

Konfiguration der 802.1X-Host- und Sitzungsauthentifizierung auf Switches der Serien 200, 220 und 300

Ziel

802.1X ist ein IEEE-Standard für Port-basierte Netzwerkzugriffskontrolle (Network Access Control, PNAC), der Geräten, die mit Ports verbunden sind, eine Authentifizierungsmethode bereitstellt. Auf der Seite Host and Session Authentication (Host- und Sitzungsauthentifizierung) in der Administrations-GUI des Switches wird definiert, welcher Authentifizierungstyp für jeden Port verwendet wird. Die portabhängige Authentifizierung ist eine Funktion, mit der Netzwerkadministratoren die Switch-Ports nach dem gewünschten Authentifizierungstyp aufteilen können. Die Seite "Authentifizierte Hosts" zeigt Informationen über Hosts an, die authentifiziert wurden.

In diesem Artikel wird erläutert, wie die Host- und Sitzungsauthentifizierung auf Port-Basis konfiguriert wird und wie die authentifizierten Hosts in den 802.1X-Sicherheitseinstellungen auf den Managed Switches der Serien 200, 220 und 300 angezeigt werden.

Unterstützte Geräte

- Sx200-Serie
- Sx220-Serie
- Sx300-Serie

Software-Version

- 1.4.5.02 — Serie Sx200, Serie Sx300
- 1.1.0.14 - Sx220-Serie

Host- und Sitzungsauthentifizierung

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Security > 802.1X > Host and Session Authentication** aus.

Hinweis: Die unten stehenden Bilder stammen vom SG220-26P Smart Switch.



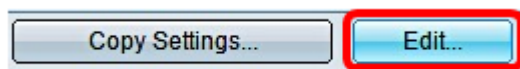
Schritt 2: Klicken Sie auf das Optionsfeld des Ports, den Sie bearbeiten möchten.

Host and Session Authentication

Host and Session Authentication Table							
	Entry No.	Port	Host Authentication	Single Host			
				Action on Violation	Traps	Trap Frequency	Number of Violation
<input type="radio"/>	1	GE1	Multiple Host				
<input checked="" type="radio"/>	2	GE2	Multiple Host				
<input type="radio"/>	3	GE3	Multiple Host				
<input type="radio"/>	4	GE4	Multiple Host				
<input type="radio"/>	5	GE5	Multiple Host				
<input type="radio"/>	6	GE6	Multiple Host				
<input type="radio"/>	7	GE7	Multiple Host				

Hinweis: In diesem Beispiel wird Port GE2 ausgewählt.

Schritt 3: Klicken Sie auf **Bearbeiten**, um die Host- und Sitzungsauthentifizierung für den angegebenen Port zu bearbeiten.



Schritt 4: Das Fenster "Edit Port Authentication" wird angezeigt. Stellen Sie in der Dropdown-Liste Interface (Schnittstelle) sicher, dass der angegebene Port derjenige ist, den Sie in Schritt 2 gewählt haben. Andernfalls klicken Sie auf den Dropdown-Pfeil, und wählen Sie den richtigen Port aus.

Interface: Port

Host Authentication: Single Host Multiple Host Multiple Sessions

Hinweis: Wenn Sie die Serie 200 oder 300 verwenden, wird das Fenster "Edit Host and Session Authentication" angezeigt.

Schritt 5: Klicken Sie im Feld "*Host Authentication*" auf das Optionsfeld für den gewünschten Authentifizierungsmodus. Folgende Optionen sind verfügbar:

- Single Host - Der Switch gewährt nur einem autorisierten Host Zugriff auf den Port.
- Multiple Host (802.1X) - Mehrere Hosts können Zugriff auf den einzelnen Port erhalten. Dies ist der Standardmodus. Für den Switch muss nur der erste Host autorisiert werden. Anschließend haben alle anderen Clients, die an den Port angeschlossen sind, Zugriff auf das Netzwerk. Sollte die Authentifizierung fehlschlagen, wird dem ersten Host und allen verbundenen Clients der Zugriff auf das Netzwerk verweigert.
- Mehrere Sitzungen - Mehrere Hosts können Zugriff auf einen einzelnen Port erhalten, jeder Host muss jedoch authentifiziert werden.

Hinweis: In diesem Beispiel wird Single host ausgewählt.

Interface: Port

Host Authentication: Single Host
 Multiple Host
 Multiple Sessions

Hinweis: Wenn Sie die Option "Mehrere Hosts" oder "Mehrere Sitzungen" ausgewählt haben, fahren Sie mit [Schritt 9 fort](#).

Schritt 6: Klicken Sie im Bereich Single Host Violation Settings (Einstellungen für Host-Verletzung) auf das Optionsfeld für die gewünschte Aktion bei Verletzung. Eine Verletzung tritt auf, wenn Pakete von einem Host mit einer MAC-Adresse eingehen, die nicht mit der MAC-Adresse des ursprünglichen Supplicant übereinstimmt. In diesem Fall bestimmt die Aktion, was mit Paketen geschieht, die von Hosts stammen, die nicht als die ursprüngliche Komponente betrachtet werden. Folgende Optionen sind verfügbar:

- Schützen (Verwerfen) - Verwirft die Pakete. Dies ist die Standardaktion.
- Restrict (Forward) (Einschränken (Weiterleiten)): Gewährt Zugriff auf und leitet die Pakete weiter.
- Herunterfahren - Die Pakete werden blockiert und der Port wird heruntergefahren. Der Port bleibt inaktiv, bis er wieder aktiviert wird oder bis der Switch neu gestartet wird.

