802.1X Port Authentication Configuration auf Cisco Managed Switches der Serien 200 und 300

Ziel

Ziel dieses Dokuments ist es, die 801.1X-Port-Authentifizierung für die Managed Switches der Serien 200 und 300 zu erläutern. 802.1X-Port-Authentifizierung ermöglicht die Konfiguration von 802.1X-Parametern für jeden Port. Ein Port, der Authentifizierung anfordert, wird als Supplicant bezeichnet. Der Authentifizierer ist ein Switch oder Access Point, der als Netzwerkwächter für Supplicants fungiert. Der Authentifikator leitet Authentifizierungsmeldungen an den RADIUS-Server weiter, sodass ein Port authentifiziert werden kann und Informationen senden und empfangen kann.

Unterstützte Geräte

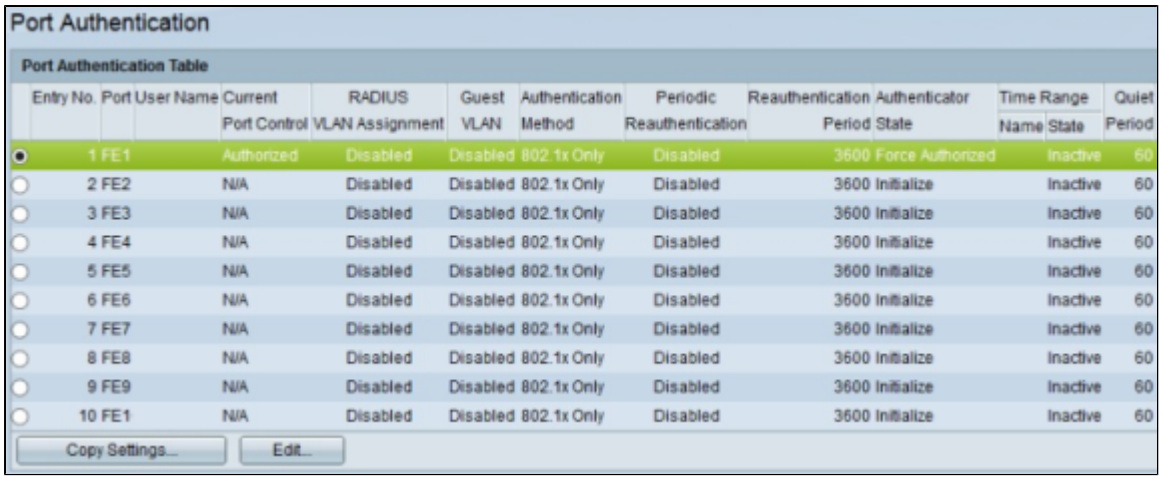
ãƒ» Managed Switches der Serien SF/SG 200 und SF/SG 300

