Außerbetriebnahme von Kerberos von ASA 9.22

Inhalt

Einleitung

In diesem Dokument werden Erkenntnisse zur Kerberos-Deprecation von ASA 9.22 beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse folgender grundlegender Sicherheitskonzepte verfügen:

- Grundlegende Kenntnisse der ASA CLI
- Grundkenntnisse von AAA (Authentifizierung, Autorisierung und Abrechnung)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Alle ASA-Plattformen
- ASA CLI 9.22.1
- ASDM 7,22,1
- CSM 4,29

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

ASA CLI-Konfiguration - exemplarische Vorgehensweise

ASA CLI im Überblick:

- In der Befehlsausgabe wurden die Optionen inbold italichaus der CLI entfernt.
- Upgrades von älteren Versionen als Version 9.22, die diese Konfigurationen enthalten, führen während des Bootvorgangs zu einer Warnmeldung auf der Konsole.

ciscoasa(config)# aaa-server curb protocol ?

Befehle/Optionen für den Konfigurationsmodus:

HTTP-Form Protokoll, formularbasiert

Kerberos-Protokoll Kerberos (VERALTET)

LDAP LDAP-Protokoll

RADIUS-Protokoll

sdi-Protokoll SDI

TACACS+-Protokoll TACACS+

ciscoasa(config)# aaa-server curb-Protokoll kerberos

ciscoasa(config-aaa-server-group)#

AAA-Serverkonfigurationsbefehle:

Beenden Beenden des Konfigurationsmodus aaa-server group

Hilfe zu AAA-Serverkonfigurationsbefehlen

max-failed-attempts Geben Sie die maximale Anzahl von Fehlern an, die für einen beliebigen Server in der Gruppe zulässig sind, bevor dieser Server deaktiviert wird.

no Artikel aus aaa-server-Gruppenkonfiguration entfernen

Reaktivierungsmodus Geben Sie an, wie ausgefallene Server reaktiviert werden sollen.

validate-kdc KDC-Validierung während der Kerberos-Benutzerauthentifizierung aktivieren

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

Befehle/Optionen des exec-Modus:

delegieren Eingeschränkte Delegierung von Test Kerberos

host Geben Sie dieses Schlüsselwort ein, um die IP-Adresse für den Server anzugeben.

imitieren Test Kerberos Protokoll Übergang

Kennwort Kennwort Kennwort-Schlüsselwort

Selbsttest Kerberos Selbstfahrscheinabruf

username Benutzername Schlüsselwort

ciscoasa(config)# aaa-server ldaps Protokoll ldap

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

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

aaa-server-host mode-Befehle/-Optionen:

Digest-MD5 auswählen

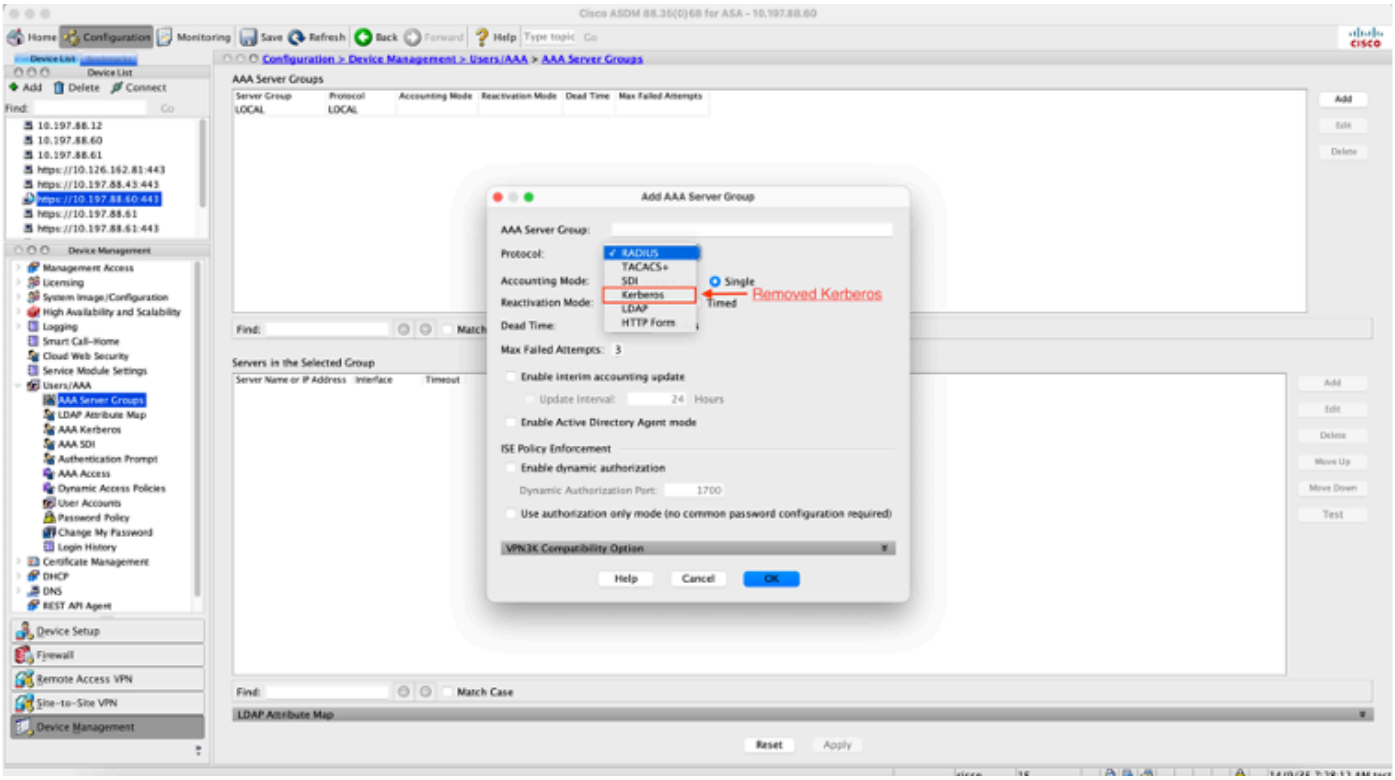
kerberos auswählen Kerberos

ciscoasa(config)# debug kerberos

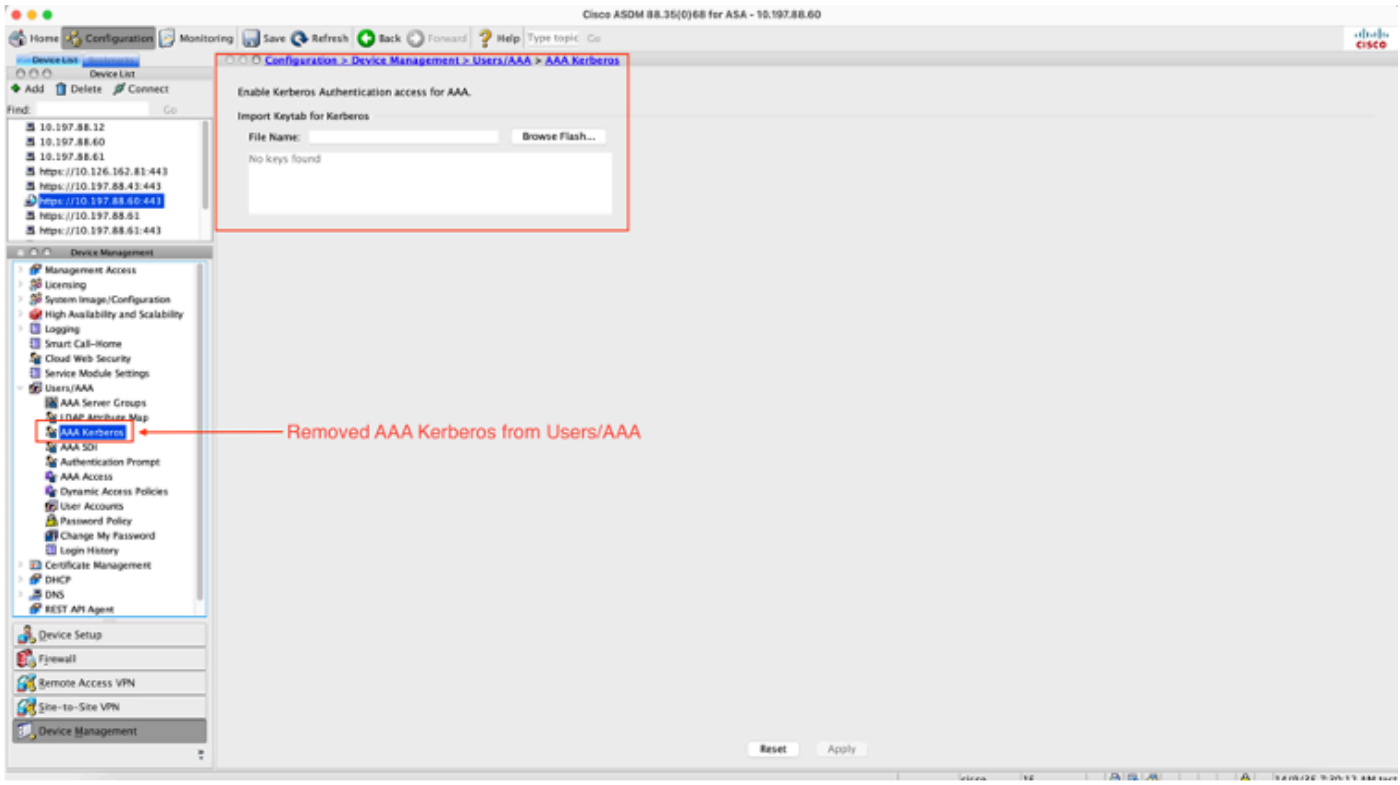
ASDM-Konfiguration - exemplarische Vorgehensweise

