Decommission of Kerberos from ASA 9.22

Contents

Introduction

This document describes insight on Kerberos Deprecation from ASA 9.22.

Prerequisites

Requirements

Cisco recommends that you have knowledge of basic security concepts:

- Basic Knowledge of ASA CLI.
- Basic knowledge of AAA (Authentication, Authorization, and Accounting)

Components Used

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

- All ASA platforms
- ASA CLI 9.22.1
- ASDM 7.22.1
- CSM 4.29

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.

ASA CLI Configuration Walkthrough

ASA CLI Overview:

- In the command output, the options in***bold italic***have been removed from the CLI.
- Upgrades from versions prior to 9.22 that contain these configurations result in a warning message on the console during boot time.

ciscoasa(config)# aaa-server kerb protocol ?

configure mode commands/options:

http-form Protocol HTTP form-based

kerberos Protocol Kerberos (DEPRECATED)

ldap Protocol LDAP

radius Protocol RADIUS

sdi Protocol SDI

tacacs+ Protocol TACACS+

ciscoasa(config)# aaa-server kerb protocol kerberos

ciscoasa(config-aaa-server-group)# ?

AAA server configuration commands:

exit Exit from aaa-server group configuration mode

help Help for AAA server configuration commands

max-failed-attempts Specify the maximum number of failures that allowed for any server in the group before that server is deactivated

no Remove an item from aaa-server group configuration

reactivation-mode Specify the method by which failed servers are reactivated

validate-kdc Enable KDC validation during kerberos user auth

ciscoasa(config)# test aaa-server authentication kerb ?

exec mode commands/options:

delegate Test Kerberos constrained delegation

host Enter this keyword to specify the IP address for the server

impersonate Test Kerberos protocol transition

password Password keyword

self Test Kerberos self-ticket retrieval

username Username keyword

ciscoasa(config)# aaa-server ldaps protocol ldap

ciscoasa(config-aaa-server-group)# aaa-server ldaps host x.x.x.x

ciscoasa(config-aaa-server-host)# sasl-mechanism ?

aaa-server-host mode commands/options:

digest-md5 select Digest-MD5

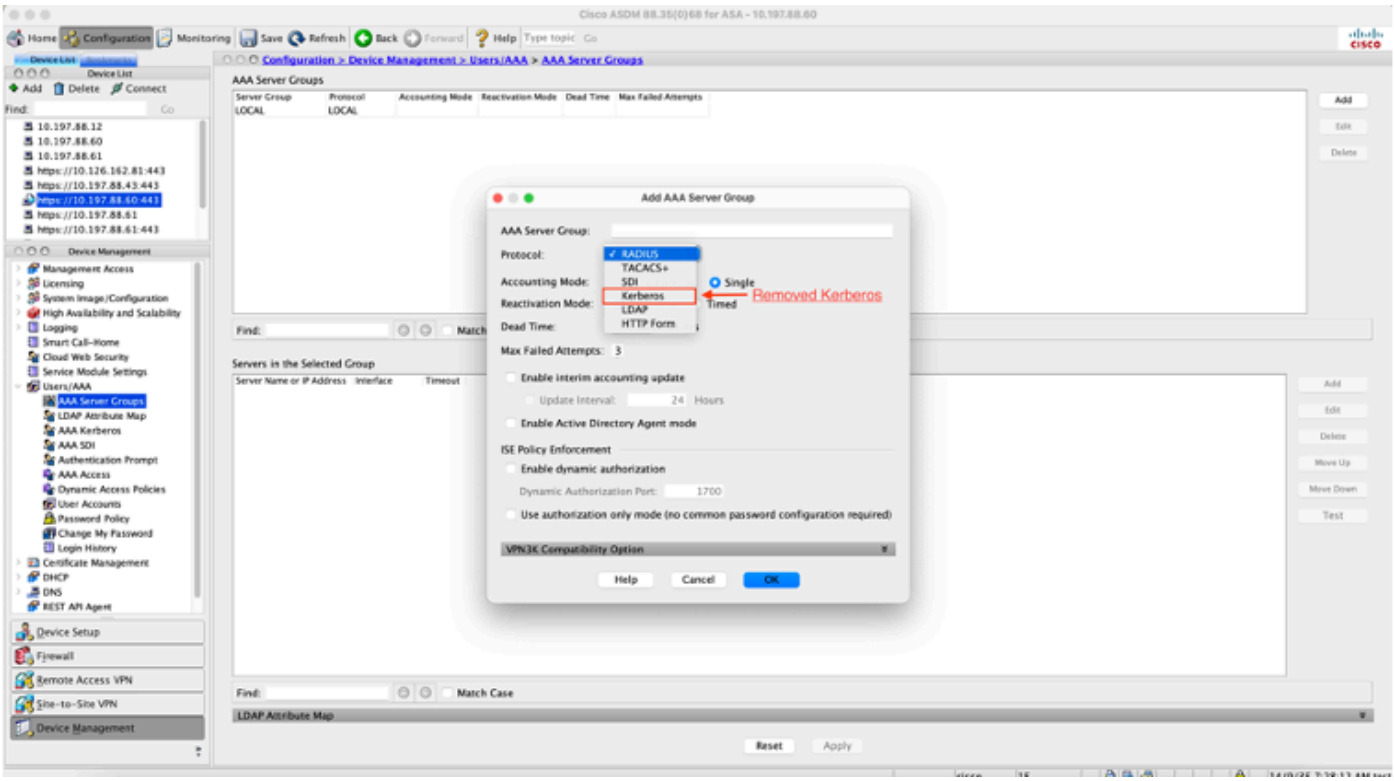
kerberos select Kerberos

ciscoasa(config)# ***debug kerberos***

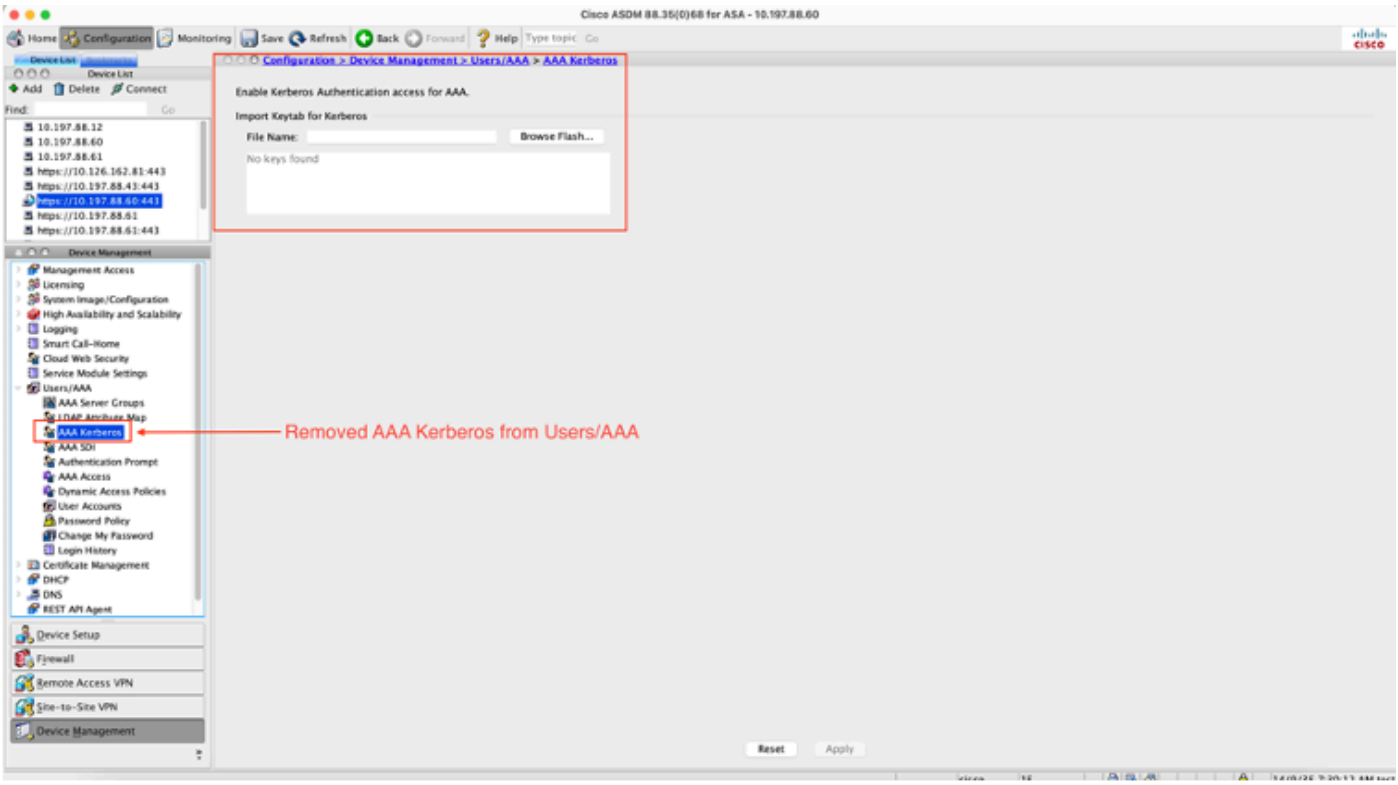
ASDM Configuration Walkthrough

ASDM overview:

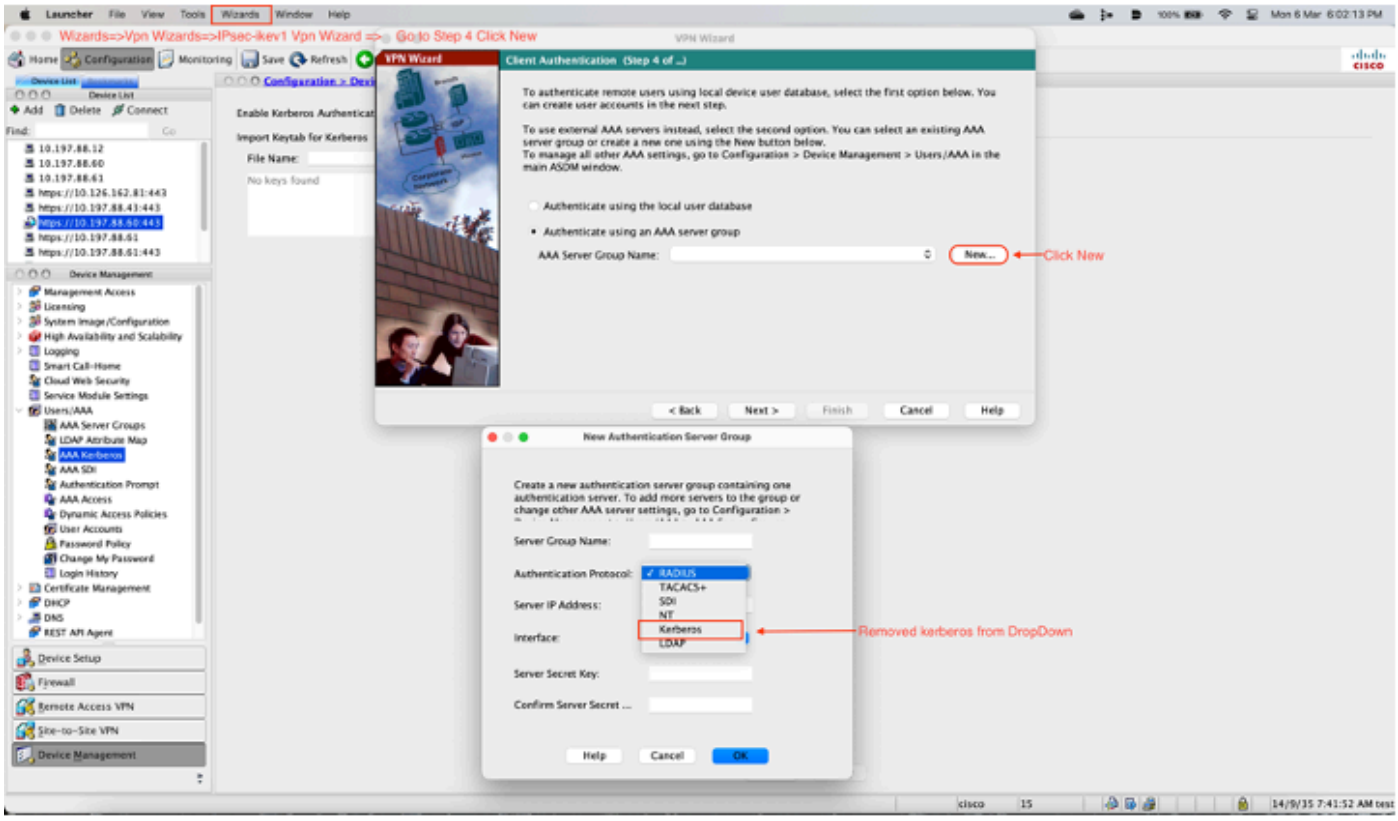
- Kerberos is no longer supported from ASDM 7.22
- This deprecates the ability for end users to configure AAA server groups with the Kerberos Protocol as well as the LDAP SASL mechanism.
- As part of this deprecation, AAA Kerberos is no longer listed in TreeMenu under Users/AAA in Device Management.
- Microsoft KCD Server is also no longer supported.



