

1.4. Connection Diagram



2. Operation Guide

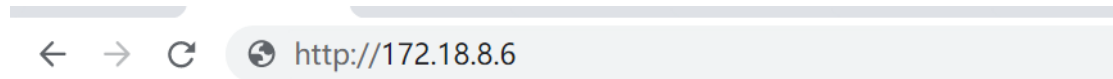
In this part, we use i30 door phone as example to introduce the detailed steps on setting up blacklist feature, two i53W are also used for tests.

Before we start, please make sure i30 and two i53W are registered to the same SIP server and can call each other, about registration, you may check other FAQ documents.

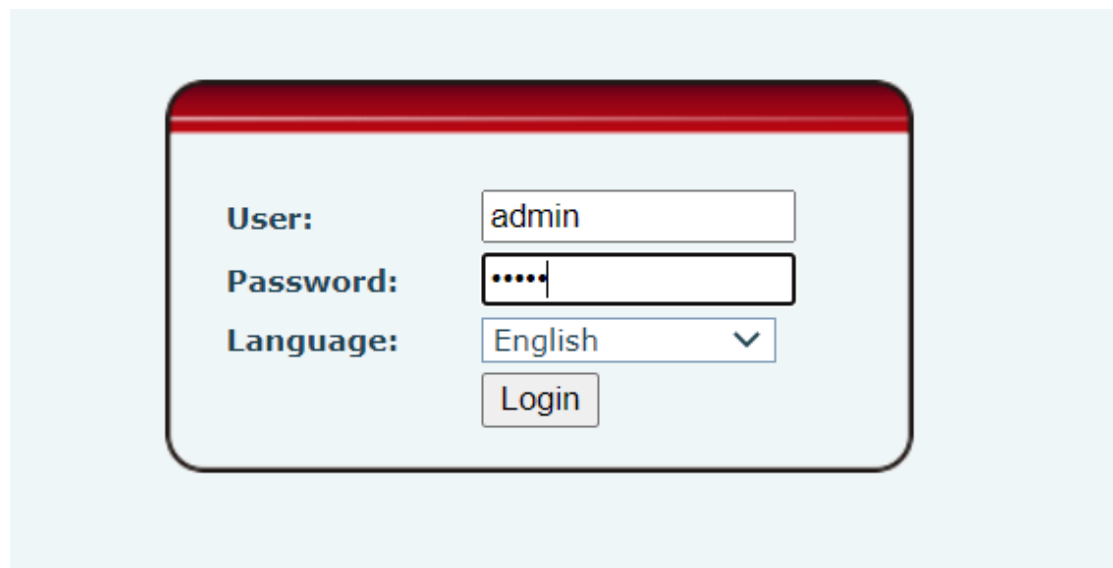
2.1. Restrict All IP Calls

As we all know, device can receive direct IP calls and ordinary calls from SIP server, most anonymous calls are IP calls. If you are working with SIP server and don't need direct IP calls, you can forbid all IP calls by enabling strict UA match, steps are as following:

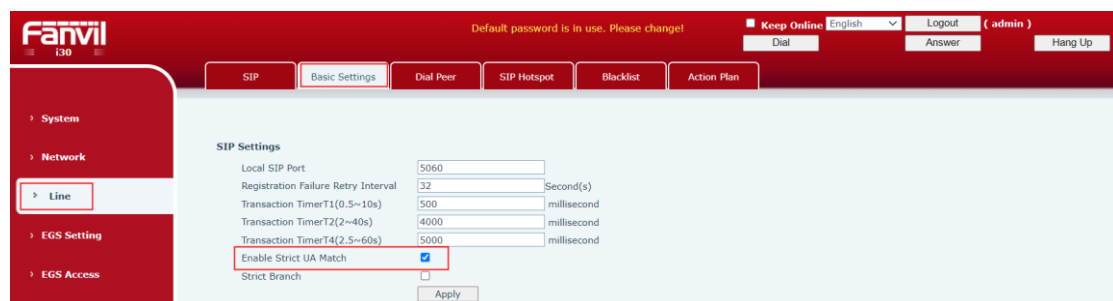
Step1. Open web browser and input device's IP address in browser;



Step2. Input web login username and password;



Step3. Go to Line→SIP page, Enable Strict UA Match;

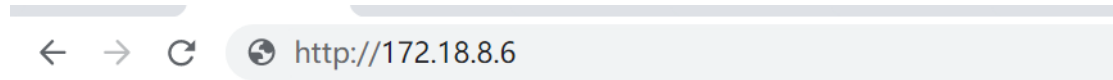


Then any device makes direct IP calls to i30, it will reject the call directly.