ASDM - Übersicht:

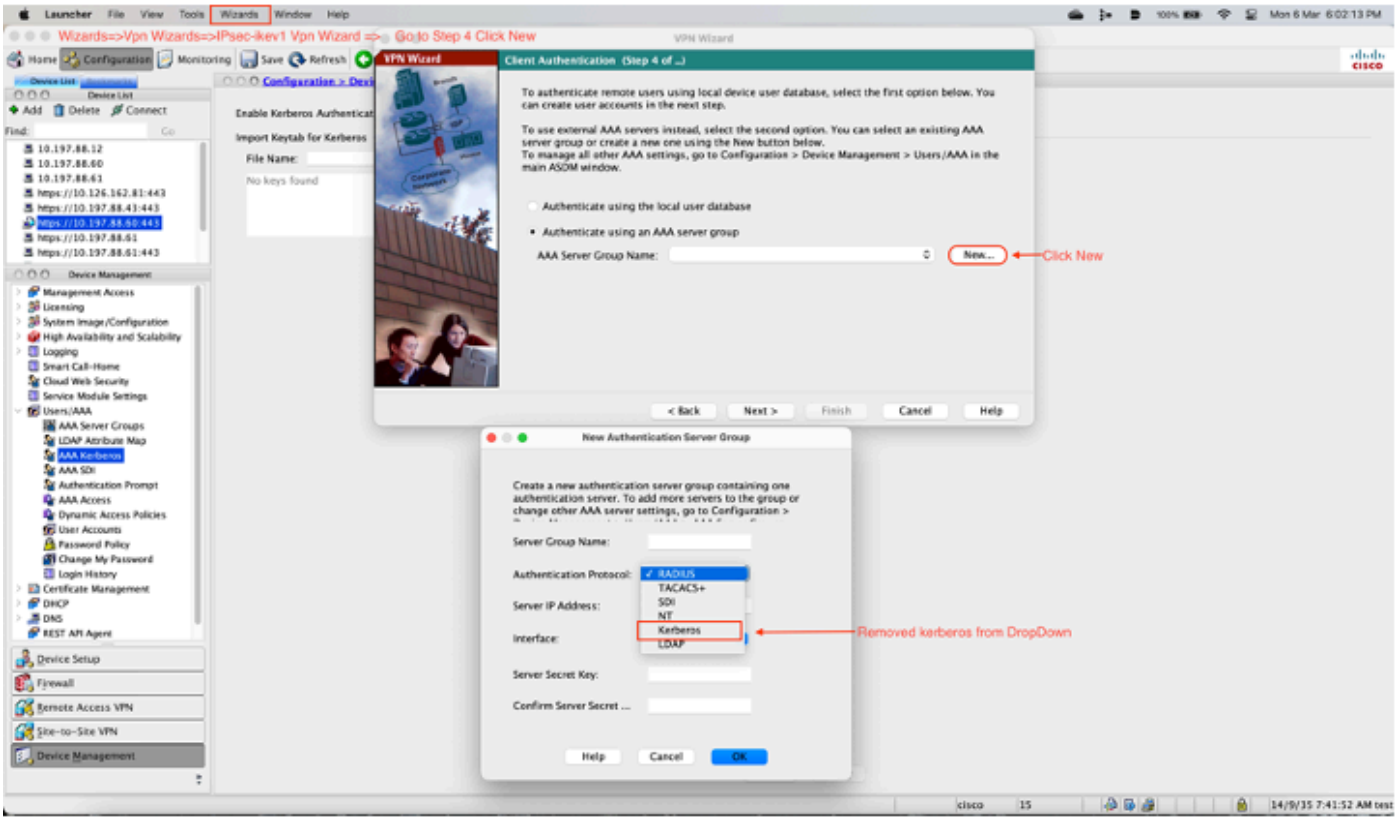
- Kerberos wird von ASDM 7.22 nicht mehr unterstützt.
- Dadurch wird die Möglichkeit für Endbenutzer vernachlässigt, AAA-Servergruppen mit dem Kerberos-Protokoll und dem LDAP-SASL-Mechanismus zu konfigurieren.
- Als Teil dieser Wertminderung wird AAA Kerberos in der Geräteverwaltung nicht mehr im TreeMenu unter Benutzer/AAA aufgeführt.
- Microsoft KCD Server wird ebenfalls nicht mehr unterstützt.