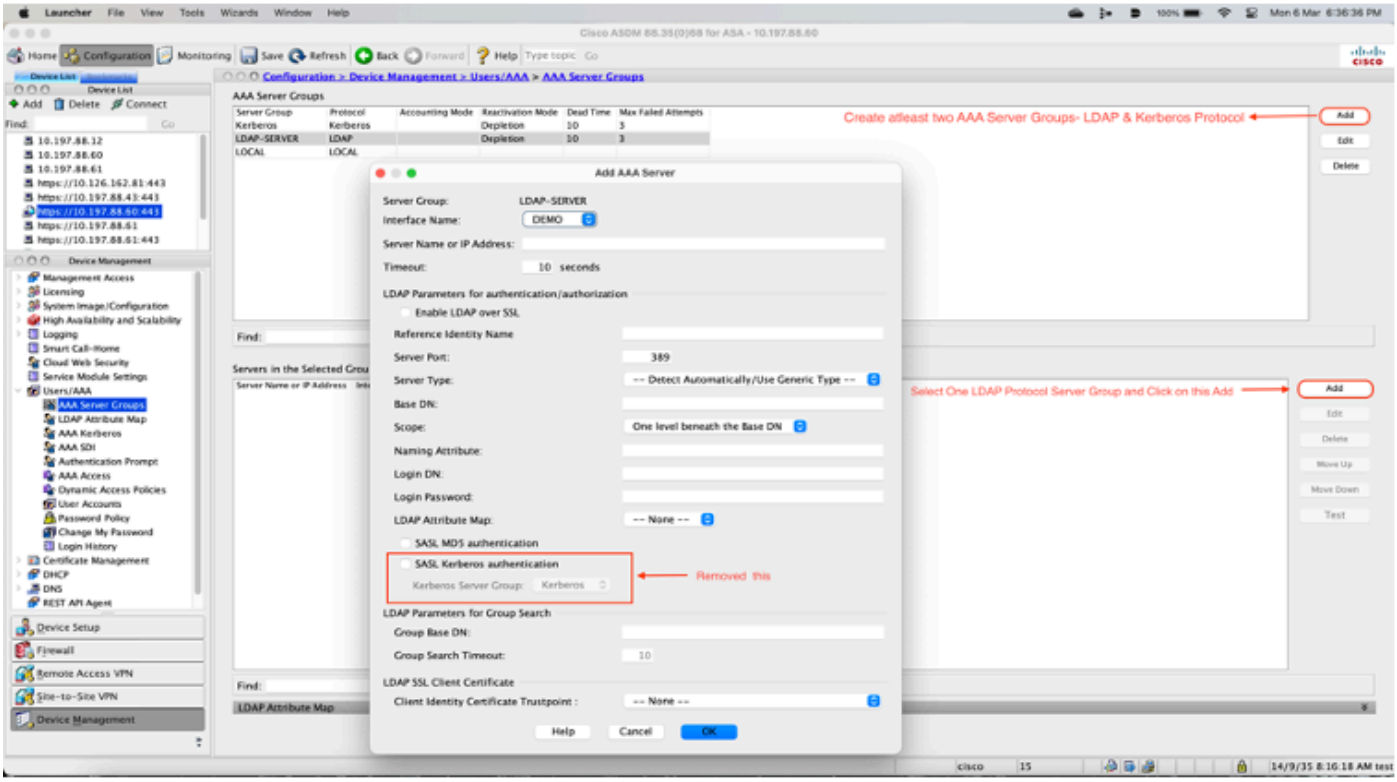
ASDM: Kerberos Protocol in New AAA Server Group



