Konfigurieren der Kerberos Single-Sign-On-Authentifizierung in SWA

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Konfiguration von Proxy-Benutzern für die Single-Sign-On (SSO)-Authentifizierung über Kerberos in Secure Web Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SWA-Verwaltung.
- Grundlegende Active Directory-Verwaltung.

Cisco empfiehlt die Installation der folgenden Tools:

- Physisches oder virtuelles SWA.

- Administrator-Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administrator-Zugriff auf das Active Directory

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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.

Vorbereitungen

Wenn der Proxy-Client versucht, auf eine Website zuzugreifen, und aufgefordert wird, die Anmeldeinformationen manuell einzugeben, gehen Sie zur Fehlerbehebung wie folgt vor.

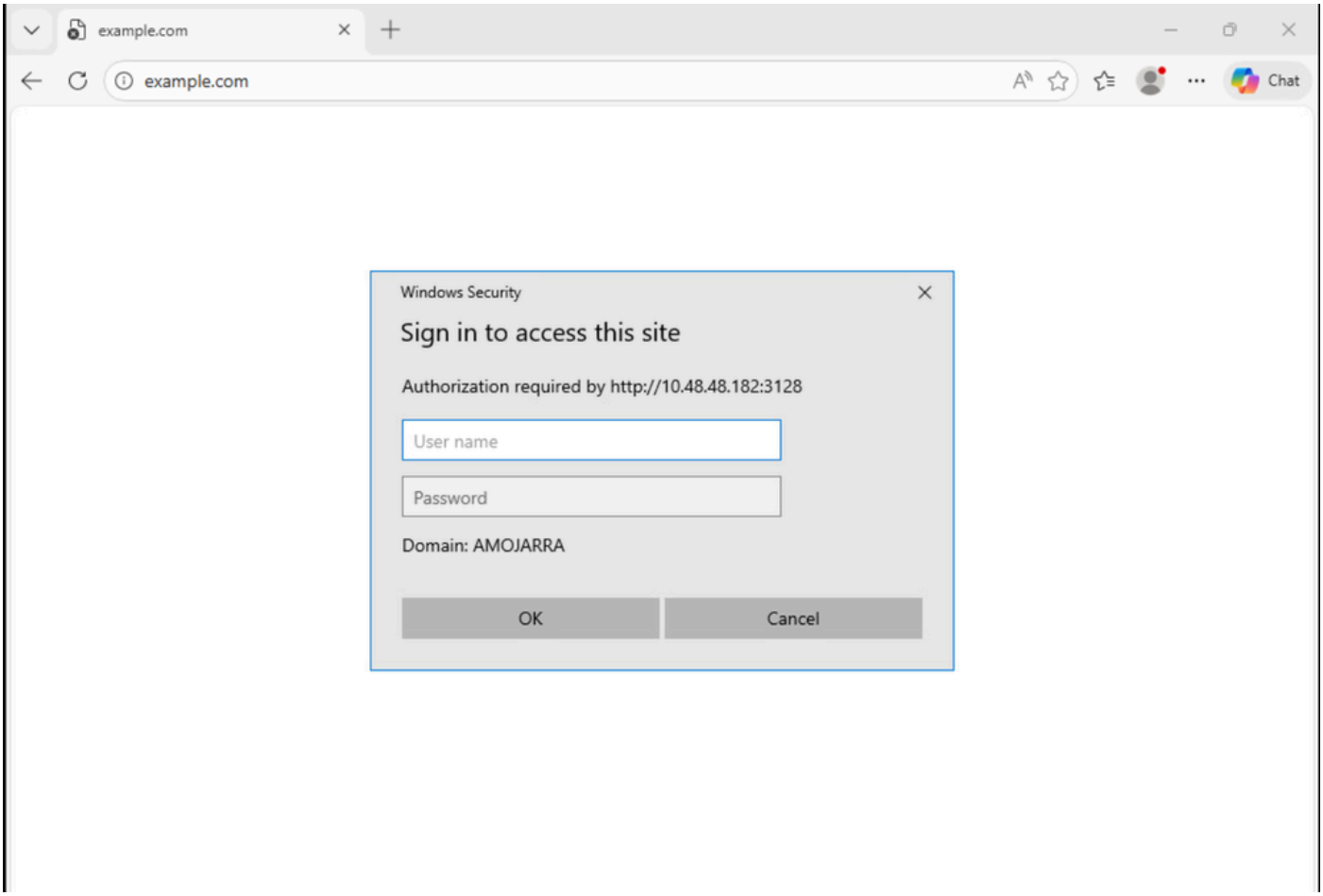


Bild - Aufforderung zur Benutzerauthentifizierung

Schritt 1: Überprüfen Sie die Zugriffsprotokolle für den Client.

