Configure AnyConnect with LDAP Authentication on CSM

Contents

Introduction

This document describes how to configure AnyConnect with LDAP Authentication on CSM.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CSM 4.23
- AnyConnect configuration
- SSL protocol

Components Used

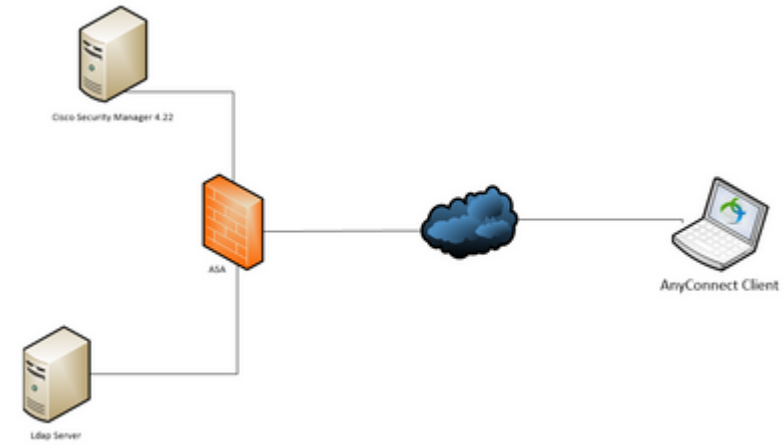
The information in this document is based on these software and hardware versions:

