Oct 21, 2020 02:09

Domain Whitelist (Allow Origin) Configuration - Admin Instruction

This Admin Instruction explains how to configure domain whitelist to protect PBX from cross-site request forgery (CSRF) attacks.

Created: April 2018

Updated: June 2018

WMS Version: 3.88

Permalink: https://confluence.wildix.com/x/SwBuAQ

- Introduction
- Configuration of Domain Whitelist

IMPORTANT: Trusted domains must be added to a domain whitelist! Please note that any Web API / PBX API integration will stop working if the domain is not added.

If you are using Firewalls, make sure the following pool of IP addresses is present in your Whitelist for access to Wildix microservices:

3.122.16.10
3.122.188.91
3.122.21.65
3.122.78.100

Introduction

The main purpose of adding domains to a whitelist is to protect PBX from cross-site request forgery (CSRF) attacks.

How it works:
Generally, web requests are restricted to only the current domain, per the same-origin policy. The same-origin policy is a significant security standard implemented by web browsers to prevent requests against a different origin (e.g., different domain) than the one from which it was served. At the same time, the same-origin policy also prevents legitimate interactions between a server and clients of a known and trusted origin.

To allow such interactions, Cross-origin resource sharing (CORS) is used. It is a standard that allows cross-domain requests. CORS can be defined as a set of headers that allow a browser and server to communicate about which requests are/ are not allowed. The simplest way is to check that the request originates from a trusted site, using Origin request header. For example,

```
Origin: https://ucua.wildixin.com
```

If a server decides that the request should be allowed, it sends `Access-Control-Allow-Origin` header with the same origin that was sent. For example,

```
Access-Control-Allow-Origin: https://ucua.wildixin.com
```

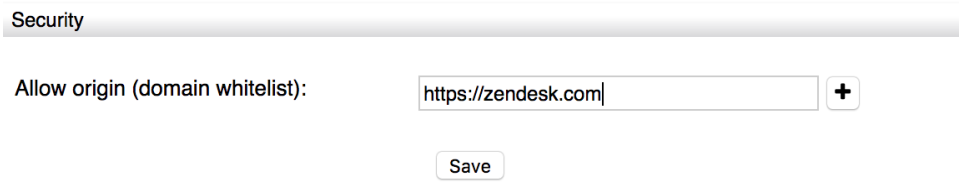
If this header is missing or the origins don't match, then the request is not allowed. If origins match, then a browser processes the request.

Configuration of Domain Whitelist

Whitelist is configured in WMS -> Settings -> PBX -> Security.

To configure a domain whitelist:

1. Enter IP address/ domain name and click **+** to add the value:



Supported formats of IP address/ domain name:

- http://<domain or IP address> / https://domain or IP address>
- http://<domain or IP address>:port / https://<domain or IP address>:port

Examples:

- https://ucua.wildixin.com/
- https://ucua.wildixin.com:4443/
- http://ucua.wildixin.com/

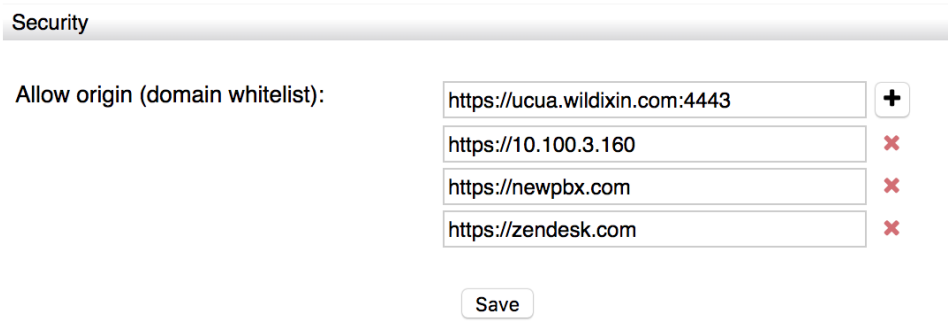
It is also possible to add patterns using asterisk symbol "*" that replaces letters, numbers and dashes:
Examples:

- https://*.wildixin.com
- *://*.wildixin.com
- https://*.*.wildixin.com

> ⚠ Note: IP range can't be specified in this case. You just need to enter one IP address.

> ⚠ Note: Wildix Portal "https://pbx.wildix.com/" and Wildix Chrome Extension "https://chrome-extension://lobgohpoobpijgfegnlhdnppegdbomkn" are hardcoded in the whitelist, there is no need to add them.

2. After you enter all the values, click **Save:**



To delete the value from the list, click **X.**