Schritt 1.1. Melden Sie sich bei der CLI an.

Schritt 1.2. Führen Sie grep aus.

Schritt 1.3. Wählen Sie die Nummer aus, die mit der verknüpft ist. Zugriffsprotokolle.

Schritt 1.4. Geben Sie im Feld Geben Sie den regulären Ausdruck für grep die Client-IP-Adresse ein.

Schritt 1.5. Drücken Sie die Eingabetaste, bis Folgendes angezeigt wird: Möchten Sie die Protokolle zurücksetzen, geben Sie "Y" ein, und drücken Sie die Eingabetaste, bis die Accesslogs angezeigt werden.

Schritt 1.6. Wiederholen Sie das Problem, indem Sie versuchen, auf eine Website vom Client-PC zuzugreifen.

Schritt 1.7: Bestätigen Sie das Identifikationsprofil, dass der Datenverkehr eintrifft.

In diesem Beispiel lautet das Identifizierungsprofil Auth_ID:

```
1776248928.353 0 10.48.48.195 TCP_DENIED/407 0 GET http://cisco.com/ - NONE/- - OTHER-NONE-Auth_ID-NONE
```

Schritt 2: Überprüfen Sie das Identifikationsprofil.

Schritt 2.1. Melden Sie sich bei der SWA-GUI an.

Schritt 2.2: Wählen Sie im Websicherheits-Manager Identifikationsprofile aus.

Schritt 2.3: Klicken Sie auf den Namen des Identifikationsprofils, auf das der Datenverkehr traf.

Schritt 2.4. Bestätigen Sie, dass das Authentifizierungsschema nicht auf "Basic" (Grundlegend) festgelegt ist.