- CSM 4.23
- ASA 5515
- AnyConnect 4.10.6090

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

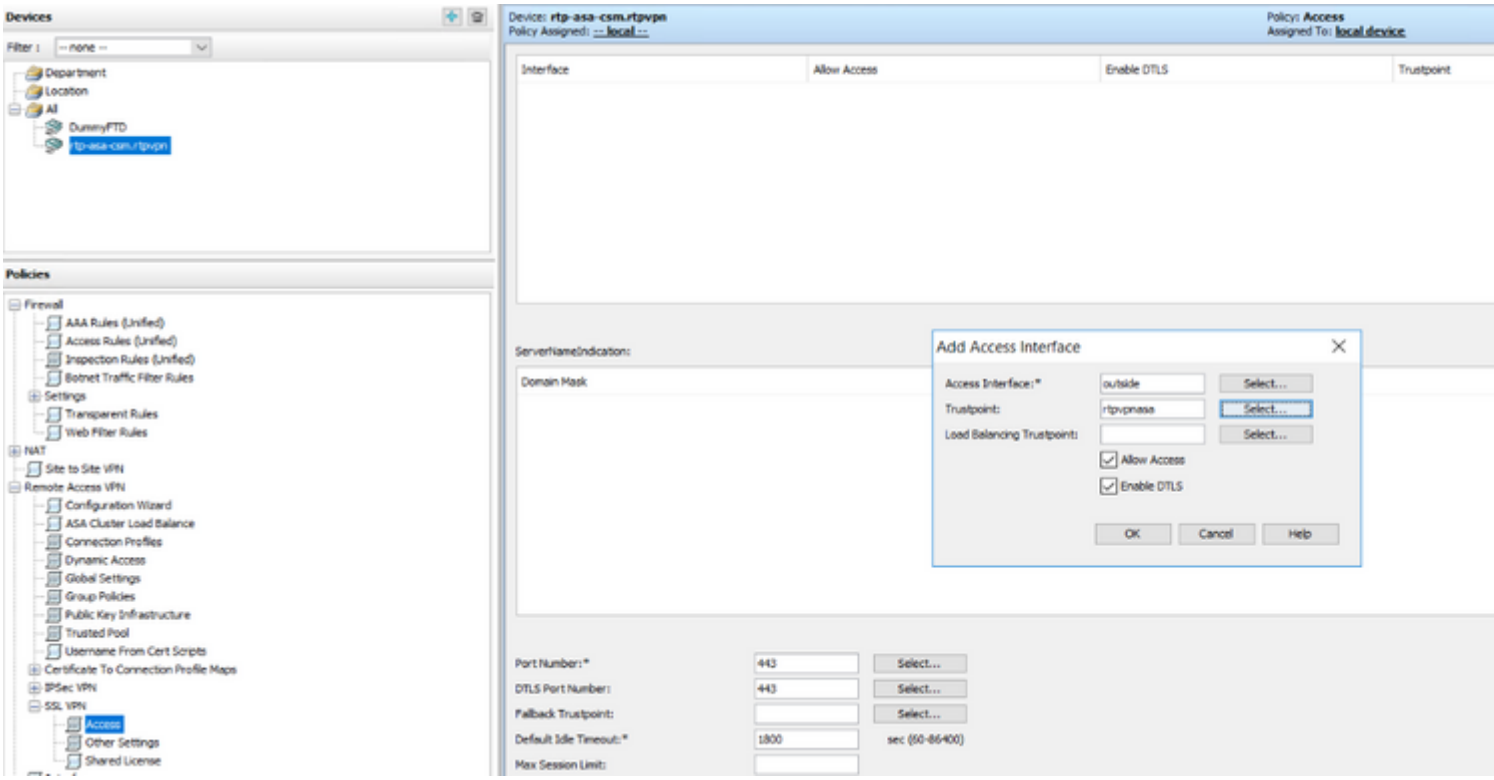
Network Diagram



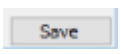
Configurations

Step 1. Configure the SSLVPN Access

Go to Policies > SSL VPN > Access:



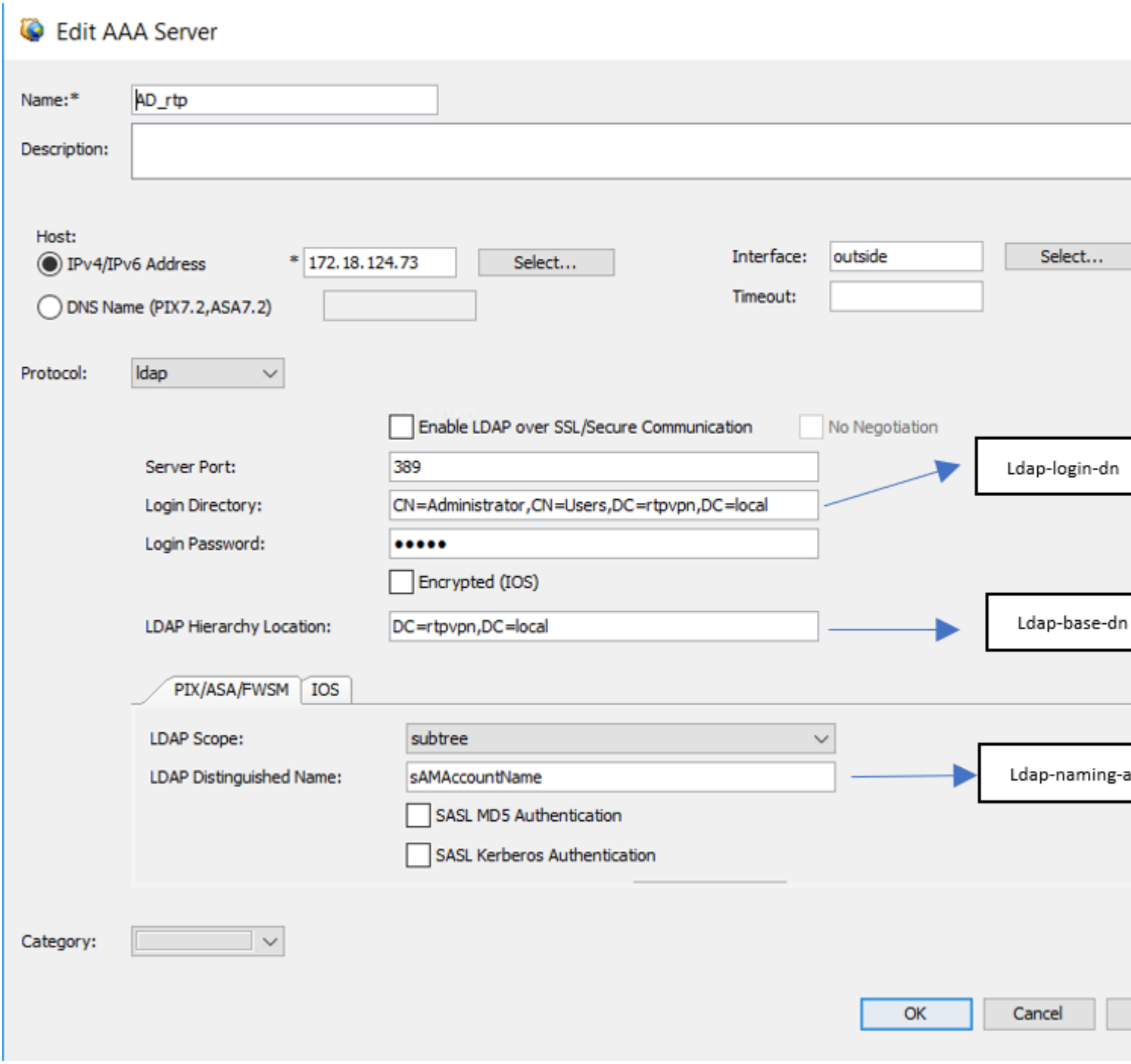
After configuring the Access Interface make sure you click **Save**:



