SANGFOR

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.

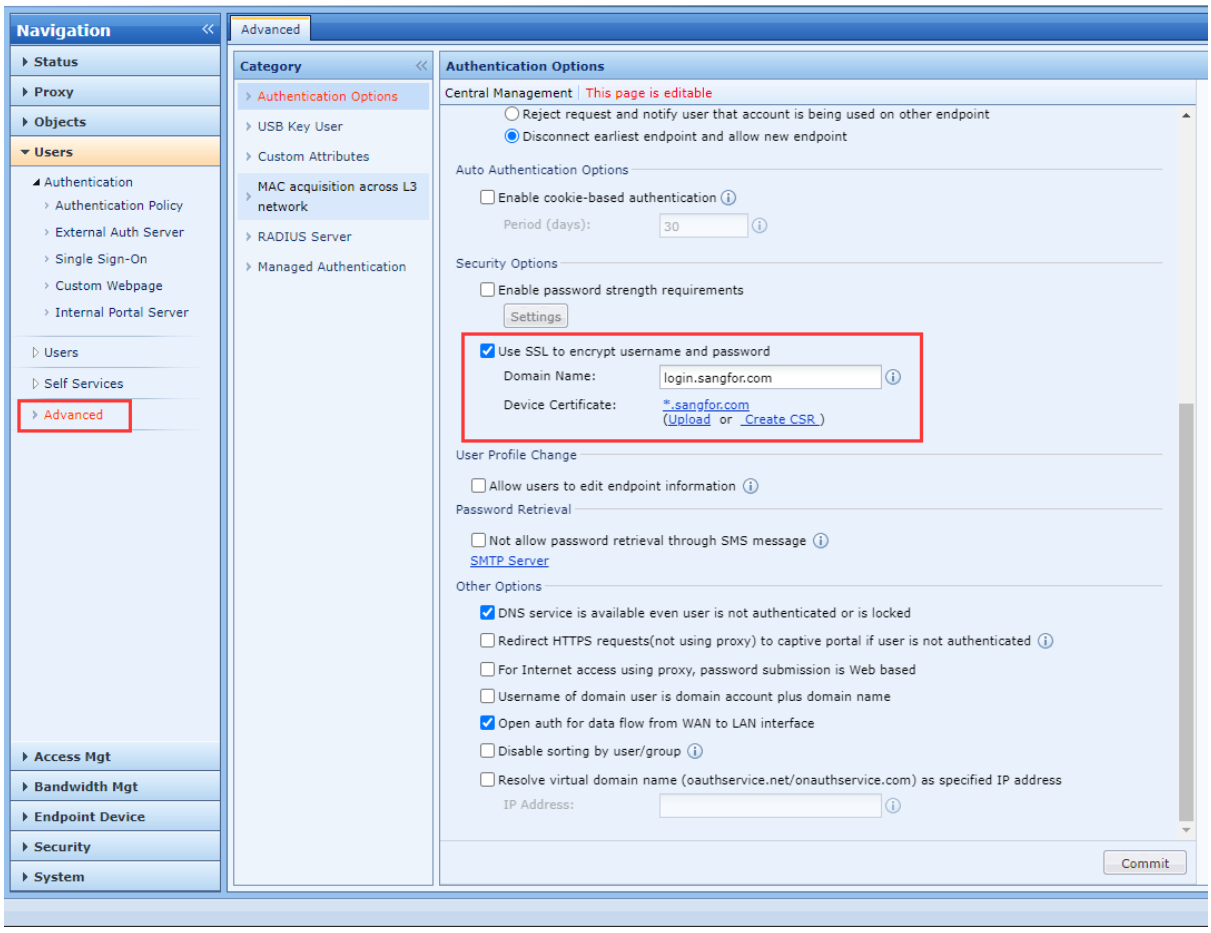
Daftar Isi

Bab 1 Persyaratan

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.

