



IAM

Https to submit Username and password Configuration Guide

Version 12.0.42



Change Log

Date	Change Description
Dec 9, 2020	Version 12.0.42 document release.

CONTENT

Chapter 1 requirements	1
Chapter 2 Configuration Guide	1
Chapter 3 Result	3
Chapter 4 Precaution.....	4

Chapter 1 requirements

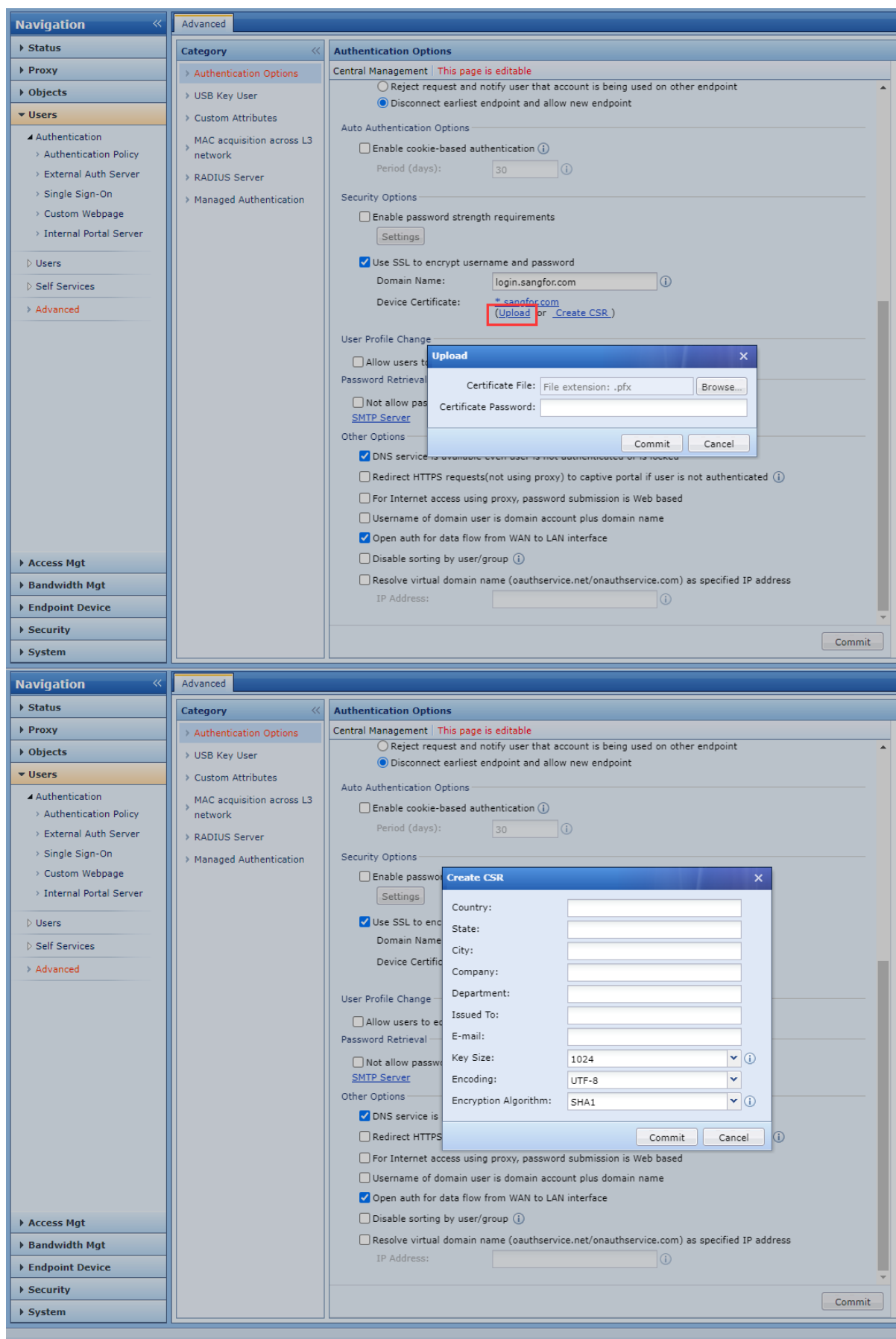
Currently the website based on the https become more popular and secure, some of the user required to use the https login page with domain name instead of using the http user login page, in this scenario, below is the guide to make the username and password submit through the https login page.

Chapter 2 Configuration Guide

1. Navigate to the Users -> Advanced -> Authentication Options and enable the “Use SSL to encrypt username and password”

The screenshot shows the Sangfor IAM configuration interface. On the left, the 'Navigation' pane has 'Users' expanded, and 'Advanced' is selected. The main area shows 'Authentication Options' under the 'Advanced' tab. A red box highlights the 'Use SSL to encrypt username and password' checkbox, which is checked. Below this, the 'Domain Name' is 'login.sangfor.com' and the 'Device Certificate' is '*.sangfor.com' with links for 'Upload' and 'Create CSR'. Other options include 'Enable cookie-based authentication', 'Enable password strength requirements', 'DNS service is available even user is not authenticated or is locked', 'Redirect HTTPS requests(not using proxy) to captive portal if user is not authenticated', 'For Internet access using proxy, password submission is Web based', 'Username of domain user is domain account plus domain name', 'Open auth for data flow from WAN to LAN interface', 'Disable sorting by user/group', and 'Resolve virtual domain name (oauthservice.net/onauthservice.com) as specified IP address'.