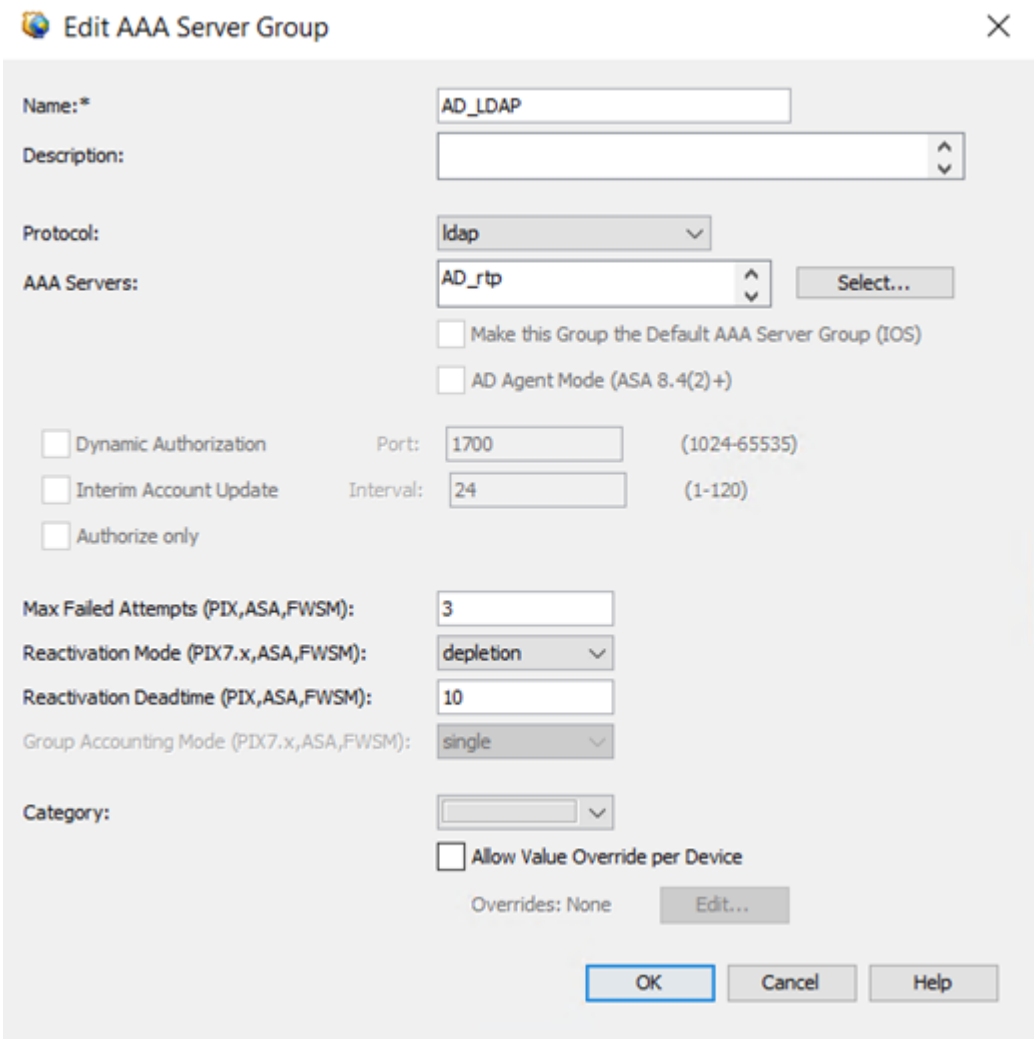
Step 2. Configure the Authentication Server

