# Umgehen der Authentifizierung in einer sicheren Web-Appliance

## Inhalt


[Einleitung](#)

[Voraussetzungen](#)

- [Anforderungen](#)
- [Verwendete Komponenten](#)

[Authentifizierung ausschließen](#)

[Methoden zur Freistellung der Authentifizierung in Cisco SWA](#)

[Schritte zur Umgehung der Authentifizierung](#)

[Zugehörige Informationen](#)


## Einleitung

In diesem Dokument werden die Schritte zum Ausschließen der Authentifizierung in einer sicheren Webappliance (SWA) beschrieben.

## Voraussetzungen

### Anforderungen

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

- SWA-Verwaltung.

Cisco empfiehlt die Installation der folgenden Tools:

- Physisches oder virtuelles SWA
- Administratorzugriff auf die grafische Benutzeroberfläche (GUI) von SWA

### 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.

## Authentifizierung ausschließen

Die Freistellung der Authentifizierung für bestimmte Benutzer oder Systeme in der Cisco SWA kann entscheidend sein, um die Betriebseffizienz aufrechtzuerhalten und spezifische Anforderungen zu erfüllen. Zum einen erfordern einige Benutzer oder Systeme einen ununterbrochenen Zugriff auf kritische Ressourcen oder Dienste, der durch Authentifizierungsprozesse behindert werden könnte. So benötigen automatisierte Systeme oder Dienstkonten, die regelmäßige Updates oder Backups durchführen, einen nahtlosen Zugriff ohne Verzögerungen oder potenzielle Fehler aufgrund von Authentifizierungsmechanismen.

Darüber hinaus gibt es Szenarien, in denen der Webdienstanbieter empfiehlt, keinen Proxy für den Zugriff auf seinen Dienst zu verwenden. In solchen Fällen gewährleistet die Freistellung der Authentifizierung die Einhaltung der Anbieterrichtlinien und die Aufrechterhaltung der Dienstzuverlässigkeit. Um den Datenverkehr für bestimmte Benutzer effektiv zu blockieren, ist es zudem häufig erforderlich, diese zuerst von der Authentifizierung auszunehmen und dann die entsprechenden Blockierungsrichtlinien anzuwenden. Dieser Ansatz ermöglicht eine präzise Kontrolle der Zugriffsberechtigungen.

In einigen Fällen ist der Webdienst, auf den zugegriffen wird, vertrauenswürdig und allgemein akzeptabel, z. B. bei Microsoft-Updates. Die Befreiung der Authentifizierung für solche Dienste vereinfacht den Zugriff für alle Benutzer. Darüber hinaus gibt es Situationen, in denen das Benutzerbetriebssystem oder die Anwendung den konfigurierten Authentifizierungsmechanismus im SWA nicht unterstützt. Daher ist ein Bypass erforderlich, um die Verbindung sicherzustellen.

Server mit festen IP-Adressen ohne Benutzeranmeldungen und mit eingeschränktem, vertrauenswürdigem Internetzugriff erfordern keine Authentifizierung, da ihre Zugriffsmuster vorhersehbar und sicher sind.

Durch die strategische Freistellung der Authentifizierung in diesen Fällen können Unternehmen Sicherheitsanforderungen mit Betriebseffizienz in Einklang bringen.

## Methoden zur Freistellung der Authentifizierung in Cisco SWA

Die Freistellung der Authentifizierung in SWAs kann durch verschiedene Methoden erreicht werden, die jeweils auf bestimmte Szenarien und Anforderungen zugeschnitten sind. Es gibt einige gängige Methoden zum Konfigurieren von Authentifizierungsausnahmen:

- IP-Adresse oder Subnetzmaske: Eine der einfachsten Methoden besteht darin, bestimmte IP-Adressen oder ganze Subnetze von der Authentifizierung auszunehmen. Dies ist besonders für Server mit festen IP-Adressen oder vertrauenswürdigen Netzwerksegmenten nützlich, die einen unterbrechungsfreien Zugriff auf das Internet oder interne Ressourcen benötigen. Durch die Angabe dieser IP-Adressen oder Subnetzmasken in der SWA-Konfiguration können Sie sicherstellen, dass diese Systeme den Authentifizierungsprozess umgehen.
- Proxy-Ports: Sie können das SWA so konfigurieren, dass Datenverkehr auf Basis bestimmter Proxy-Ports von der Verarbeitung ausgenommen wird. Dies ist nützlich, wenn bestimmte Anwendungen oder Dienste designierte Ports für die Kommunikation verwenden.