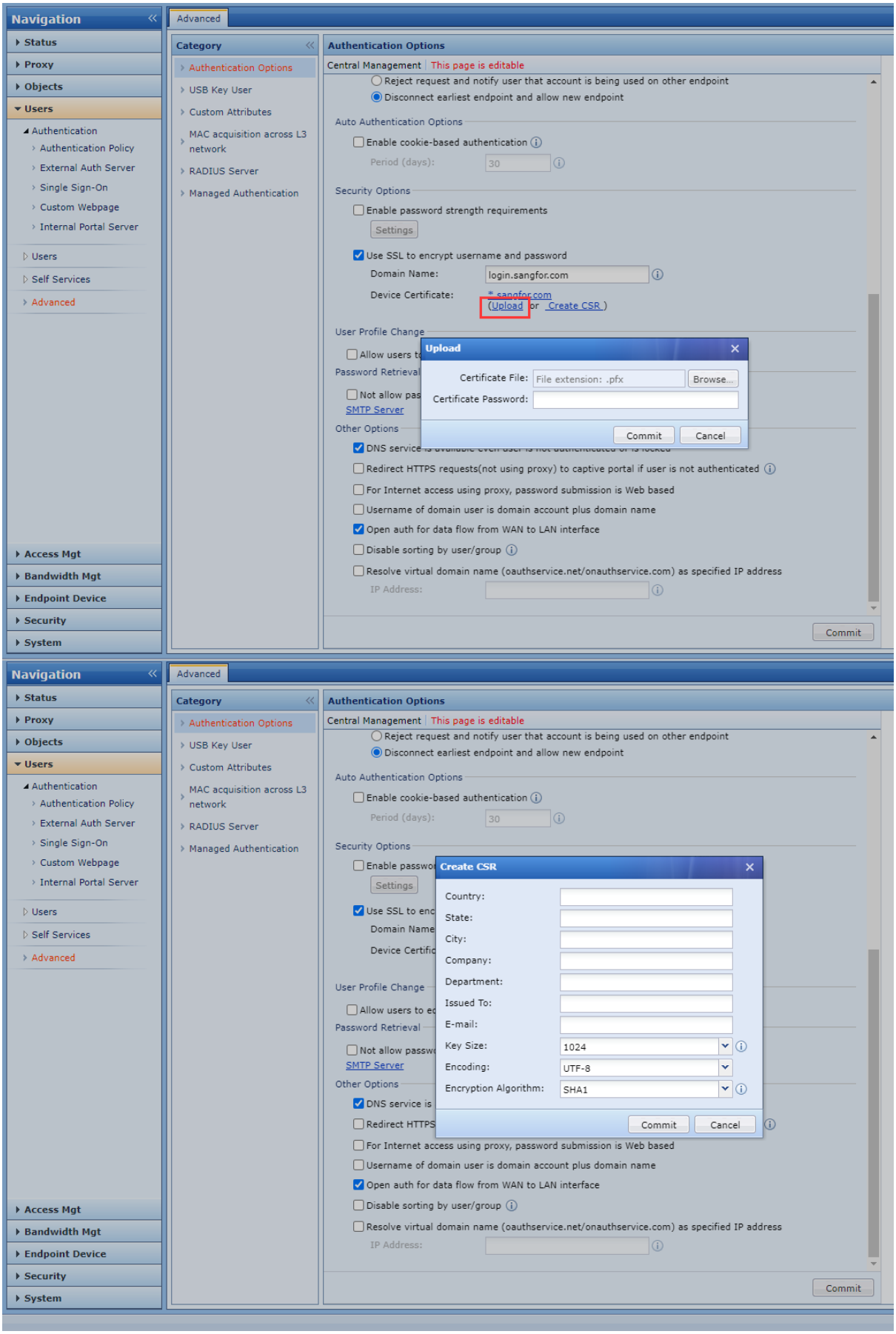
Bab 2 Panduan Konfigurasi

1. Navigate ke Users -> Advanced -> Authentication Options dan aktifkan “Use SSL to encrypt username dan password”



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.