Go to Policy **Object Manager > All Object Types > AAA Servers > Add**. 

Configure the IP of the server, the source interface, Login Directory, Login Password, LDAP Hierarchy Location, LDAP Scope and LDAP Distinguished Name:



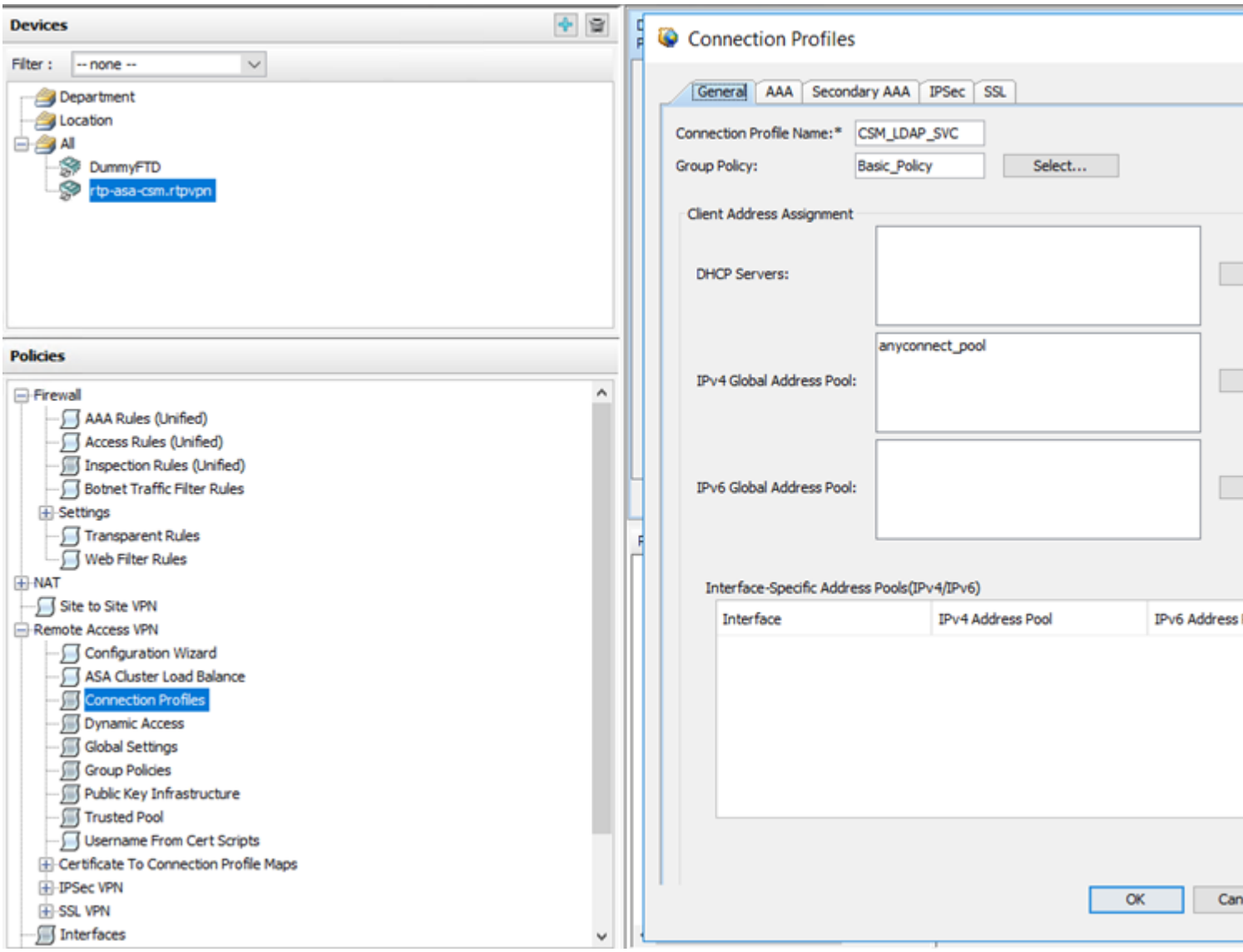
Now add the AAA Server to **AAA Server Groups > Add**.