Software-Version

â€¢1.3.0.62

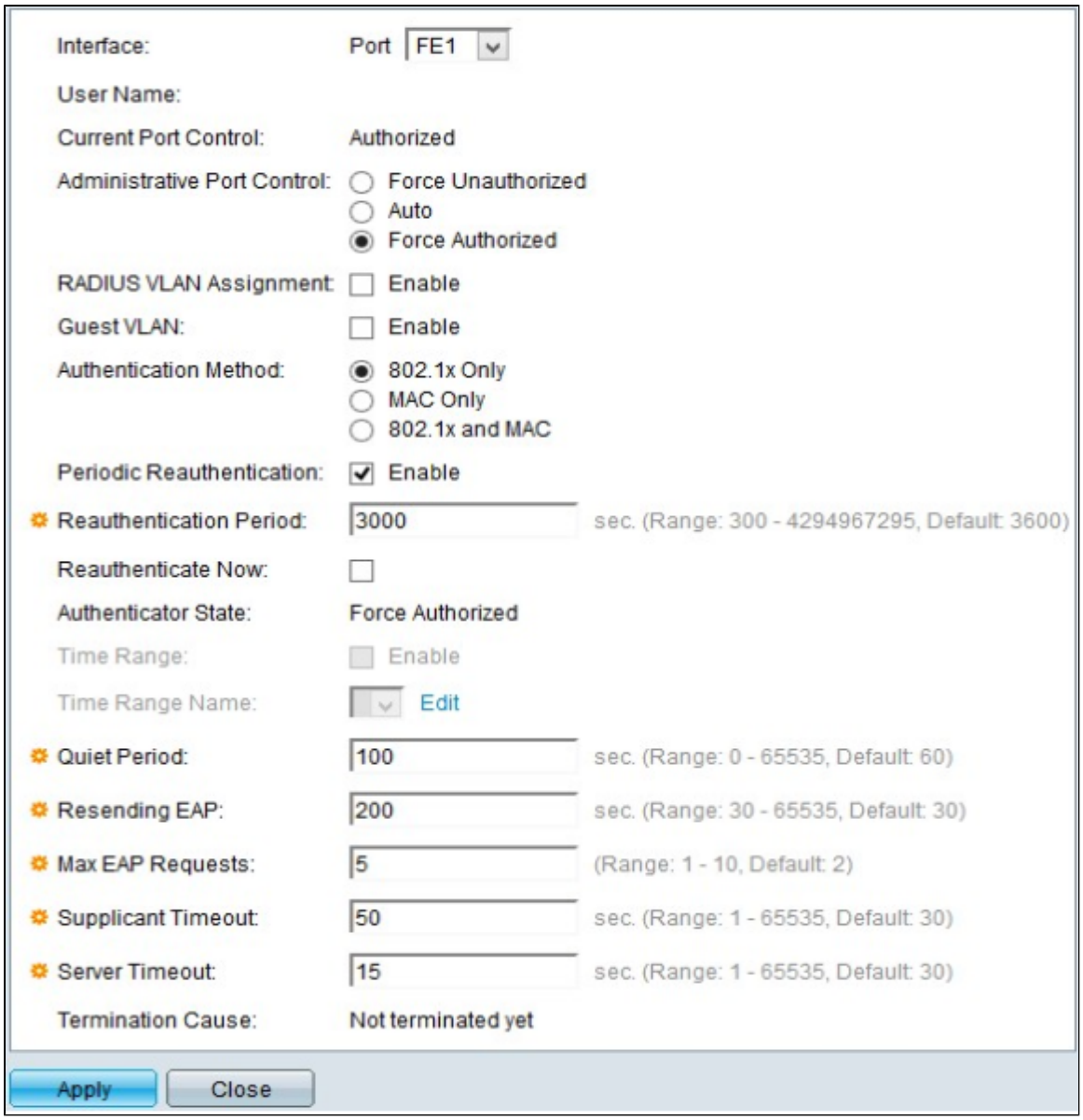
Konfiguration der Port-Authentifizierung

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > 802.1x > Port Authentication aus**. Die Seite *Port Authentication* wird geöffnet:



Schritt 2: Klicken Sie auf das Optionsfeld für den Port, den Sie bearbeiten möchten.

Schritt 3: Klicken Sie auf **Bearbeiten**. Das Fenster *Edit Port Authentication* wird angezeigt.



Im Feld User Name (Benutzername) wird der Benutzername des Ports angezeigt.

Hinweis: Im Feld "Current Port Control" (Aktuelle Portsteuerung) wird der aktuelle Portstatus angezeigt. Wenn sich der Port im Status Unauthorized befindet, bedeutet dies, dass der Port entweder nicht authentifiziert ist, oder dass Administrative Port Control auf Force Unauthorized festgelegt ist. Befindet sich der Port hingegen im Authorized-Status, bedeutet dies, dass er entweder authentifiziert ist oder dass Administrative Port Control auf Force Authorized festgelegt ist.

