

Configurazione dell'impostazione di autenticazione della porta 802.1x su uno switch

Obiettivo

IEEE 802.1x è uno standard che facilita il controllo dell'accesso tra un client e un server. Prima che i servizi possano essere forniti a un client da una LAN (Local Area Network) o da uno switch, il client connesso alla porta dello switch deve essere autenticato dal server di autenticazione che esegue RADIUS (Remote Authentication Dial-In User Service).

L'autenticazione 802.1x impedisce ai client non autorizzati di connettersi a una LAN tramite porte accessibili per la pubblicità. L'autenticazione 802.1x è un modello client-server. In questo modello, i dispositivi di rete hanno i seguenti ruoli specifici:

Client o supplicant: un client o un supplicant è un dispositivo di rete che richiede l'accesso alla LAN. Il client è connesso a un autenticatore.

Autenticatore: un autenticatore è un dispositivo di rete che fornisce servizi di rete e al quale sono collegate le porte supplicant. Sono supportati i seguenti metodi di autenticazione:

Basato su 802.1x: supportato in tutte le modalità di autenticazione. Nell'autenticazione basata su 802.1x, l'autenticatore estrae i messaggi EAP (Extensible Authentication Protocol) dai messaggi 802.1x o dai pacchetti EAPoL (EAP over LAN) e li passa al server di autenticazione, utilizzando il protocollo RADIUS.

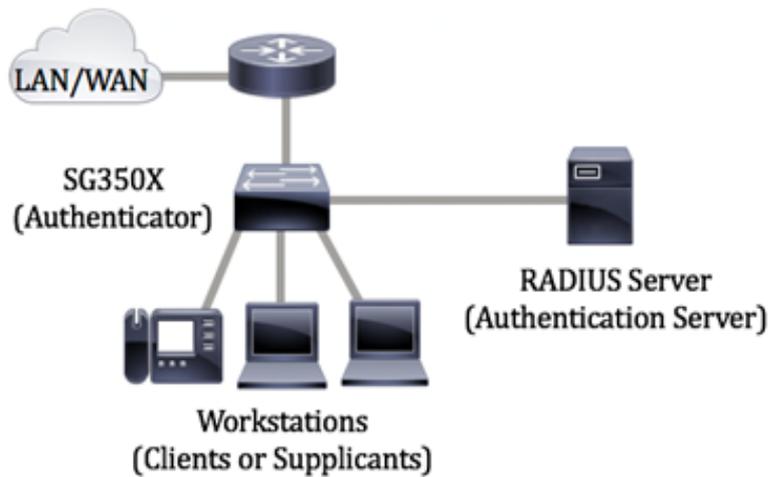
Basato su MAC: supportato in tutte le modalità di autenticazione. Con il Media Access Control (MAC), l'autenticatore esegue la parte client EAP del software per conto dei client che richiedono l'accesso alla rete.

Basato su Web - Supportato solo in modalità multiseSSIONE. Con l'autenticazione basata sul Web, l'autenticatore stesso esegue la parte client EAP del software per conto dei client che richiedono l'accesso alla rete.

Server di autenticazione: un server di autenticazione esegue l'autenticazione effettiva del client. Il server di autenticazione per il dispositivo è un server di autenticazione RADIUS con estensioni EAP.

Nota: Un dispositivo di rete può essere un client o un supplicant, un autenticatore o entrambi per porta.

L'immagine seguente mostra una rete che ha configurato i dispositivi in base ai ruoli specifici. Nell'esempio viene usato uno switch SG350X.



Linee guida per la configurazione di 802.1x:

Creare una VLAN (Virtual Access Network). Per creare le VLAN con l'utility basata sul Web dello switch, fare clic [qui](#). Per le istruzioni basate sulla CLI, fare clic [qui](#).

Configurare le impostazioni della porta sulla VLAN sullo switch. Per eseguire la configurazione utilizzando l'utility basata sul Web, fare clic [qui](#). Per utilizzare la CLI, fare clic [qui](#).

Configurare le proprietà 802.1x sullo switch. Per abilitare l'autenticazione basata sulla porta 802.1x, è necessario abilitare globalmente lo switch 802.1x. Per istruzioni, fare clic [qui](#).

(Facoltativo) Configurare l'intervallo di tempo sullo switch. per informazioni su come configurare le impostazioni dell'intervallo di tempo sullo switch, fare clic [qui](#).

Configurare l'autenticazione della porta 802.1x. In questo documento viene spiegato come configurare le impostazioni di autenticazione della porta 802.1x sullo switch.

per informazioni su come configurare l'autenticazione basata su mac su uno switch, fare clic [qui](#).

Dispositivi interessati

Serie Sx300

Serie Sx350

Serie SG350X

Serie Sx500

Serie Sx550X

Versione del software

1.4.7.06 — Sx300, Sx500

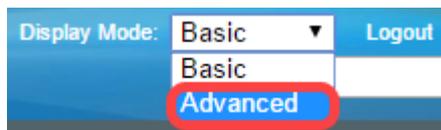
2.2.8.04 - Sx350, SG350X, Sx550X

Configurazione delle impostazioni di autenticazione della porta 802.1x su uno switch

Configura impostazioni client RADIUS

Passaggio 1. Accedere all'utility basata sul Web dello switch, quindi selezionare **Advanced** (Avanzate) dall'elenco a discesa Display Mode (Modalità di visualizzazione).

Nota: Le opzioni di menu disponibili possono variare a seconda del modello di dispositivo. Nell'esempio viene usato SG550X-24.