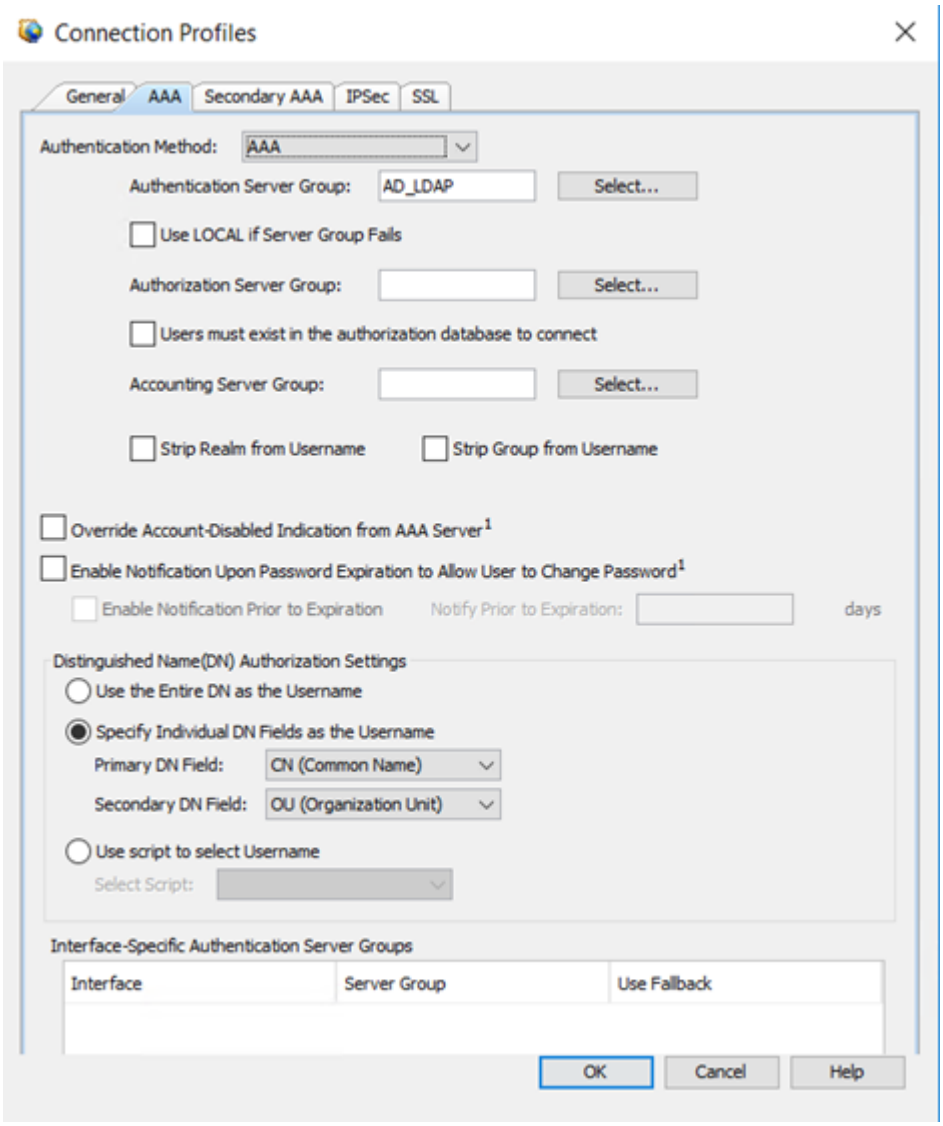
Step 3. Configure the Connection Profile