Durch die Identifizierung dieser Ports können Sie die SWA so einrichten, dass die Authentifizierung für den Datenverkehr an diesen Ports umgangen wird, um einen nahtlosen Zugriff für die relevanten Anwendungen oder Services sicherzustellen.

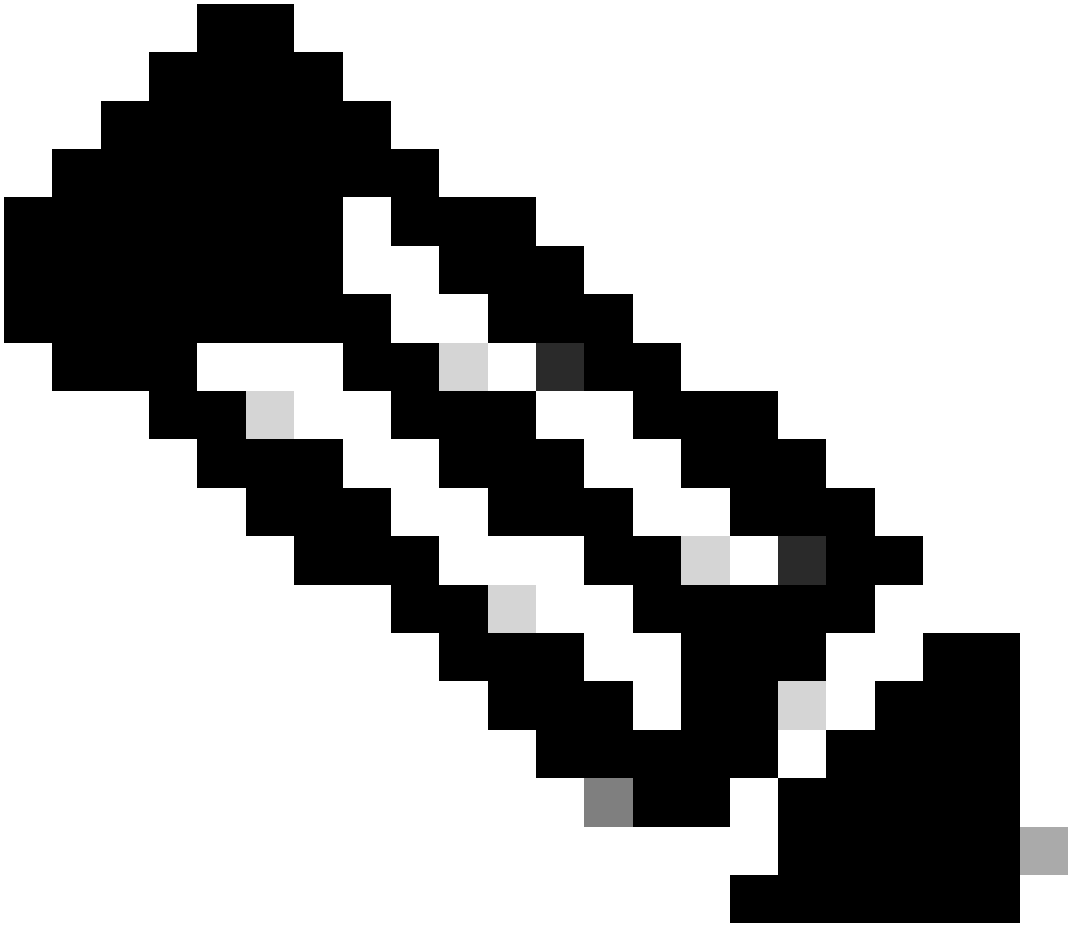
- URL-Kategorien: Eine weitere Methode besteht darin, die Authentifizierung auf Basis von URL-Kategorien auszunehmen. Dies kann sowohl vordefinierte Cisco Kategorien als auch benutzerdefinierte URL-Kategorien umfassen, die Sie auf Basis Ihrer unternehmensspezifischen Anforderungen definieren. Wenn beispielsweise bestimmte Webdienste wie Microsoft-Updates als vertrauenswürdig und allgemein akzeptabel eingestuft werden, können Sie die SWA so konfigurieren, dass die Authentifizierung für diese URL-Kategorien umgangen wird. Dadurch wird sichergestellt, dass alle Benutzer ohne Authentifizierung auf diese Services zugreifen können.
- Benutzer-Agents: Die Freistellung der Authentifizierung auf Basis von Benutzer-Agents ist nützlich, wenn es um bestimmte Anwendungen oder Geräte geht, die die konfigurierten Authentifizierungsmechanismen nicht unterstützen. Durch die Identifizierung der Benutzer-Agent-Strings dieser Anwendungen oder Geräte können Sie die SWA so konfigurieren, dass die Authentifizierung für den von ihnen ausgehenden Datenverkehr umgangen wird, um eine nahtlose Verbindung sicherzustellen.