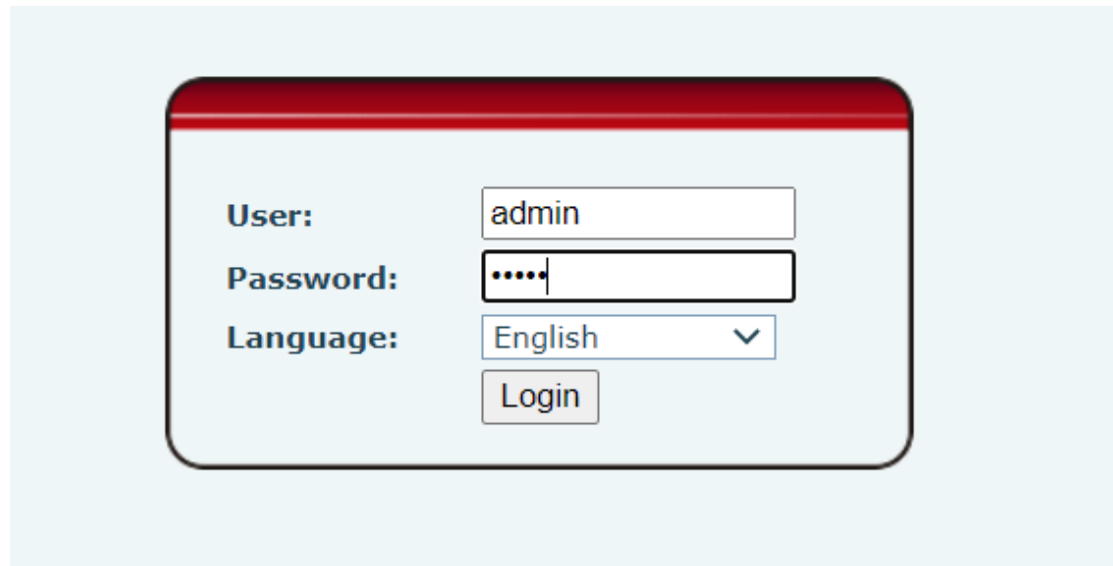
2.2. Restrict Specified Calls

Some anonymous calls are not direct IP calls, or customers need IP calls but just want to allow some IPs or extension numbers to call in, then they can work with Blacklist feature. Steps are as following:

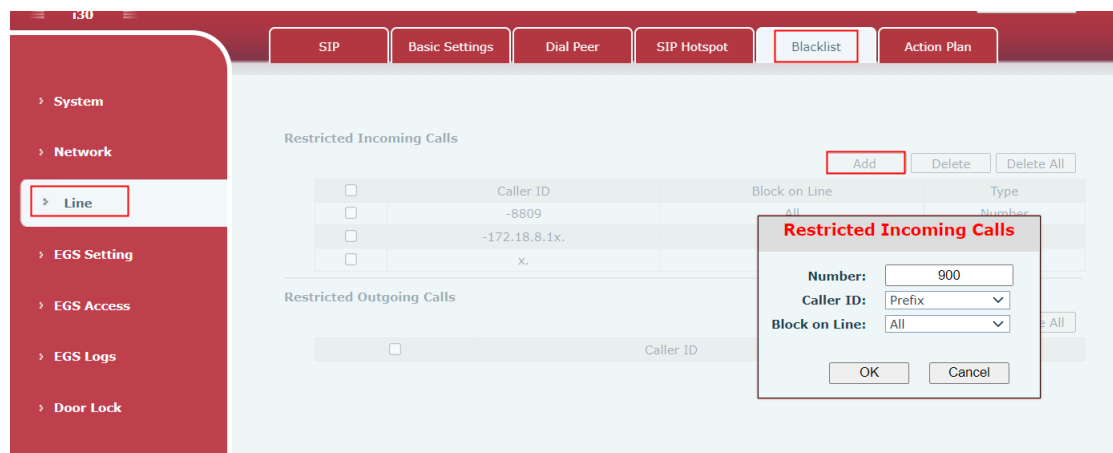
Step1. Open web browser and input device's IP address in browser;



Step2. Input web login username and password;



Step3. Go to Line→Blacklist page, click Add to add one blacklist or whitelist rule.



Number: Input the number or prefix of number which you need add to the list.

Numbers start with character “-” will be added to whitelist, other numbers will be added to blacklist. For example, if you input ‘-8809’ in **Number** option, then it will be recognized as whitelist number; if you input ‘1009’ in **Number** option, then it will be recognized as blacklist number.

Caller ID: Select Prefix or Number

1)Prefix: All the numbers which starts with the content user inputs in **Number** option will be added as Blacklist or Whitelist number.

For example, if you input ‘900’ in **Number** option and select ‘**Prefix**’ as **Caller ID**, then all the extension numbers start with 900 will be recognized as blacklist number.

2)Number: Only the specified number user inputs in Number option will be added as Blacklist or

Whitelist number.

For example, if you if you input '-800' in **Number** option and select '**Number**' as **Caller ID**, then the extension number 800 will be recognized as whitelist number.

Block on Line: Select from line1/line2/all, if you select line1, the rule only works on line1, but IP calls doesn't distinguish line1 or line2.