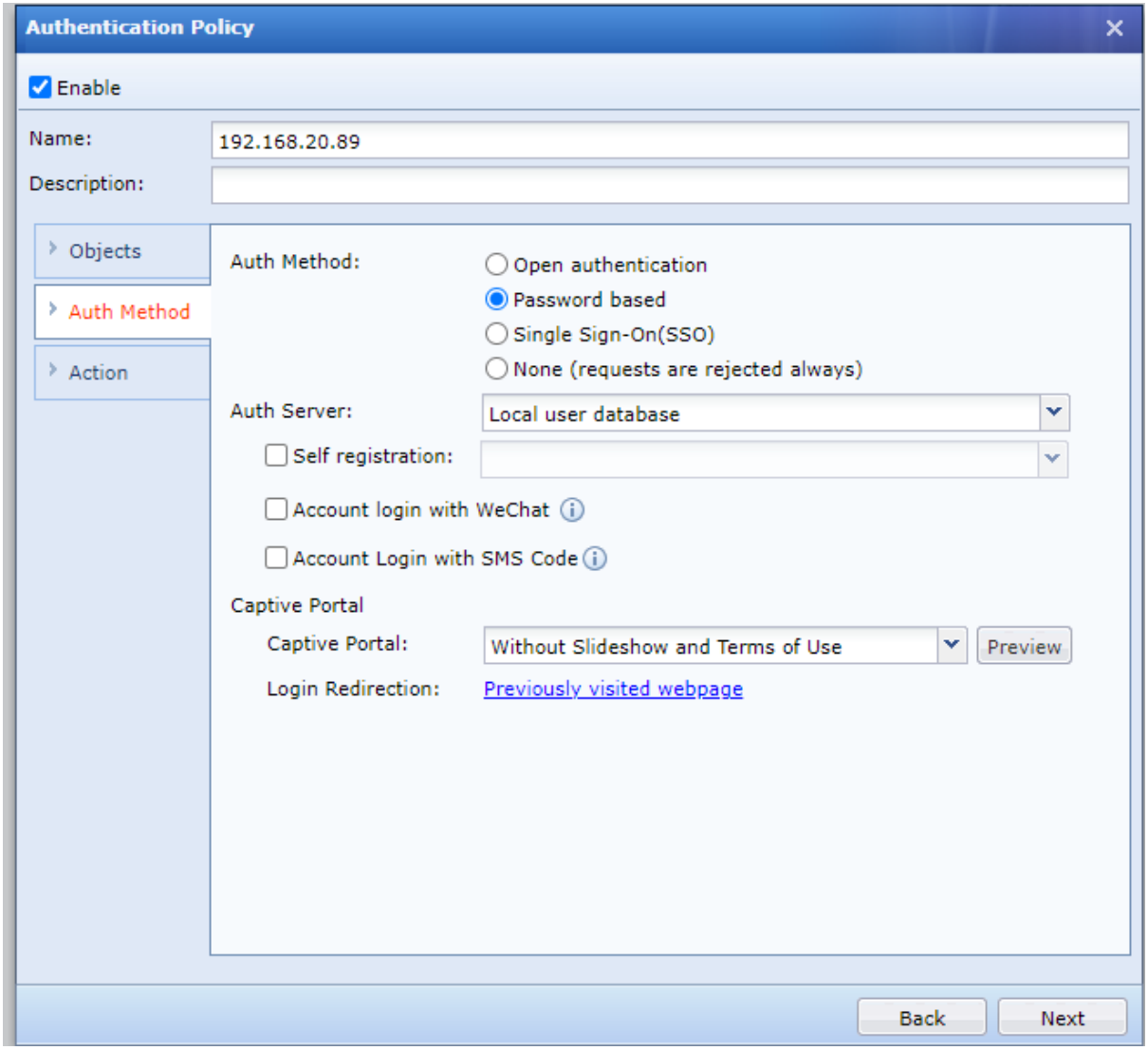
   Dalam skenario ini, kami akan menggunakan sertifikat perangkat untuk *.sangfor.com untuk membuat perangkat dipercaya oleh sertifikat root lainnya.