Schritt 4: Klicken Sie im Feld "Administrative Port Control" (Administrative Port-Steuerung) auf eines der verfügbaren Optionsfelder, um den Port-Autorisierungsstatus zu bestimmen:

ãƒ» Unautorisierte erzwingen â€" Mit dieser Option wird die ausgewählte Schnittstelle in den Status Unautorisiert verschoben. In diesem Zustand ermöglicht der Switch keine Authentifizierung des mit der Schnittstelle verbundenen Clients.

ãƒ» Auto (Automatisch): Diese Option ermöglicht die Authentifizierung und Autorisierung auf der ausgewählten Schnittstelle. In diesem Zustand stellt der Switch den mit der Schnittstelle verbundenen Clients eine 802.1X-Authentifizierung zur Verfügung und entscheidet auf der Grundlage des Austausches von Authentifizierungsinformationen mit dem Client, ob der Client authentifiziert ist oder nicht, und verschiebt die Schnittstelle in den Status Authorized (Autorisiert) oder Unauthorized (Nicht autorisiert).

ãƒ» Force Authorized - Mit dieser Option wird die Schnittstelle auf Authorized ohne Client-Authentifizierung gesetzt.

Schritt 5: Aktivieren Sie im Feld Gast-VLAN das Kontrollkästchen **Aktivieren,** um ein Gast-VLAN für nicht autorisierte Ports zu verwenden.

Schritt 6: Klicken Sie im Feld "Authentication Method" auf eine der verfügbaren Optionsschaltflächen, um den Port zu authentifizieren. Folgende Optionen sind verfügbar:

ãƒ» Nur 802.1X: Nur 802.1X-Authentifizierung wird für den Port durchgeführt.

ãƒ» Nur MAC - Nur die MAC-basierte Authentifizierung wird für den Port durchgeführt. An einem einzelnen Port können nur 8 MAC-basierte Authentifizierungen durchgeführt werden.

ãƒ» 802.1X und MAC: Beide Authentifizierungsverfahren werden auf dem Port durchgeführt.

Schritt 7. Aktivieren Sie im Feld "Periodic Reauthentication" das Kontrollkästchen **Enable**, um die regelmäßige Authentifizierung des Ports auf Basis des Werts für den Reauthentication-Zeitraum zu aktivieren.

Schritt 8: Geben Sie im Feld "Reauthentication Period" die Zeit in Sekunden ein, nach der der Port erneut authentifiziert werden soll.

Schritt 9. Aktivieren Sie das Kontrollkästchen **Jetzt neu authentifizieren**, um den Port sofort neu zu authentifizieren.

Hinweis: Das Feld "Authenticator State" (Authentifizierungsstatus) zeigt den aktuellen Authentifizierungsstatus an.

Schritt 10. (Optional) Wenn die portbasierte Authentifizierung auf dem Switch aktiviert ist, sind die Felder "Time Range" (Zeitbereich) und "Time Range Name" (Name des Zeitbereichs) aktiviert. Geben Sie im Feld "Time Range" (Zeitbereich) die Zeit (in Sekunden) ein, zu der der Port verwendet werden darf, wenn die 802.1X-Autorisierung aktiviert ist. Wählen Sie in der Dropdown-Liste "Time Range Name" (Name des Zeitbereichs) das Profil aus, das den Zeitraum identifiziert.

Schritt 11. Geben Sie in das Feld "Quiet Period" (Stille Periode) ein, wie lange der Switch nach einem fehlgeschlagenen Authentifizierungsaustausch im Status "Quiet" (Geräumiger Zustand) bleibt. Wenn sich der Switch im Ruhezustand befindet, bedeutet dies, dass der Switch keine neuen Authentifizierungsanforderungen vom Client abhört.