2. Input the domain name inside the SSL content, in this scenario, we will use the login.sangfor.com as the domain name for the login page.
3. Import the https device cert with the pfx format or create the CSR to obtain the device cert. In this scenario, we will use the device cert for the *.sangfor.com to make the device trusted by other root cert.



- After imported, click the **commit** to make the device take effect.

Chapter 3 Result

1. Create an authentication policy for the device under the IAM's Lan and select the authentication method as password based.

Authentication Policy

☒ Enable

Name: 192.168.20.89

Description:

Objects

Auth Method

Action

Auth Method:

☐ Open authentication

☒ Password based

☐ Single Sign-On(SSO)

☐ None (requests are rejected always)

Auth Server: Local user database

☐ Self registration:

☐ Account login with WeChat

☐ Account Login with SMS Code

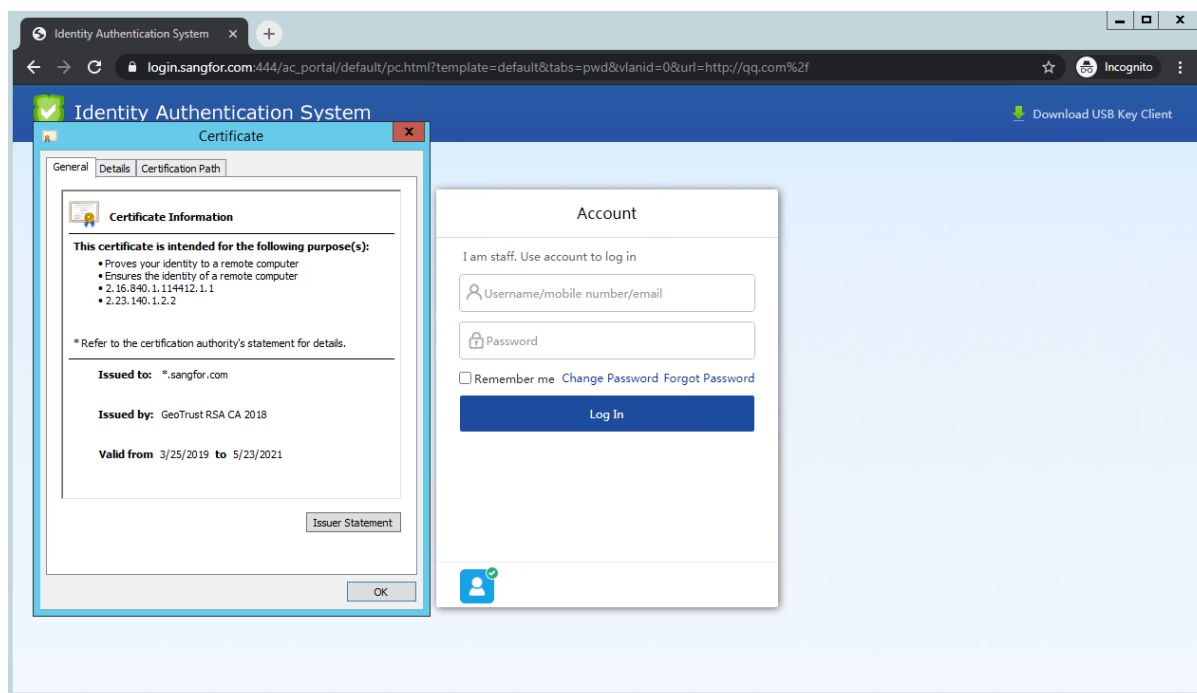
Captive Portal

Captive Portal: Without Slideshow and Terms of Use Preview

Login Redirection: Previously visited webpage

Back Next

2. After the device will redirect the http or https request to the https login page, you may also manually key in the domain name like login.sangfor.com to direct access to the https login page.