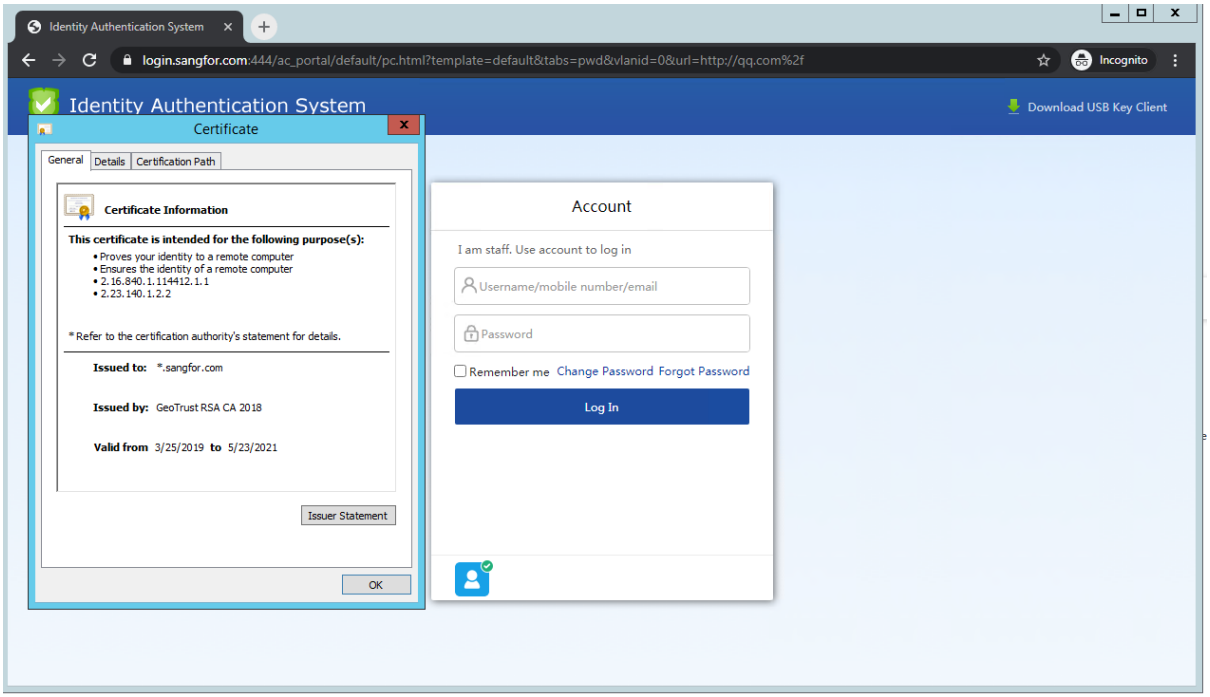
4. Setelah import, klik **commit** untuk membuat perangkat mengambil efek.

Bab 3 Hasil

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



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

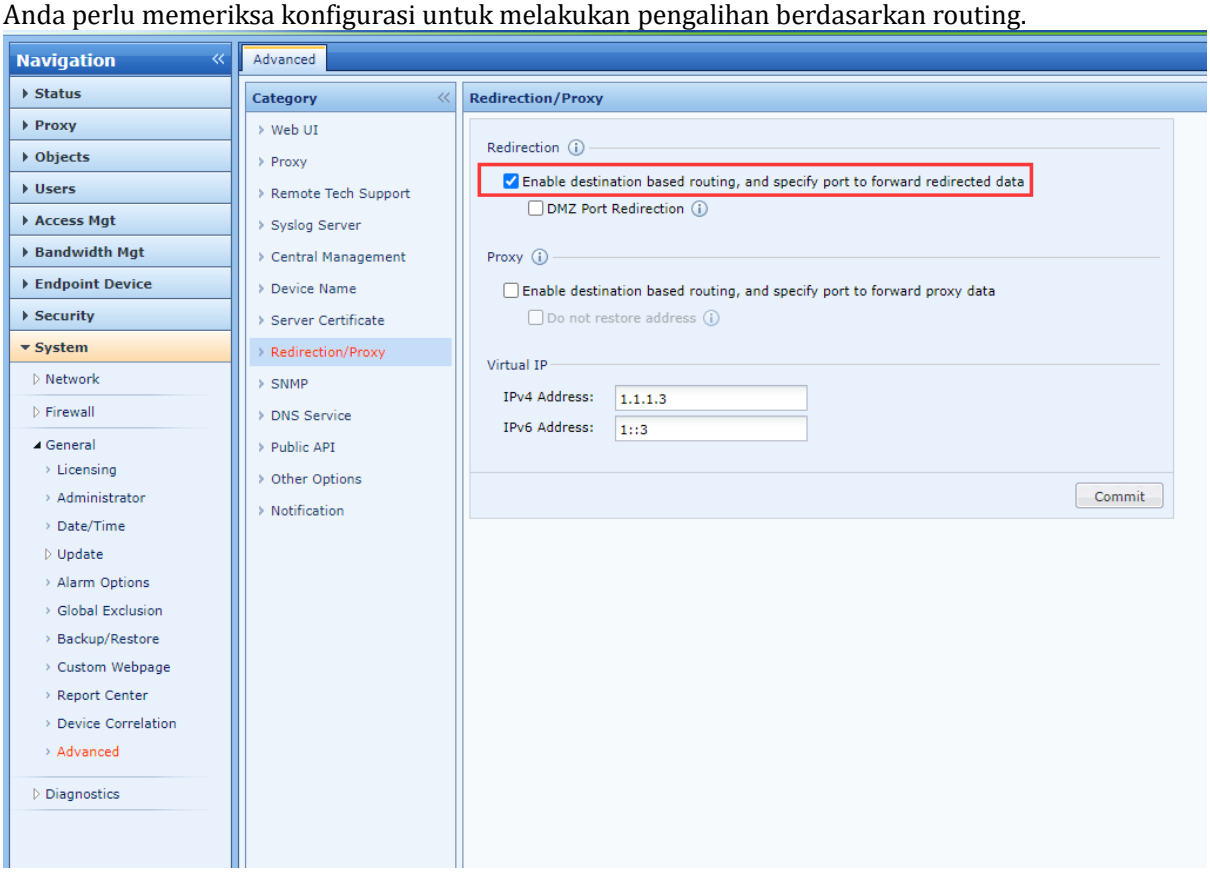
1. Untuk memastikan perangkat endpoint dapat mengakses domain name, DNS server diperlukan untuk *meresolve* domain name dengan **IP address perangkat IAM atau virtual IP (Bridge mode)**, ini diperlukan untuk konfigurasi internal DNS server atau file host perangkat endpoint.