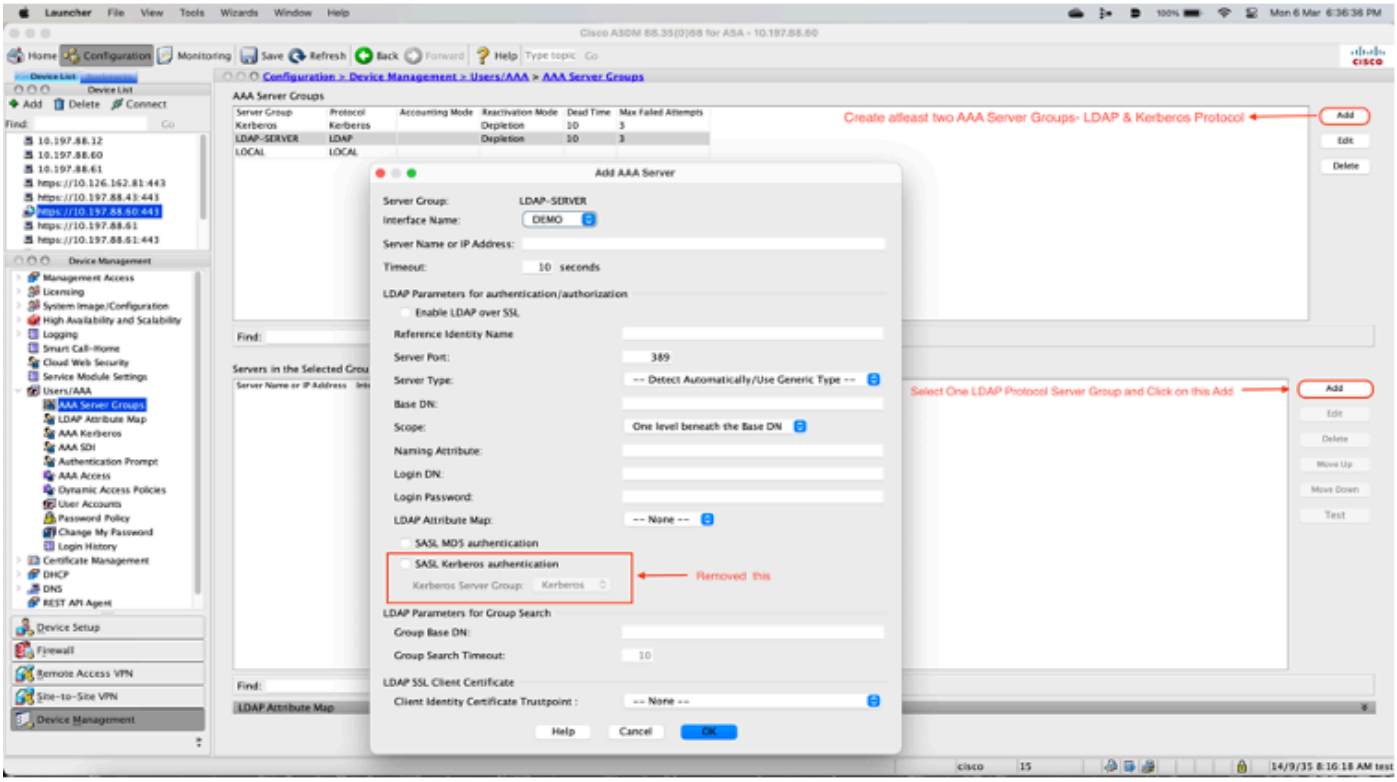
ASDM: Kerberos-Protokoll in neuer AAA-Servergruppe