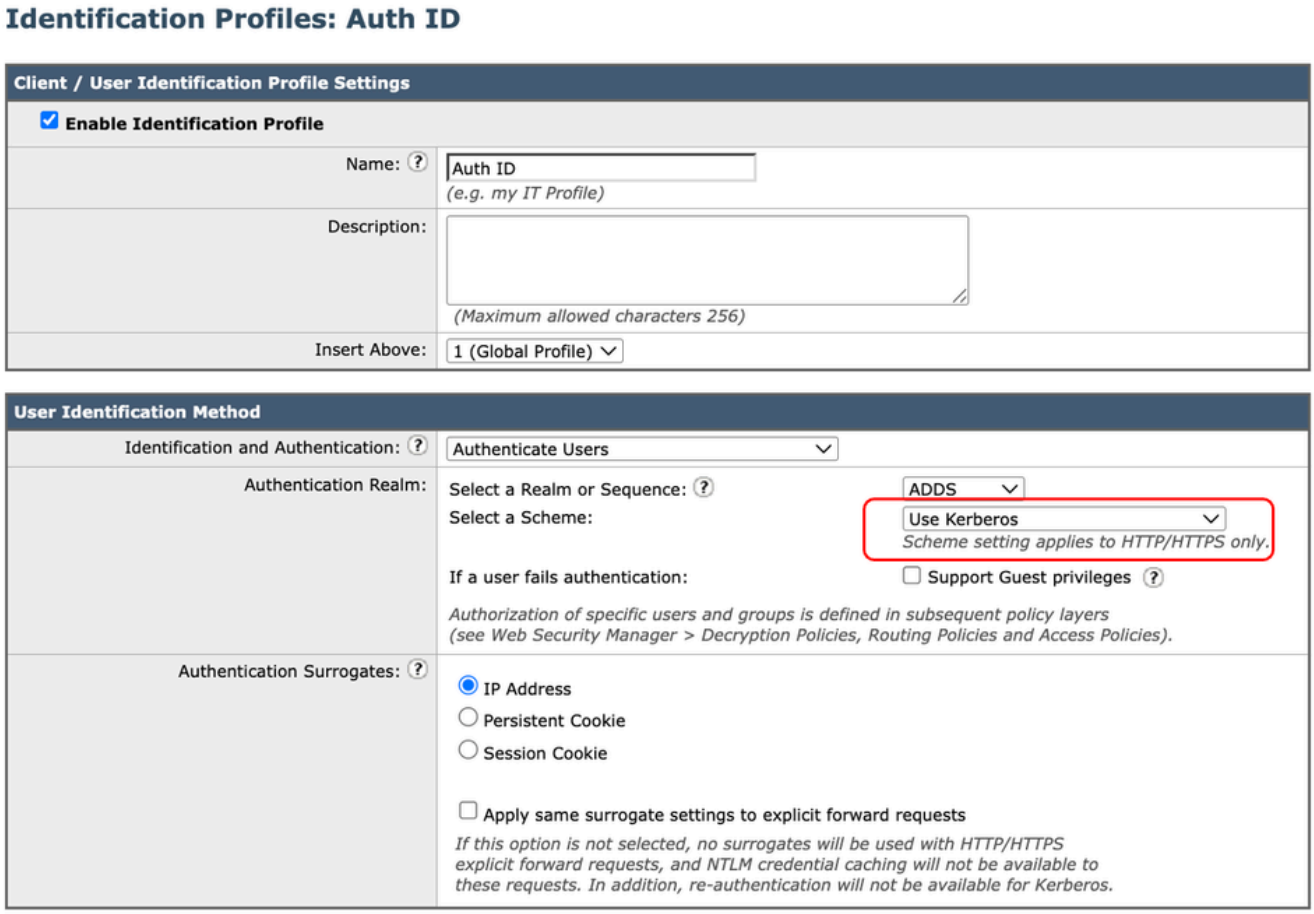


Bild - Authentifizierungsschema

Schritt 3: Testen der SWA- und Active Directory-Verbindungen

Schritt 3.1: Navigieren Sie in der SWA-GUI zu Netzwerk, und wählen Sie Authentication (Authentifizierung) aus.

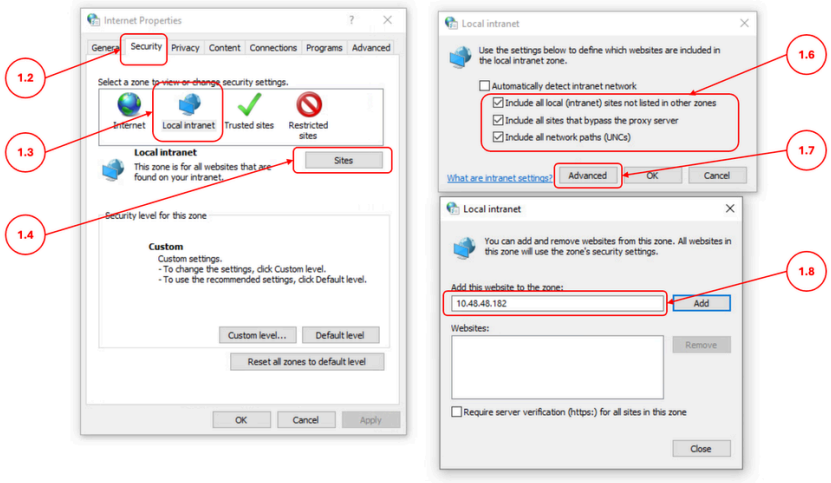
Schritt 3.2: Klicken Sie auf den Namen des Authentifizierungsbereichs.