.

## Schritte zur Umgehung der Authentifizierung

So erstellen Sie ein Identifizierungsprofil, das nicht authentifiziert werden soll:

Schritt 1: Wählen Sie in der GUI Web Security Manager aus, und klicken Sie dann auf Identification Profiles.
Schritt 2: Klicken Sie auf Profil hinzufügen, um ein Profil hinzuzufügen.
Schritt 3: Verwenden Sie das Kontrollkästchen Identifikationsprofil aktivieren, um dieses Profil zu aktivieren oder es schnell zu deaktivieren, ohne es zu löschen.
Schritt 4: Weisen Sie einen eindeutigen Profilnamen zu.
Schritt 5: (optional) Beschreibung hinzufügen.
Schritt 6: Wählen Sie aus der Dropdown-Liste Einfügen aus, wo dieses Profil in der Tabelle angezeigt werden soll.



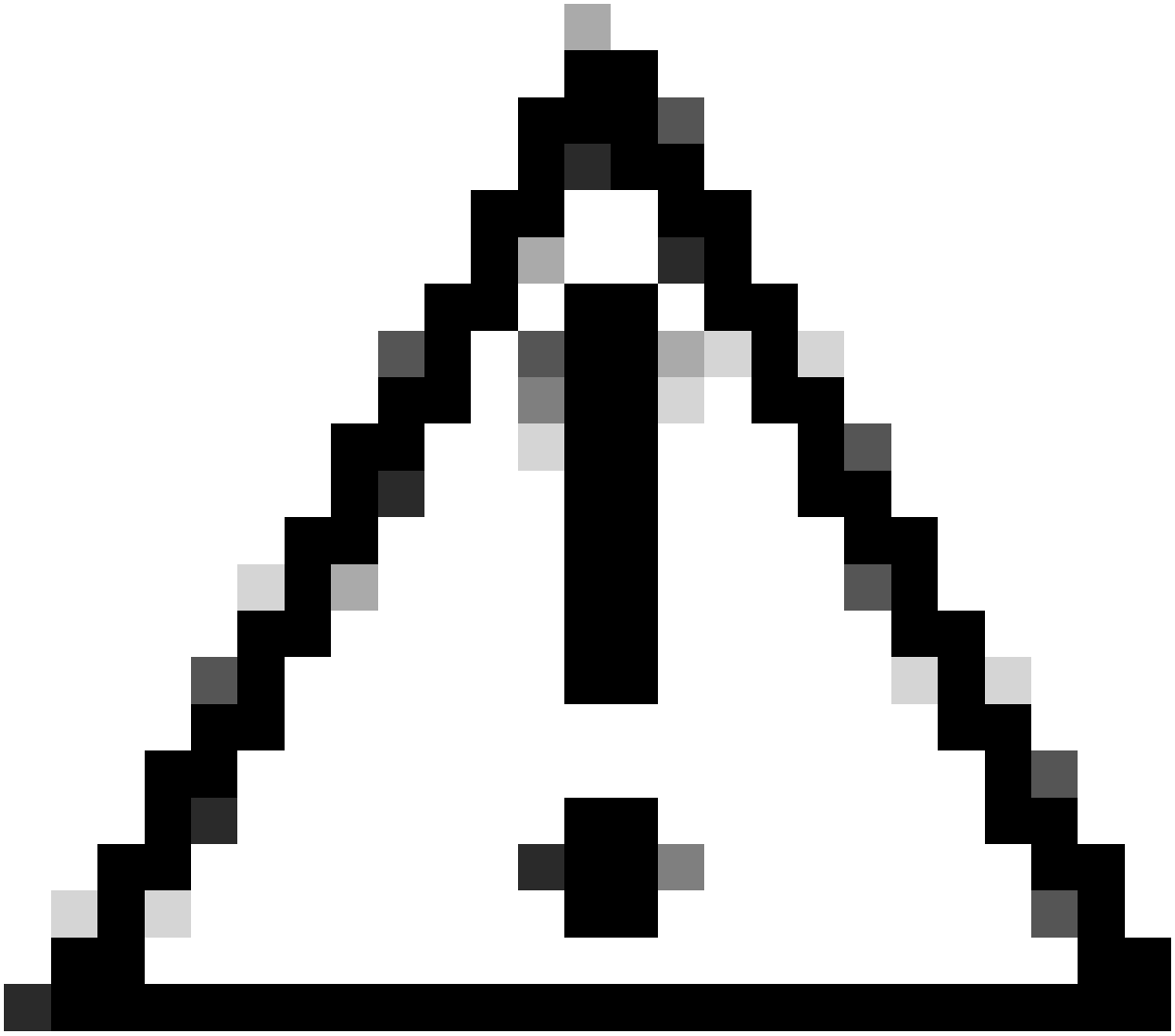
Hinweis: Positionieren Sie Identifikationsprofile, die keine Authentifizierung erfordern, ganz oben in der Liste. Dieser Ansatz entlastet die SWA, minimiert die Authentifizierungswarteschlange und führt zu einer schnelleren Authentifizierung für andere Benutzer.

---

Schritt 7. Wählen Sie im Abschnitt User Identification Method die Option Exempt from authentication/identification (Von Authentifizierung/Identifizierung ausnehmen) aus.

Schritt 8: Geben Sie unter Mitglieder nach Subnetz definieren die IP-Adressen oder Subnetze ein, die dieses Identifikationsprofil anwenden muss. Sie können IP-Adressen, CIDR-Blöcke (Classless Inter-Domain Routing) und Subnetze verwenden.