ASDM: AAA Kerberos



ASDM: Kerberos-Protokoll in neuer AAA-Servergruppe

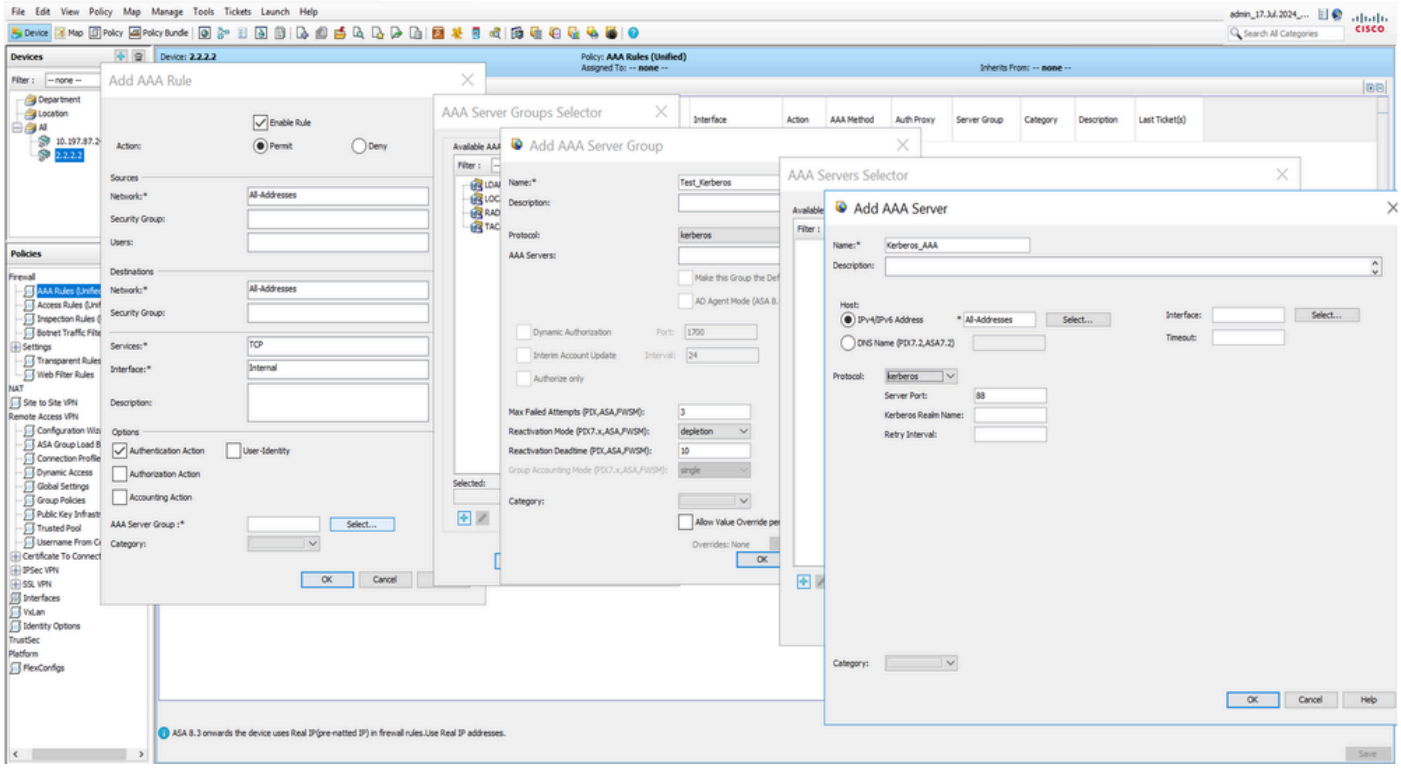


ASDM: Kerberos-Konfiguration für LDAP-SASL

CSM-Konfiguration - exemplarische Vorgehensweise

CSM im Überblick:

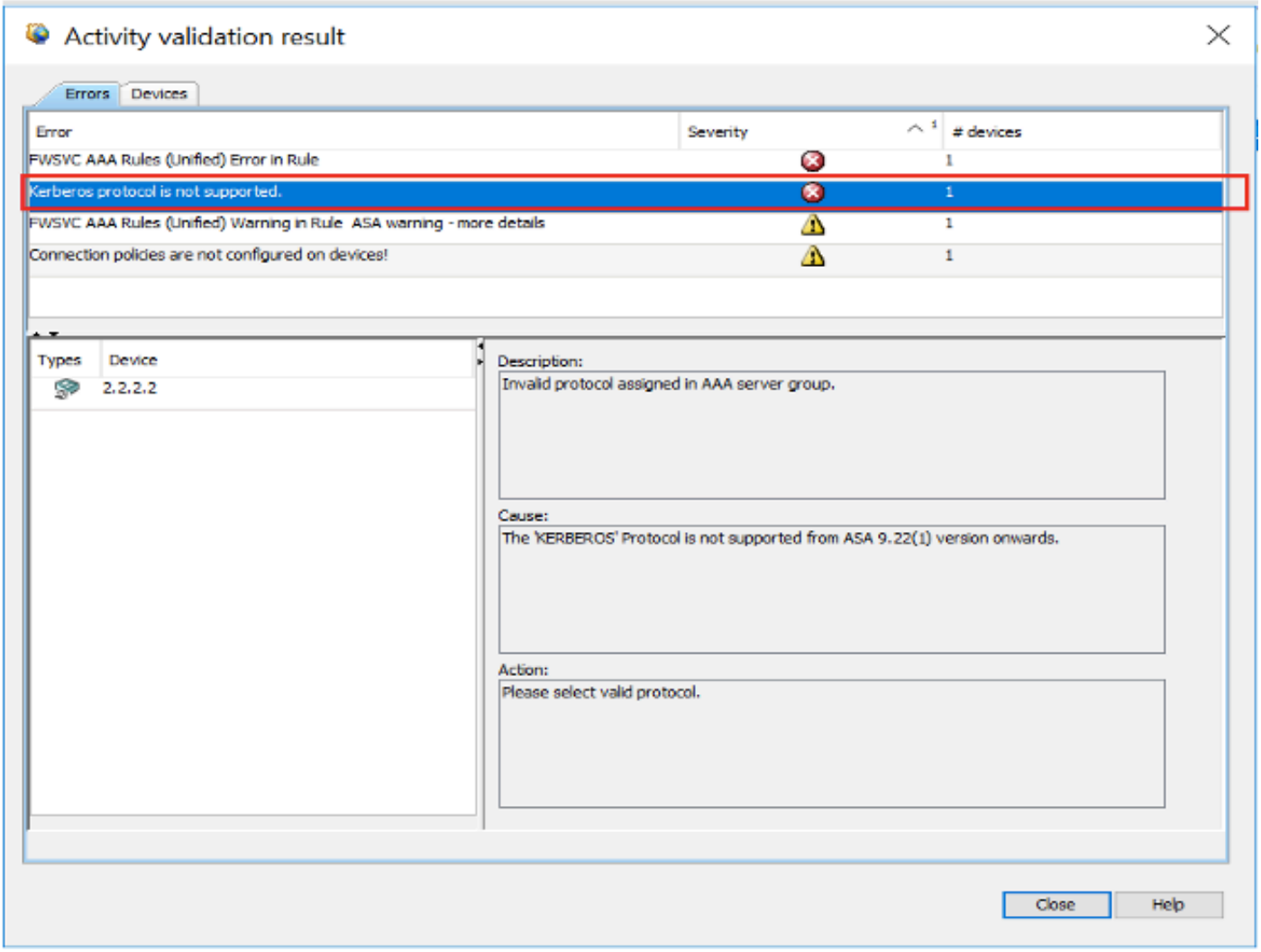
- Das Kerberos-Protokoll wird nicht mehr unterstützt.
- Dadurch wird die Möglichkeit für Endbenutzer vernachlässigt, AAA-Servergruppen mit dem Kerberos-Protokoll und dem LDAP-SASL-Mechanismus zu konfigurieren.
- Microsoft KCD Server wird ebenfalls nicht mehr unterstützt.
- Anstatt die Kerberos-Unterstützung aus CSM zu entfernen, wird sie in der Aktivitätsvalidierung behandelt.
- Die Aktivitätsvalidierung löst eine Fehlermeldung für die ASA-Version 9.22.1 aus, die besagt, dass das Kerberos-Protokoll ab Version 9.22.1 nicht mehr unterstützt wird.