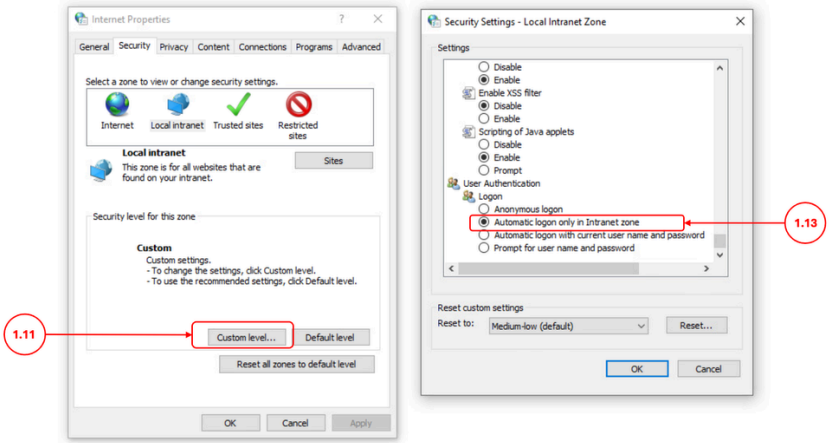
Schritt 3.3: Klicken Sie auf Test starten, um den Verbindungsstatus von SWA und Active Directory zu überprüfen.

Wenn keine Fehler gefunden werden, überprüfen Sie die Client-PC-Konfiguration wie in diesem Artikel beschrieben.

Client-PC konfigurieren

Überprüfen Sie anhand der folgenden Schritte die Client-PC-Konfiguration:

Schritte	Details
Schritt 1: Lokale Intranet-Sites	Schritt 1.1. Geben Sie im Startmenü Internet Option ein, und drücken Sie die Eingabetaste. Schritt 1.2. Klicken Sie im Fenster Interneteigenschaften auf die Registerkarte Sicherheit. Schritt 1.3. Wählen Sie Lokales Intranet. Schritt 1.4. Klicken Sie auf die Sites. Schritt 1.5. Vergewissern Sie sich, dass das Kontrollkästchen Intranetnetzwerk automatisch erkennen nicht aktiviert ist. Schritt 1.6. Wählen Sie alle drei Optionen aus: • Alle lokalen (Intranet-) Standorte einbeziehen, die nicht in anderen Zonen aufgeführt sind • Alle Standorte einbeziehen, die den Proxyserver umgehen • Alle Netzwerkpfade (UNC) einschließen Schritt 1.7. Klicken Sie auf Erweitert. Schritt 1.8: Geben Sie den FQDN oder die IP-Adresse Ihres SWA ein, und fügen Sie sie der Liste hinzu. Schritt 1.9. (Optional) Abhängig von Ihren internen Sicherheitsrichtlinien können Sie die Option Serververifizierung erforderlich deaktivieren.  Bild - Konfigurieren der lokalen Internet-Standorte Schritt 1.10. Klicken Sie auf Schließen und OK.

	Schritt 1.11. Klicken Sie auf der Registerkarte Sicherheit auf Stufe anpassen. Schritt 1.12: Navigieren Sie zu Benutzerauthentifizierung. Schritt 1.13. Stellen Sie sicher, dass die automatische Anmeldung nur in der Intranet-Zone ausgewählt ist.  Bild - Automatische Anmeldung für Intranet-Benutzer
Schritt 2: Sammeln der Protokolle	Wenn in Schritt 1 die SSO-Authentifizierung über Kerberos nicht behoben wurde: Schritt 2.1: Ändern Sie die SWA-Auth-Protokolle in Trace (Nachverfolgung), und überprüfen Sie die Protokolle. Schritt 2.2: Fügen Sie [Auth-Method = %m] den Zugriffsprotokollen als benutzerdefiniertes Feld hinzu. Weitere Informationen finden Sie unter: Konfigurieren Sie den Leistungsparameter in den Zugriffsprotokollen. Schritt 2.3: Führen Sie einen Paketerfassungsfilter für die Client-IP- und Active Directory-IP-Adresse aus, und bestätigen Sie, dass der Client PC das Kerberos-Service-Ticket an den SWA sendet.

Anmerkung: Stellen Sie sicher, dass Sie den FQDN des SWA in den Proxyeinstellungen Ihres Browsers konfiguriert haben.

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.0 für Cisco Secure Web Appliance

- Firewall für sichere Web-Appliance konfigurieren
- Konfigurieren der Paketerfassung auf der Content Security Appliance
- Konfigurieren von Leistungsparametern in Zugriffsprotokollen
- Zugreifen auf Protokolle der sicheren Web-Appliance
- Best Practices für sichere Web-Appliances - Cisco
- Umgehung der Authentifizierung in einer sicheren Web-Appliance - Cisco

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.