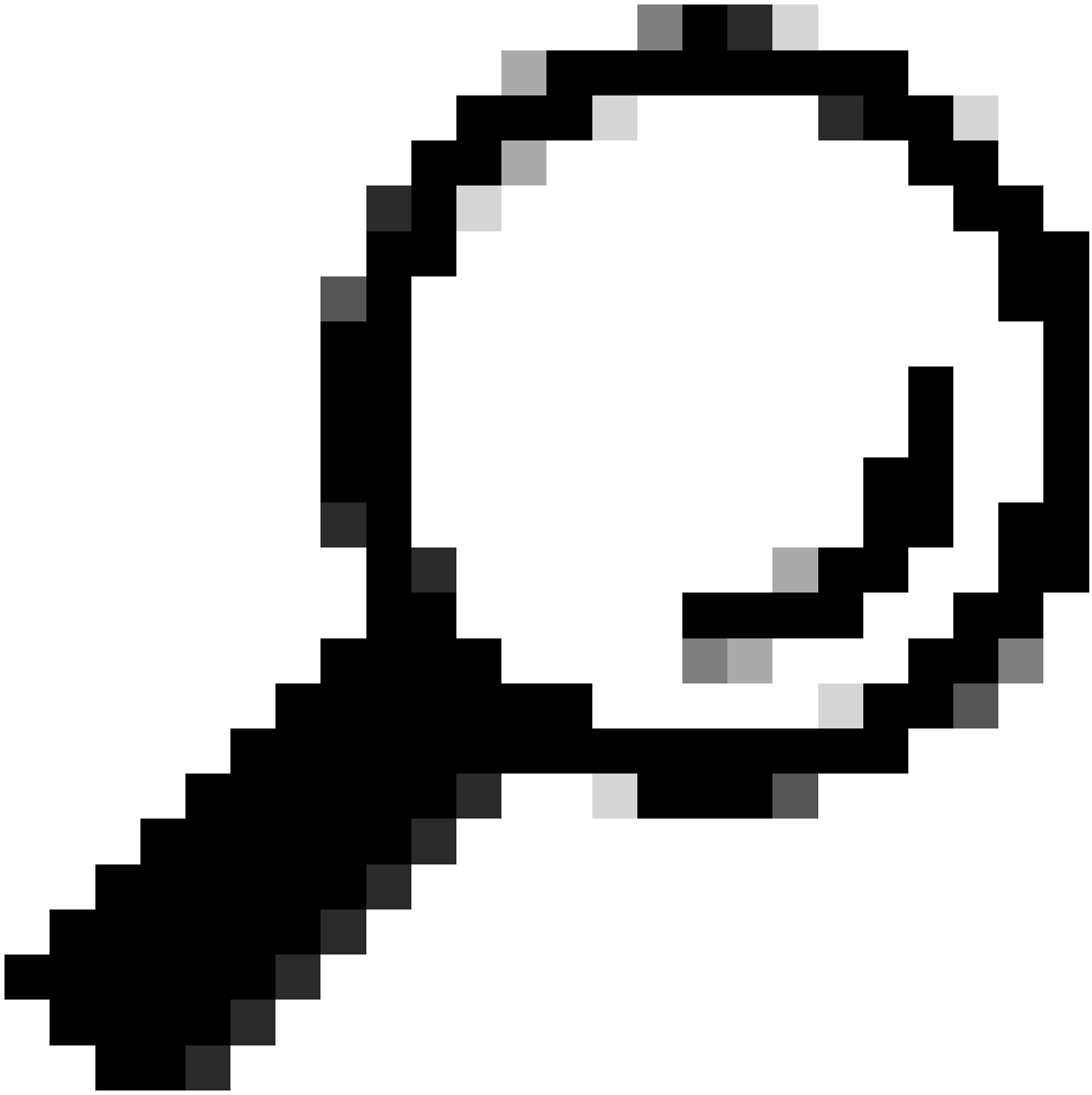
Schritt 9. (Optional) Klicken Sie auf "Erweitert", um zusätzliche Mitgliedschaftskriterien zu definieren, z. B. Proxy-Ports, URL-Kategorien oder Benutzer-Agents.



Achtung: Bei einer transparenten Proxy-Bereitstellung kann SWA keine Benutzer-Agenten oder die vollständige URL für HTTPS-Datenverkehr lesen, es sei denn, der Datenverkehr wird entschlüsselt. Wenn Sie das Identifizierungsprofil mithilfe von Benutzer-Agents oder einer benutzerdefinierten URL-Kategorie mit regulären Ausdrücken konfigurieren, stimmt dieser Datenverkehr nicht mit dem Identifizierungsprofil überein.

---

Weitere Informationen zum Konfigurieren einer benutzerdefinierten URL-Kategorie finden Sie unter: [Konfigurieren benutzerdefinierter URL-Kategorien in einer sicheren Webappliance - Cisco]



Tipp: Die Richtlinie verwendet eine AND-Logik, d. h., dass alle Bedingungen erfüllt sein müssen, damit das ID-Profil übereinstimmt. Wenn erweiterte Optionen festgelegt sind, muss jede einzelne Anforderung erfüllt sein, damit die Richtlinie angewendet werden kann.