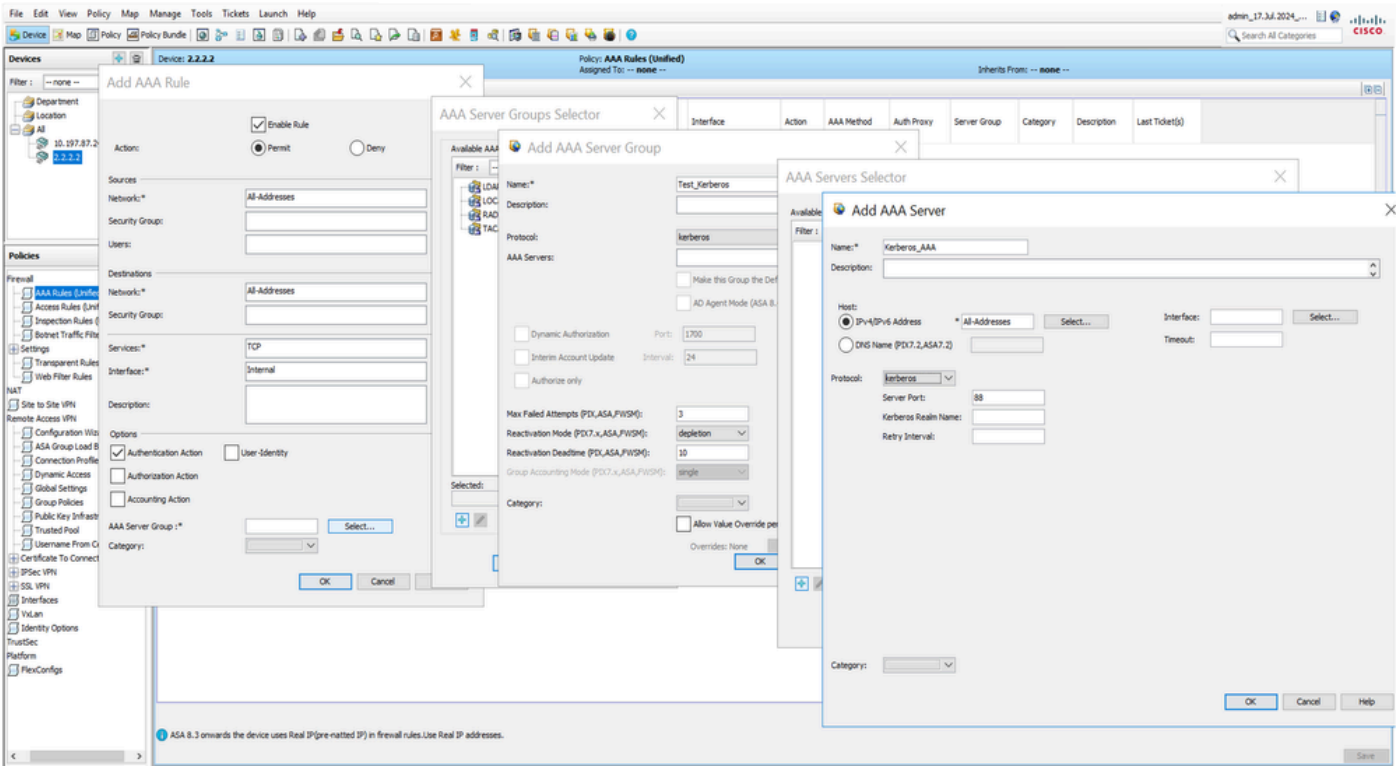


Konfiguration des CSM-Kerberos

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

1. Speichern
2. Vorschau der Konfiguration für das Ergebnis der Aktivitätsvalidierung

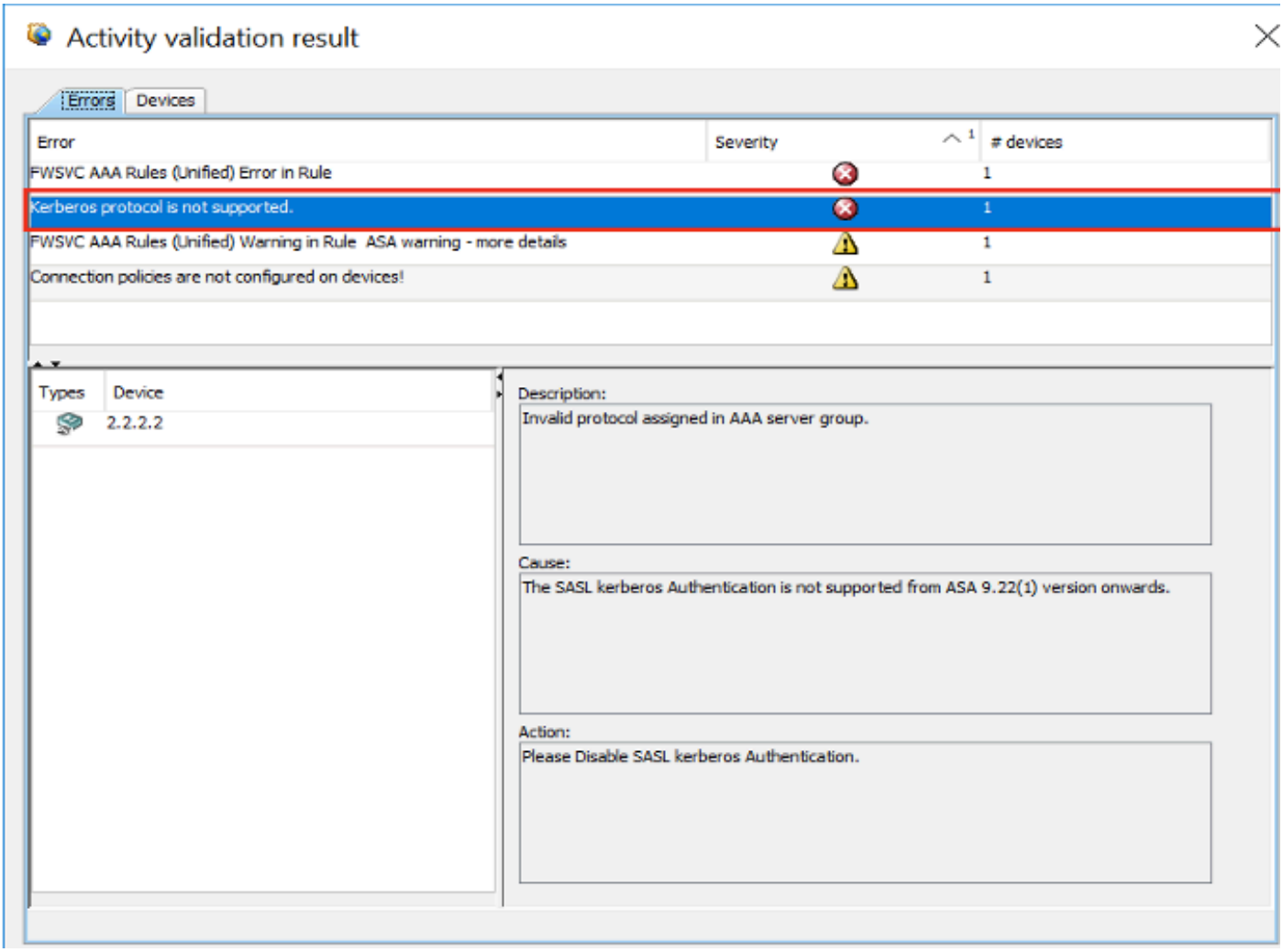




CSM-Kerberos-Konfiguration für LDAP-SASL

PFAD: CSM>Firewall > AAA-Regeln > AAA-Servergruppe > Hinzufügen > Protokoll > LDAP > SASL

1. Speichern
2. Vorschau der Konfiguration für das Ergebnis der Aktivitätsvalidierung



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.