ASDM: AAA Kerberos



ASDM: Kerberos Protocol in New AAA Server Group

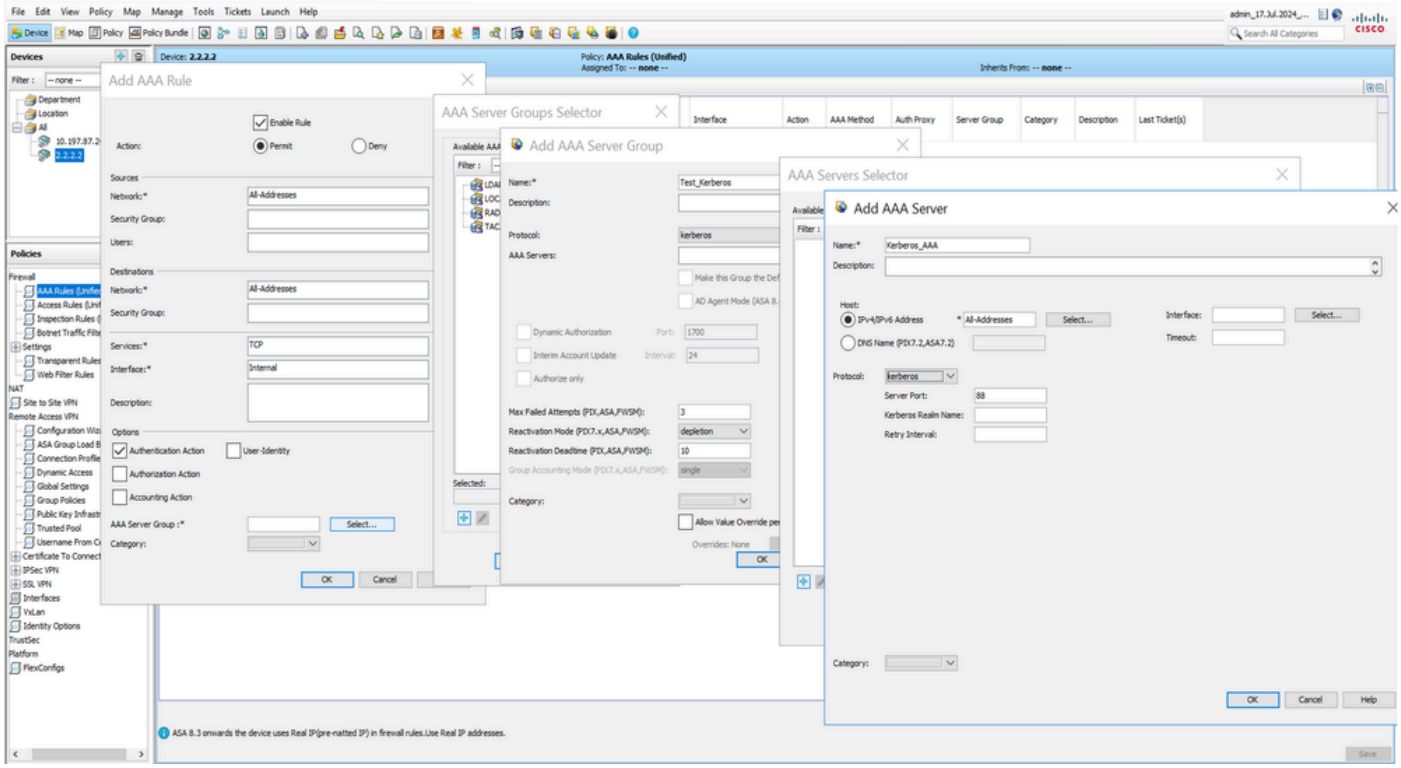


ASDM: Kerberos Configuration for LDAP SASL

CSM Configuration Walkthrough

CSM Overview:

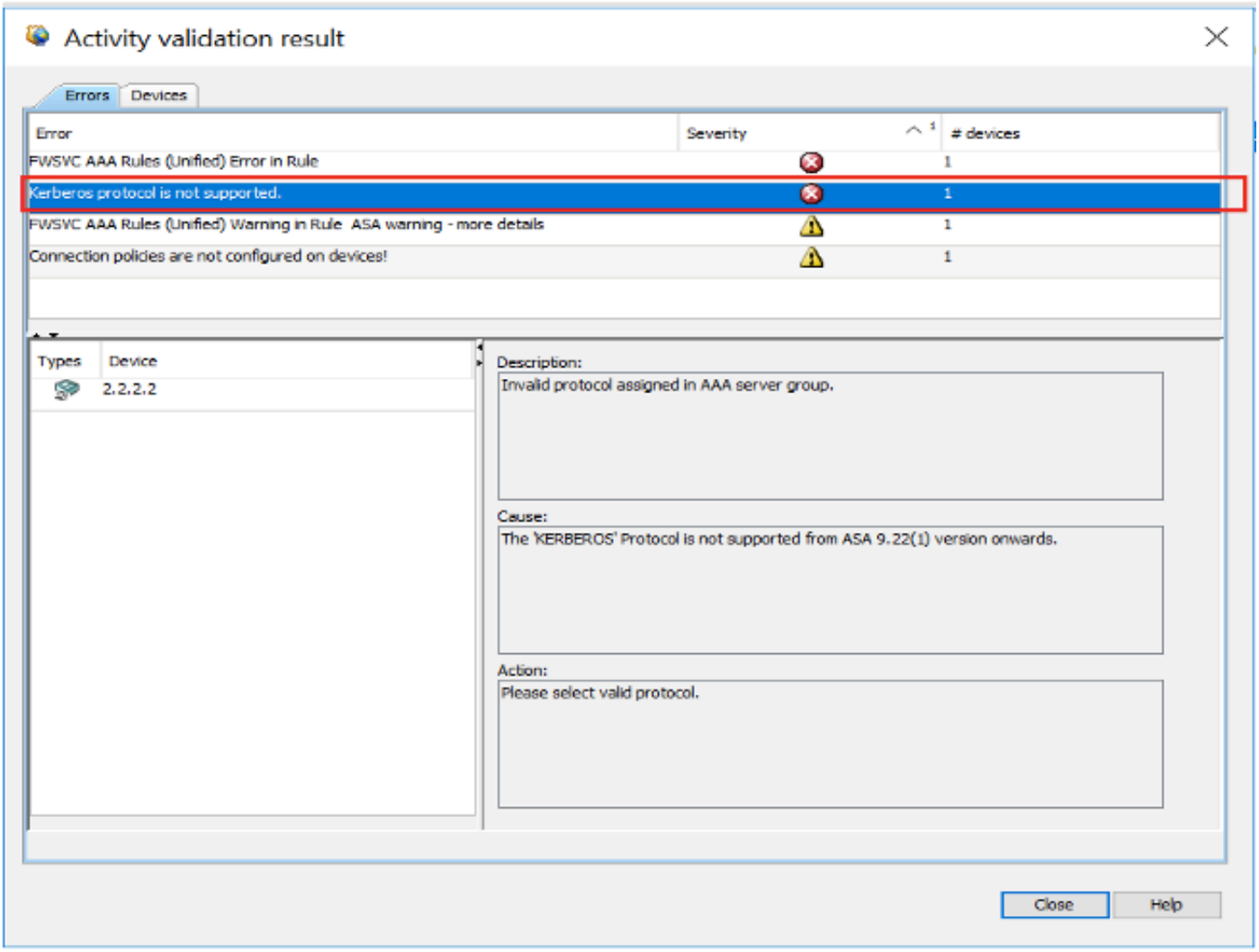
- Kerberos Protocol is no longer supported.
- This deprecates the ability for end users to configure AAA server groups with the Kerberos Protocol as well as the LDAP SASL mechanism.
- Microsoft KCD Server is also no longer supported.
- Instead of removing Kerberos Support from CSM, it is handled in Activity Validation.
- Activity Validation throw an Error message for 9.22.1 ASA version onwards saying, Kerberos protocol is not supported from 9.22.1 version onwards.