Schritt 12: Geben Sie in das Feld Resending EAP (Extensible Authentication Protocol) (Erneutes Senden des EAP (Erweiterbares Authentifizierungsprotokoll)) die Zeit ein, die der Switch auf eine Antwortnachricht von der Komponente wartet, bevor er eine Anforderung erneut sendet.

Schritt 13: Geben Sie im Feld Max EAP Requests (Max. EAP-Anfragen) die maximale Anzahl der EAP-Anfragen ein, die gesendet werden können. EAP ist eine Authentifizierungsmethode, die in 802.1X verwendet wird und den Austausch von Authentifizierungsinformationen zwischen dem Switch und dem Client ermöglicht. In diesem Fall werden EAP-Anfragen zur Authentifizierung an den Client gesendet. Der Client muss dann antworten und die Authentifizierungsinformationen abgleichen. Wenn der Client nicht antwortet, wird eine weitere EAP-Anforderung auf Basis des Resending EAP-Werts festgelegt, und der Authentifizierungsprozess wird neu gestartet.

Schritt 14: Geben Sie im Feld Supplicant Timeout (Supplicant-Zeitüberschreitung) die Zeit ein, bevor EAP-Anfragen erneut an den Supplicant gesendet werden.

Schritt 15: Geben Sie im Feld Server Timeout (Serverzeitüberschreitung) die Zeit ein, die verstreicht,

bevor der Switch eine neue Anforderung an den RADIUS-Server sendet.

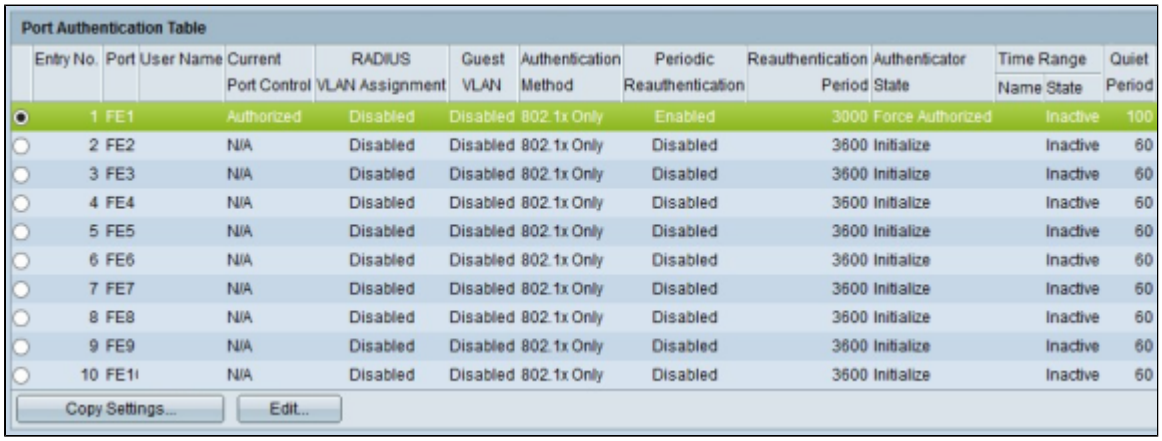
Im Feld "Terminierungsursache" werden die Gründe für einen Fehler bei der Port-Authentifizierung angezeigt.

Schritt 16: Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

Anwenden einer Schnittstellenkonfiguration auf mehrere Schnittstellen

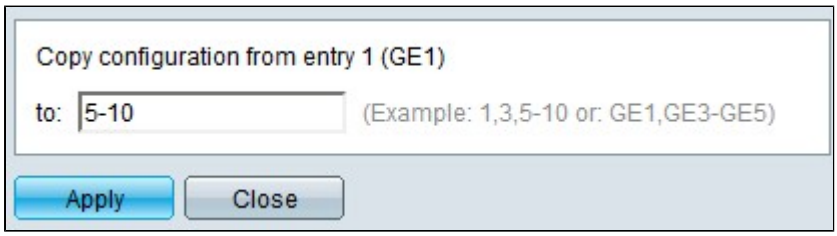
In diesem Abschnitt wird erläutert, wie die 802.1X-Authentifizierungskonfiguration eines Ports auf mehrere Ports angewendet wird.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > 802.1x > Port Authentication aus**. Die Seite *Port Authentication* wird geöffnet:



Schritt 2: Klicken Sie auf das Optionsfeld der Schnittstelle, auf die Sie die Authentifizierungskonfiguration auf mehrere Schnittstellen anwenden möchten.

