



# **IAM**

## **Panduan Konfigurasi Https untuk dikirim Username dan password**

**Versi 12.0.42**



## Catatan Perubahan

Tanggal	Deskripsi Perubahan
Dec 9, 2020	Rilis Dokumen Versi 12.0.42.

# Daftar Isi

Bab 1 Persyaratan.....	1
Bab 2 Panduan Konfigurasi.....	1
Bab 3 Hasil .....	3
Bab 4 Tindakan Pencegahan.....	4

## Bab 1 Persyaratan

Saat ini website berbasis https menjadi lebih populer dan aman, beberapa user diharuskan menggunakan halaman login https dengan domain name sebagai gantinya menggunakan halaman login pengguna http, dalam skenario ini, di bawah ini adalah panduan untuk membuat username dan password dikirimkan melalui halaman login https.

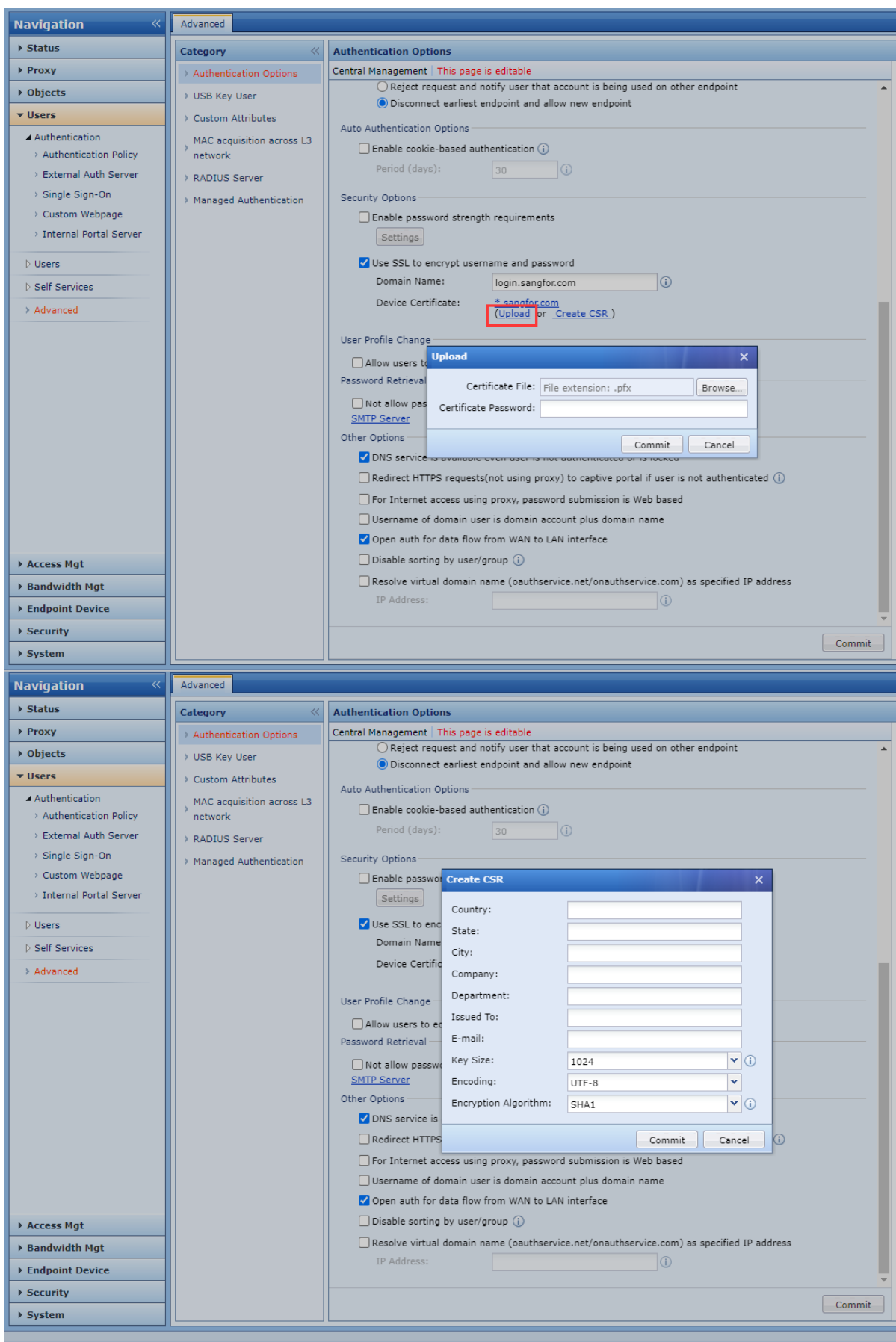
## Bab 2 Panduan Konfigurasi

1. Navigate ke Users -> Advanced -> Authentication Options dan aktifkan "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' category. The 'Central Management' section has two radio buttons: 'Reject request and notify user that account is being used on other endpoint' (unselected) and 'Disconnect earliest endpoint and allow new endpoint' (selected). The 'Auto Authentication Options' section has a checkbox for 'Enable cookie-based authentication' (unselected) and a 'Period (days)' field set to 30. The 'Security Options' section has a checkbox for 'Enable password strength requirements' (unselected). The 'Use SSL to encrypt username and password' checkbox is checked and highlighted with a red box. Below it, the 'Domain Name' is 'login.sangfor.com' and the 'Device Certificate' is '\*.sangfor.com' with links for 'Upload' and 'Create CSR'. The 'User Profile Change' section has a checkbox for 'Allow users to edit endpoint information' (unselected). The 'Password Retrieval' section has a checkbox for 'Not allow password retrieval through SMS message' (unselected) and a link for 'SMTP Server'. The 'Other Options' section has several checkboxes: 'DNS service is available even user is not authenticated or is locked' (checked), 'Redirect HTTPS requests(not using proxy) to captive portal if user is not authenticated' (unselected), 'For Internet access using proxy, password submission is Web based' (unselected), 'Username of domain user is domain account plus domain name' (unselected), 'Open auth for data flow from WAN to LAN interface' (checked), 'Disable sorting by user/group' (unselected), and 'Resolve virtual domain name (oauthservice.net/onauthservice.com) as specified IP address' (unselected). The 'IP Address' field is empty. A 'Commit' button is at the bottom right.

2. Masukkan domain name di dalam konten SSL, dalam skenario ini, kami akan menggunakan login.sangfor.com sebagai domain name untuk halaman login.
3. Import sertifikat perangkat https dengan format pfx atau buat CSR untuk mendapatkan sertifikat perangkat.

Dalam skenario ini, kami akan menggunakan sertifikat perangkat untuk \*.sangfor.com untuk membuat perangkat dipercaya oleh sertifikat root lainnya.



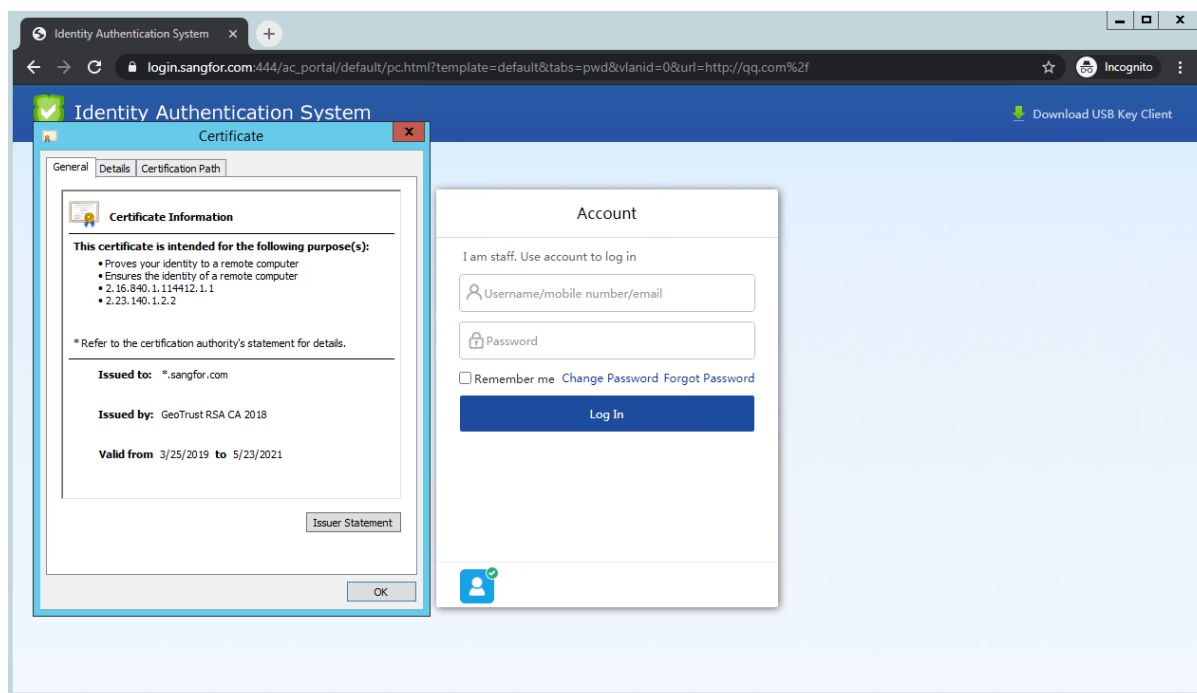
- Setelah import, klik **commit** untuk membuat perangkat mengambil efek.