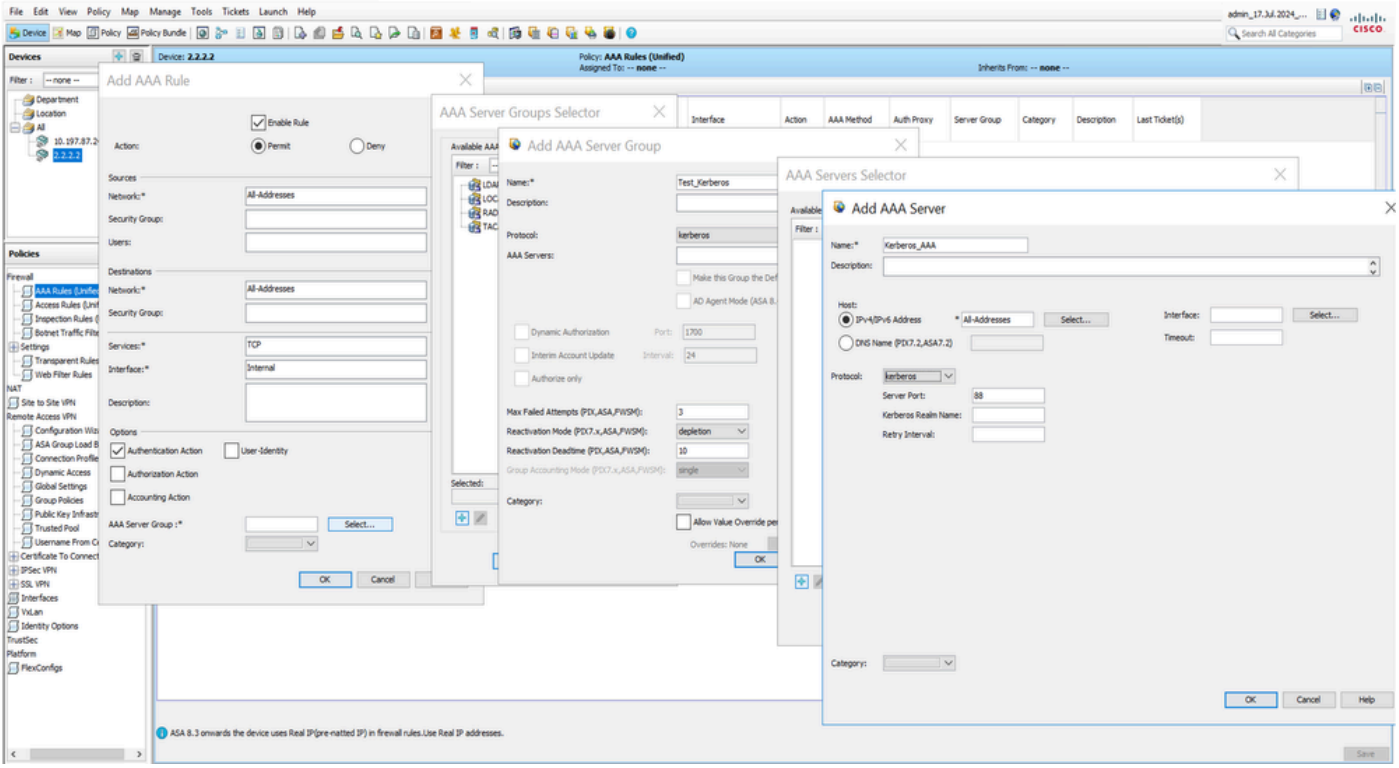


CSM Kerberos Configuration

PATH: **CSM>Firewall > AAA Rules > AAA Server Group > Add > Kerberos**

1. Save
2. Preview Config for Activity Validation result.





CSM Kerberos Configuration for LDAP SASL

PATH: **CSM>Firewall > AAA Rules > AAA Server Group > Add >Protocol > LDAP >SASL**

1. Save
2. Preview Config for Activity Validation result.