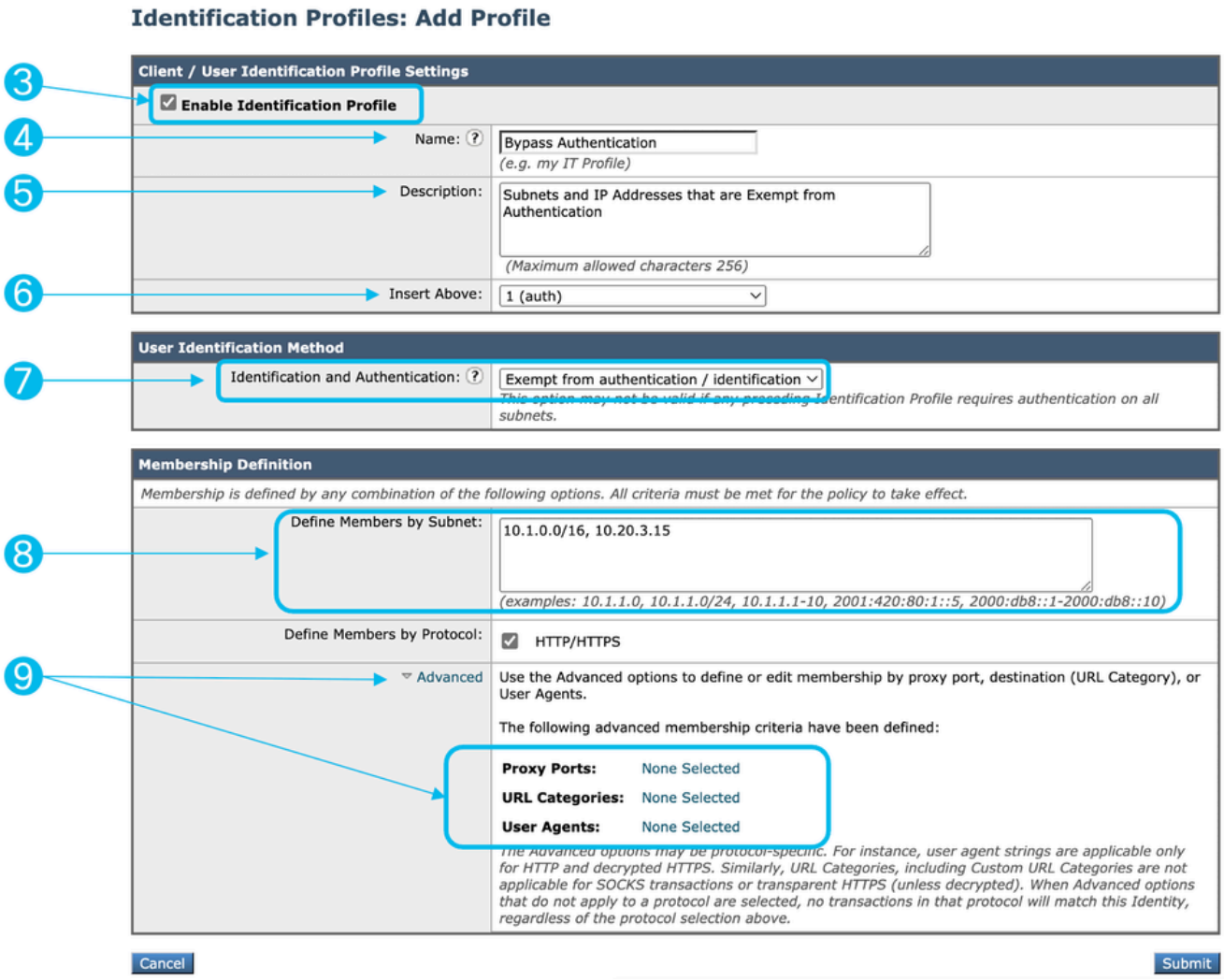



Bild - Schritte zum Erstellen eines ID-Profils zum Umgehen der Authentifizierung

Schritt 10. Änderungen einsenden und bestätigen.

# Zugehörige Informationen

- [Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Web Appliance - GD(Allgemeine Bereitstellung) - Endbenutzer für Richtlinienanwendung klassifizieren [Cisco Secure Web Appliance] - Cisco]
- [Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco]
- [Wie kann Office 365-Datenverkehr auf der Cisco Web Security Appliance (WSA) von der Authentifizierung und Entschlüsselung ausgenommen werden - 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.