## Bab 3 Hasil

1. Buat authentication policy untuk perangkat di bawah Lan IAM dan pilih authentication method sebagai berbasis password.

The screenshot shows the 'Authentication Policy' configuration window. The 'Enable' checkbox is checked. The 'Name' field contains '192.168.20.89'. The 'Description' field is empty. On the left sidebar, 'Auth Method' is selected. In the main area, 'Auth Method' is set to 'Password based' (selected with a radio button). Other options include 'Open authentication', 'Single Sign-On(SSO)', and 'None (requests are rejected always)'. The 'Auth Server' is set to 'Local user database'. There are checkboxes for 'Self registration', 'Account login with WeChat', and 'Account Login with SMS Code'. Under 'Captive Portal', the 'Captive Portal' is set to 'Without Slideshow and Terms of Use' with a 'Preview' button. The 'Login Redirection' is set to 'Previously visited webpage'. At the bottom, there are 'Back' and 'Next' buttons.

2. Setelah perangkat akan mengarahkan permintaan http atau https ke halaman login https, Anda juga dapat secara manual memasukkan domain name seperti login.sangfor.com untuk akses langsung ke halaman login https.



## Bab 4 Tindakan Pencegahan

1. Untuk memastikan perangkat endpoint dapat mengakses domain name, DNS server diperlukan untuk *meresolve* domain name dengan **IP address perangkat IAM atau virtual IP (Bridge mode)**, ini diperlukan untuk konfigurasi internal DNS server atau file host perangkat endpoint.

Dalam skenario ini, kami konfigurasi file host perangkat endpoint untuk membuat perangkat mengarahkan ulang ke IP address perangkat.

Di bawah ini adalah konfigurasi file host untuk perangkat endpoint Microsoft Windows PC, setiap jenis endpoint OS memiliki metode konfigurasi sendiri, **disarankan untuk menyelesaikan domain name melalui 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. Untuk menyelesaikan perangkat dan mengarahkan ulang ke IP address yang sebenarnya, Anda perlu memeriksa konfigurasi untuk melakukan pengalihan berdasarkan routing.

The screenshot displays the configuration interface for Sangfor IAM 12.0.42. On the left is a navigation pane with categories like Status, Proxy, Objects, Users, Access Mgt, Bandwidth Mgt, Endpoint Device, Security, System, and Diagnostics. The 'System' category is expanded, showing sub-items like Network, Firewall, General, and Advanced. The 'Advanced' sub-item is selected. The main panel shows the 'Redirection/Proxy' configuration page. Under the 'Redirection' section, the checkbox 'Enable destination based routing, and specify port to forward redirected data' is checked and highlighted with a red box. Below it, the 'Proxy' section has an unchecked checkbox 'Enable destination based routing, and specify port to forward proxy data'. The 'Virtual IP' section shows 'IPv4 Address' set to '1.1.1.3' and 'IPv6 Address' set to '1::3'. A 'Commit' button is at the bottom right.

3. Untuk versi IAM 12.0.42 telah meningkatkan halaman login https untuk mendukung versi TLS 1.2, disarankan untuk menggunakan versi ini ke atas untuk menghindari peringatan TLS dari web browser versi terbaru.
4. Nomor port yang digunakan untuk halaman login https adalah port 444.
5. Untuk pengalihan dari halaman https diperlukan untuk menginstal sertifikat root IAM SSL untuk menghindari kesalahan sertifikat.



The screenshot displays the 'Authentication Options' configuration page in the Sangfor IAM 12.0.42 web interface. The left sidebar shows the navigation menu with 'Users' expanded. The main content area is divided into 'Category' and 'Authentication Options' sections. The 'Authentication Options' section contains several configuration groups: 'Central Management', 'Auto Authentication Options', 'Security Options', 'User Profile Change', 'Password Retrieval', and 'Other Options'. The 'Other Options' group includes the option 'Redirect HTTPS requests(not using proxy) to captive portal if user is not authenticated', which is checked and highlighted with a red rectangular box. Other options in this group include 'DNS service is available even user is not authenticated or is locked', '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/onautservice.com) as specified IP address'. The 'Commit' button is located at the bottom right of the configuration area.



**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