Chapter 4 Precaution

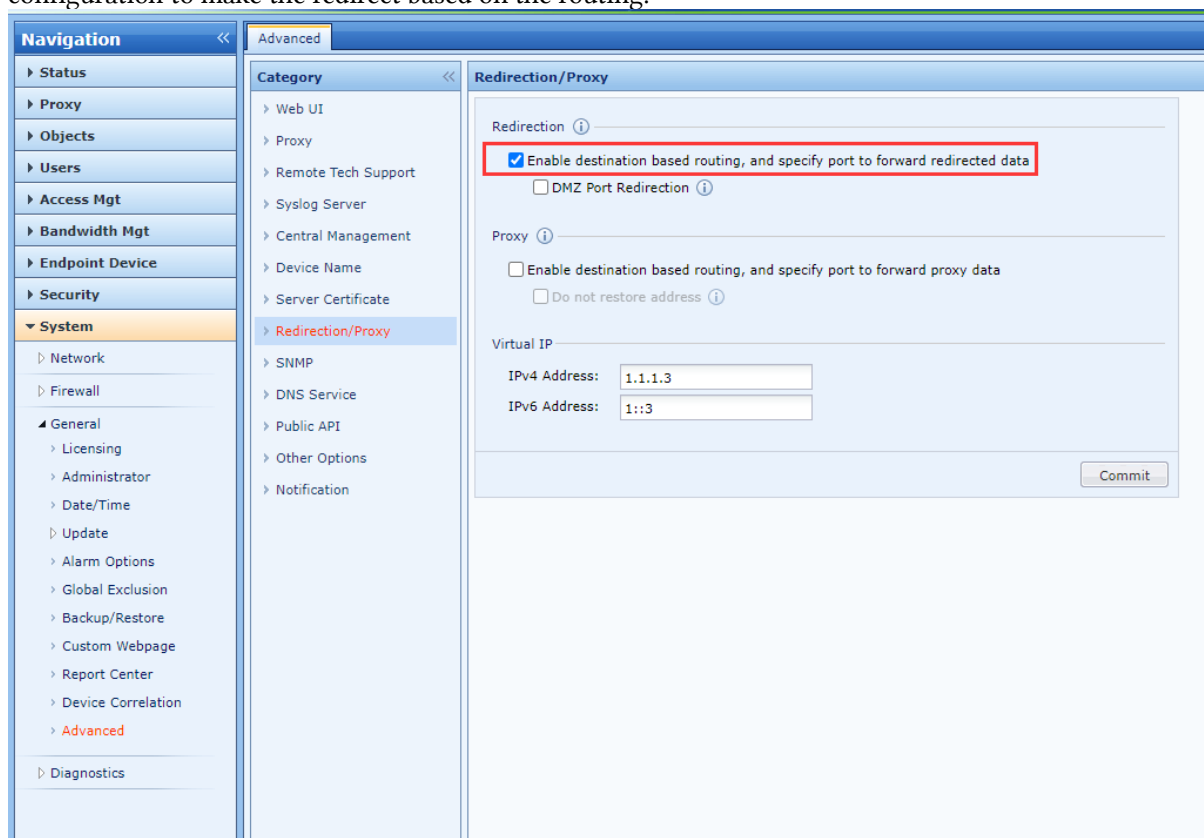
1. In order to ensure the endpoint device able to access to the domain name, the domain name required to resolve to **the device's actual IP address or virtual IP (Bridge mode)**, this required to configure in Internal DNS server or the endpoint device's host file.

In this scenario, we configure the endpoint device's host file to make the device to redirect to the device IP address.

Below is the host file configuration for the Microsoft Windows PC endpoint device, every type of endpoint OS has own configuration method, **it is recommended to resolve the domain name via the Internal DNS server.**

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com             # x client host
#
# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
1.1.1.3             iam.com
192.168.20.88 login.sangfor.com
```

2. In order to resolve the device and redirect to the actual IP address, you need to check the configuration to make the redirect based on the routing.



3. For the IAM 12.0.42 version has upgrade the https login page to support TLS 1.2 version, it is recommended to use this version and above to avoid the TLS warning from the latest version of web browser.
4. The port number used for the https login page is port 444.
5. For the redirection from the https page required to install the IAM SSL root cert to avoid prompt certification any errors.

Navigation

- Status
- Proxy
- Objects
- ▼ **Users**
 - Authentication
 - Authentication Policy
 - External Auth Server
 - Single Sign-On
 - Custom Webpage
 - Internal Portal Server
 - Users
 - Self Services
 - **Advanced**
- Access Mgt
- Bandwidth Mgt
- Endpoint Device
- Security
- System

Category

- **Authentication Options**
- USB Key User
- Custom Attributes
- MAC acquisition across L3 network
- RADIUS Server
- Managed Authentication

Authentication Options

Central Management | This page is editable

☐ Reject request and notify user that account is being used on other endpoint

☒ Disconnect earliest endpoint and allow new endpoint

Auto Authentication Options

☐ Enable cookie-based authentication ⓘ

Period (days): ⓘ

Security Options

☐ Enable password strength requirements

[Settings](#)

☒ Use SSL to encrypt username and password

Domain Name: ⓘ

Device Certificate: ⓘ

[\(Upload\)](#) or [Create CSR](#)

User Profile Change

☐ Allow users to edit endpoint information ⓘ

Password Retrieval

☐ Not allow password retrieval through SMS message ⓘ

[SMTP Server](#)

Other Options

☒ DNS service is available even user is not authenticated or is locked

☒ **Redirect HTTPS requests(not using proxy) to captive portal if user is not authenticated ⓘ**

☐ For Internet access using proxy, password submission is Web based

☐ Username of domain user is domain account plus domain name

☒ Open auth for data flow from WAN to LAN interface

☐ Disable sorting by user/group ⓘ

☐ Resolve virtual domain name (oauthservice.net/onauthservice.com) as specified IP address

IP Address: ⓘ

[Commit](#)



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

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