Go to **Policies > Connection Profiles > Add**. 

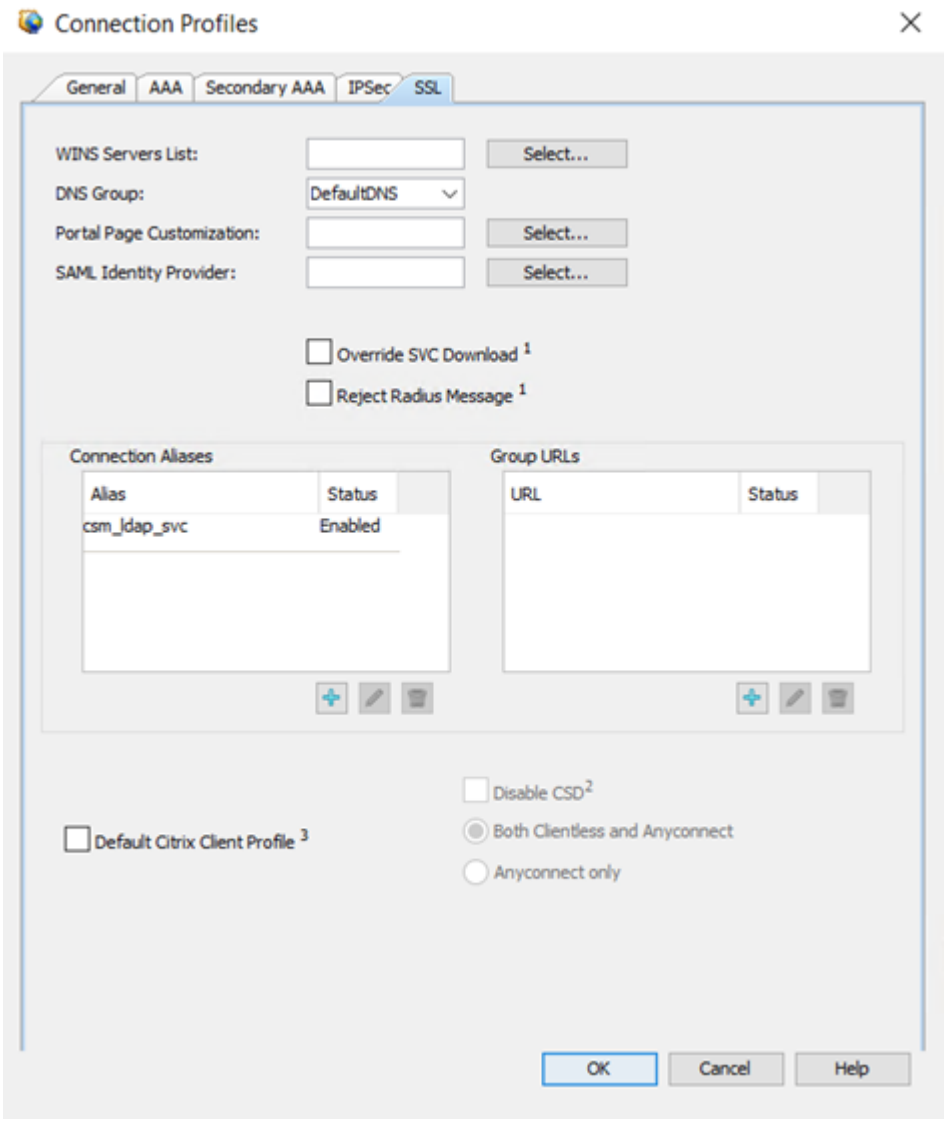
Here you have to configure the **IPv4 Global Address Pool (AnyConnect pool), Group Policy, AAA and Group Alias/URL**:



In order to select the AAA server, click on the **AAA** tab and select the server created on Step 2:



To configure a group alias/group url, dns or wins server in the connection profile, go to the **SSL** tab:



Step 4. Deploy

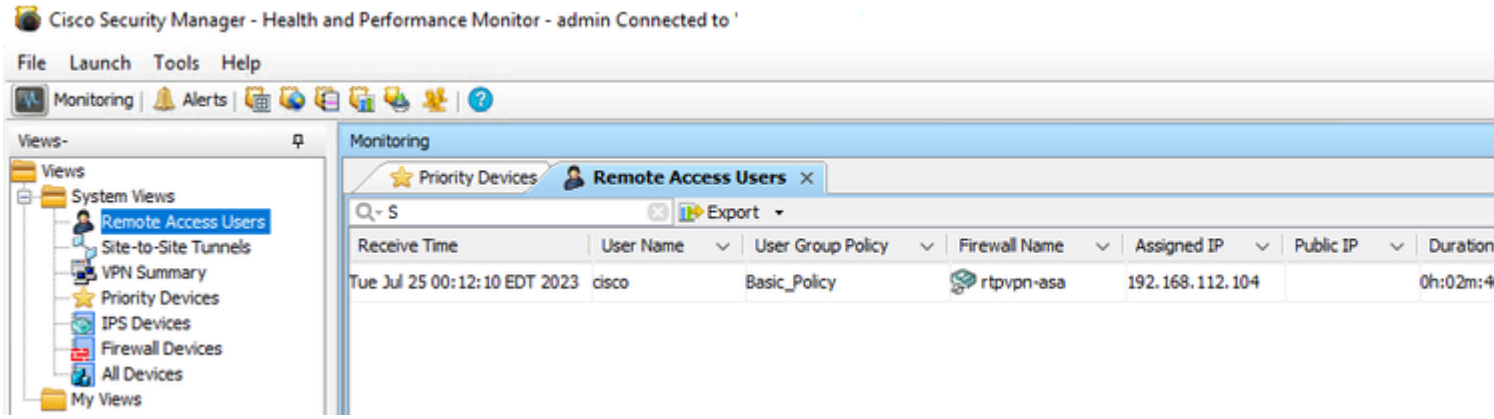
Click the deploy icon . 

Verify

This section provides information you can use in order to verify your configuration.

Accessing through CSM:

Open the **Health and Performance Monitor > Tools > Device Selector > Select the ASA > Next > Select Remote Access Users**



Note: The VPN user shows up based on the HPM refresh timer.

Through CLI:

```
ASA#show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco                        Index : 23719
Assigned IP : 192.168.20.1              Public IP : 209.165.201.25
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 15856                        Bytes Rx : 3545
Group Policy : Basic_Policy             Tunnel Group : CSM_LDAP_SVC
Login Time : 10:29:42 UTC Tue Jul 25 2023
Duration : 0h:010m:16s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A                      VLAN : none
Audt Sess ID : 0e26864905ca700064bf3396
Security Grp : none
```

Troubleshoot

In order to check possible failures during the LDAP authentication or the anyconnect establishment you can execute the next commands on the CLI:

<#root>

debug ldap 255

debug webvpn anyconnect 255