Hinweis: In diesem Beispiel wird die Option Restrict (Forward) (Einschränken (Weiterleiten)) ausgewählt.

Single Host Violation Settings:

Action on Violation: Protect (Discard)
 Restrict (Forward)
 Shutdown

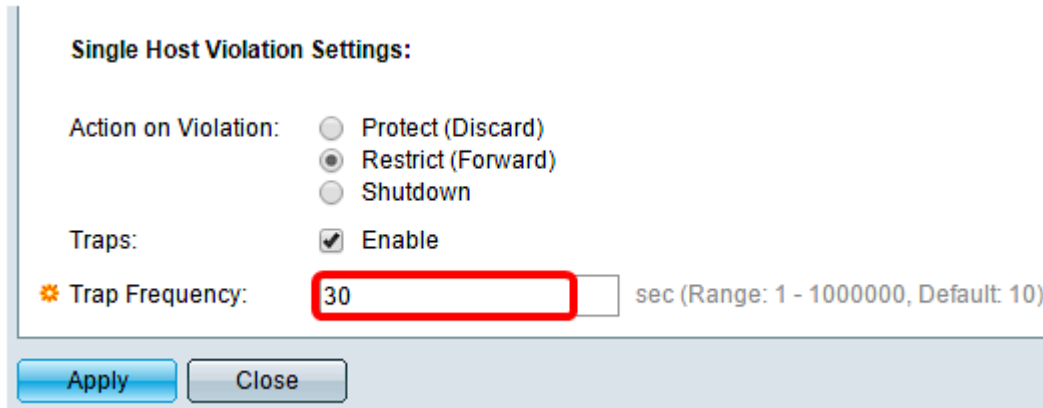
Schritt 7: Aktivieren Sie optional im Feld *Traps* die Option **Aktivieren**, um Traps zu aktivieren. Traps werden als SNMP-Nachrichten (Simple Network Management Protocol) generiert, mit denen Systemereignisse gemeldet werden. Wenn eine Verletzung auftritt, wird ein Trap an den SNMP-Manager des Switches gesendet.

Single Host Violation Settings:

- Action on Violation: Protect (Discard)
 Restrict (Forward)
 Shutdown
- Traps: Enable

Schritt 8: Geben Sie im Feld *Trap-Frequenz* die gewünschte zulässige Zeit in Sekunden zwischen gesendeten Traps ein. Legt fest, wie oft Traps gesendet werden.

Hinweis: In diesem Beispiel wird 30 Sekunden verwendet.



Single Host Violation Settings:

Action on Violation: Protect (Discard)
 Restrict (Forward)
 Shutdown

Traps: Enable

☀ Trap Frequency: sec (Range: 1 - 1000000, Default: 10)

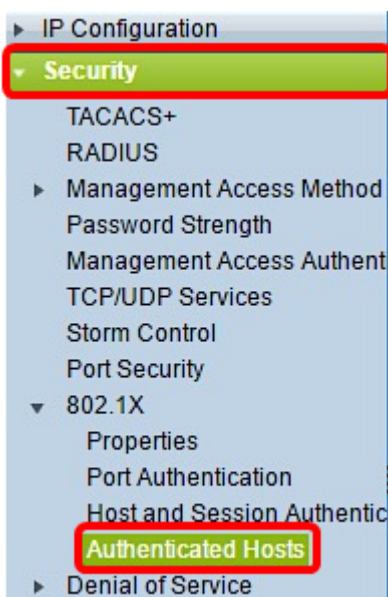
Apply Close

Schritt 9. Klicken Sie auf Apply (Anwenden).

Sie sollten nun Host- und Sitzungsauthentifizierung auf Ihrem Switch konfiguriert haben.

Authentifizierte Hosts anzeigen

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Security > 802.1X > Authenticated Host** aus.



Die Tabelle für authentifizierte Hosts zeigt die folgenden Informationen für authentifizierte Hosts an.

Authenticated Hosts

Authenticated Host Table					
User Name	Port	Session Time (DD:HH:MM:SS)	Authentication Method	MAC Address	VLAN ID
0 results found.					

- Benutzername - Gibt den Supplicant-Namen an, der auf dem Port authentifiziert wurde.
- Port - Gibt die Portnummer an, mit der der Supplicant verbunden ist.
- Session Time (Sitzungszeit): Gibt die gesamte Zeit an, die der Supplicant mit dem Port verbunden war. Das Format ist DD:HH:MM:SS (Day:Hour:Minute:Second).
- Authentifizierungsmethode — Gibt die Authentifizierungsmethode an. Folgende Werte sind gültig:
 - None - Gibt an, dass die Komponente nicht authentifiziert wurde.
 - Radius - Gibt an, dass die Komponente vom RADIUS-Server authentifiziert wurde.
 - MAC-Adresse - Gibt die MAC-Adresse des Supplicant an.
 - VLAN-ID - Gibt an, zu welchem VLAN der Host gehört. Die Spalte "VLAN ID" ist nur bei den Smart Plus Switches der Serie 220 verfügbar.

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.