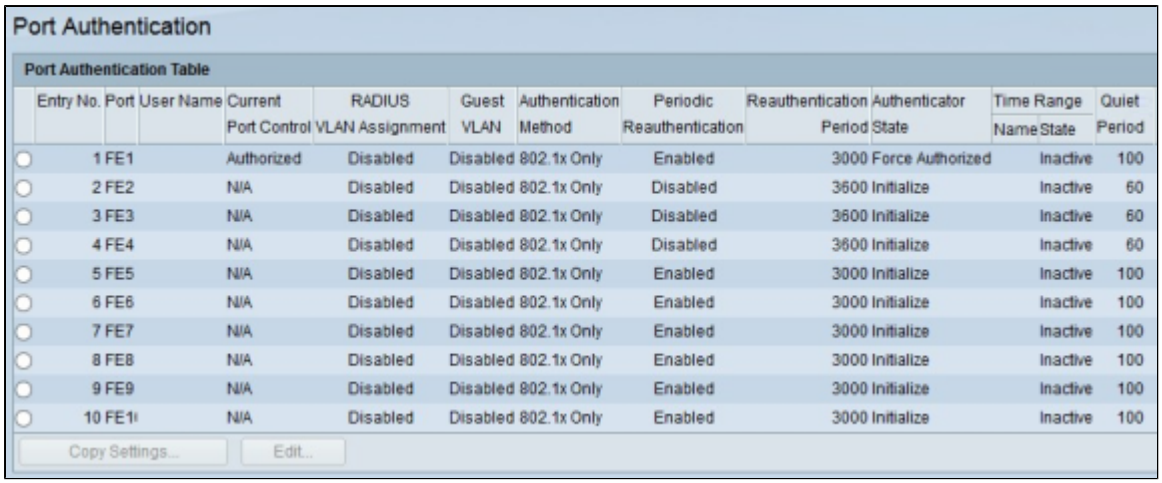
Schritt 3: Klicken Sie auf **Einstellungen kopieren**. Das Fenster *Copy Settings* wird angezeigt.



Schritt 4: Geben Sie im Feld **to** den Bereich der Schnittstellen ein, für die Sie die Konfiguration der in Schritt 2 ausgewählten Schnittstelle übernehmen möchten. Sie können die Schnittstellennummern oder den Namen der Schnittstellen als Eingabe verwenden. Sie können jede Schnittstelle durch ein Komma getrennt eingeben (z. B. 1, 3, 5 oder GE1, GE3, GE5) oder Sie können einen Bereich von Schnittstellen eingeben (z. B. 1-5 oder GE1-GE5).

Schritt 5: Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

Die nachfolgende Abbildung zeigt die Änderungen nach der Konfiguration.



Port Authentication

Port Authentication Table

	Entry No.	Port	User Name	Current Port Control	RADIUS VLAN Assignment	Guest VLAN	Authentication Method	Periodic Reauthentication	Reauthentication Period	Authenticator State	Time Range Name	Time Range State	Quiet Period
○	1	FE1		Authorized	Disabled	Disabled	802.1x Only	Enabled	3000	Force Authorized		Inactive	100
○	2	FE2		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	3	FE3		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	4	FE4		N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
○	5	FE5		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
○	6	FE6		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
○	7	FE7		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
○	8	FE8		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
○	9	FE9		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100
○	10	FE1		N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize		Inactive	100

Copy Settings... Edit...

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.