   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.**

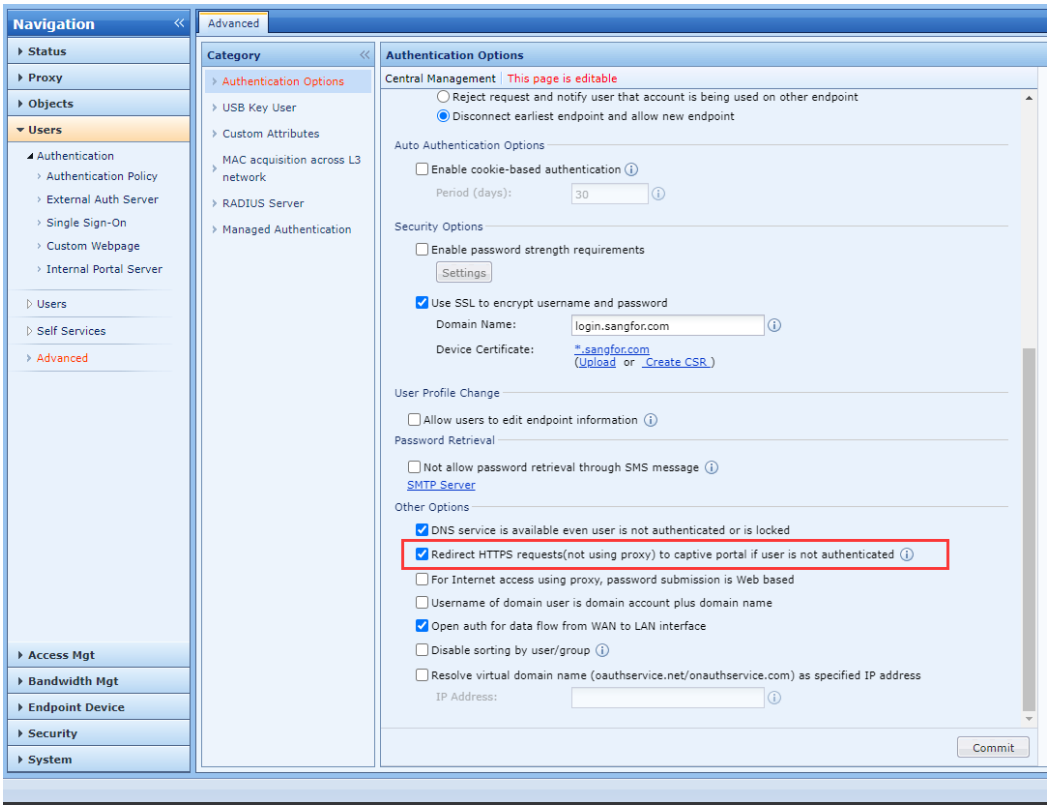
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the 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.



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 diperluan untuk menginstal sertifikat root IAM SSL untuk menghindari kesalahan sertifikat.


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
Advanced
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): 30
Security Options
Enable password strength requirements
Settings
Use SSL to encrypt username and password
Domain Name: login.sangfor.com
Device Certificate: *.sangfor.com (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