Passaggio 2. Passare a **Sicurezza > Client RADIUS**.



Passaggio 3. Scorrere fino alla sezione *Tabella RADIUS* e fare clic su **Aggiungi...** per aggiungere un server RADIUS.

Retries: 3 (Range: 1 - 15, Default: 3)

Timeout for Reply: 3 sec (Range: 1 - 30, Default: 3)

Dead Time: 0 min (Range: 0 - 2000, Default: 0)

Key String: Encrypted Plaintext (0/128 characters used)

Source IPv4 Interface: Auto

Source IPv6 Interface: Auto

Apply Cancel

RADIUS Table

Server	Priority	Key String (Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
0 results found.								

Add... Edit... Delete

An * indicates that the parameter is using the default global value.

Display Sensitive Data as Plaintext

Passaggio 4. Selezionare se specificare il server RADIUS in base all'indirizzo IP o al nome nel campo *Definizione server*. Selezionare la versione dell'indirizzo IP del server RADIUS nel campo *IP Version* (Versione IP).

Nota: In questo esempio verrà utilizzato **By IP address** e **Version 4**.

Add RADIUS Server - Google Chrome

Not secure | https://192.168.1.125/cs30a6baef/mts/mgmtauthen/security_authen_radius_a_jq.htm

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name:

Priority: (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) (0/128 characters used)

Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Passaggio 5. Immettere nel server RADIUS l'indirizzo IP o il nome.

Nota: Nel campo *Indirizzo IP/Nome server* verrà immesso l'indirizzo IP **192.168.1.146**.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) (0/128 characters used)

Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Passaggio 6. Immettere la priorità del server. La priorità determina l'ordine in cui il dispositivo tenta di contattare i server per autenticare un utente. Il dispositivo viene avviato con il server RADIUS con la priorità più alta. 0 è la priorità più alta.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) (0/128 characters used)

Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Passaggio 7. Immettere la stringa di chiave utilizzata per autenticare e crittografare la comunicazione tra il dispositivo e il server RADIUS. Questa chiave deve corrispondere alla chiave configurata nel server RADIUS. Può essere immesso in formato **crittografato** o **non crittografato**. Se si seleziona **Utilizza predefinito**, il dispositivo tenta di eseguire l'autenticazione al server RADIUS utilizzando la stringa di chiave predefinita.

Nota: Verrà utilizzato il **testo definito dall'utente (testo normale)** e verrà immesso l'**esempio** chiave.

per informazioni su come configurare le impostazioni del server RADIUS sullo switch, fare clic [qui](#).

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 characters used)

Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Passaggio 8. Nel campo *Timeout per risposta*, selezionare **Usa predefinito** o **Definito dall'utente**. Se è stata selezionata l'opzione **Definito dall'utente**, immettere il numero di secondi che il dispositivo attende dal server RADIUS prima di riprovare a eseguire la query oppure passare al server successivo se è stato raggiunto il numero massimo di tentativi. Se è selezionata l'opzione **Use Default**, il dispositivo utilizza il valore di timeout predefinito.

Nota: In questo esempio è stata selezionata l'opzione **Usa predefinito**.

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 characters used)

Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Apply Close

Passaggio 9. Immettere il numero di porta UDP della porta server RADIUS per la richiesta di autenticazione nel campo *Porta di autenticazione*. Immettere il numero della porta UDP della porta del server RADIUS per le richieste di accounting nel campo *Porta di accounting*.

Nota: In questo esempio verrà utilizzato il valore predefinito sia per la porta di autenticazione che per la porta di accounting.

Add RADIUS Server - Google Chrome
 Not secure | https://192.168.1.125/cs30a6baef/mts/mgmtauthen/security_authen_radius_a_jq.htm

IP Version: Version 6 Version 4
 IPv6 Address Type: Link Local Global
 Link Local Interface: VLAN 1
 Server IP Address/Name: 192.168.1.146
 Priority: 0 (Range: 0 - 65535)
 Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 characters used)
 Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)
 Authentication Port: 1 1812 (Range: 0 - 65535, Default: 1812)
 Accounting Port: 2 1813 (Range: 0 - 65535, Default: 1813)
 Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)
 Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)
 Usage Type: Login 802.1x All

Passaggio 10. Se per il campo *Tentativi* è selezionato **Definito da utente**, immettere il numero di richieste inviate al server RADIUS prima che si verifichi un errore. Se è stata selezionata l'opzione **Usa predefinito**, il dispositivo utilizza il valore predefinito per il numero di tentativi.

Se è selezionato **Definito dall'utente** per *Tempo inattivo*, immettere il numero di minuti che devono trascorrere prima che un server RADIUS non rispondente venga ignorato per le richieste di servizio. Se è stata selezionata l'opzione **Use Default**, il dispositivo utilizza il valore predefinito per il tempo morto. Se sono stati immessi 0 minuti, non vi sono tempi morti.

Nota: In questo esempio verrà selezionato **Usa predefinito** per entrambi i campi.

Add RADIUS Server - Google Chrome
 Not secure | https://192.168.1.125/cs30a6baef/mts/mgmtauthen/security_authen_radius_a_jq.htm

IP Version: Version 6 Version 4
 IPv6 Address Type: Link Local Global
 Link Local Interface: VLAN 1
 Server IP Address/Name: 192.168.1.146
 Priority: 0 (Range: 0 - 65535)
 Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 characters used)
 Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)
 Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)
 Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)
 Retries: 1 Use Default User Defined Default (Range: 1 - 15, Default: 3)
 Dead Time: 2 Use Default User Defined Default min (Range: 0 - 2000, Default: 0)
 Usage Type: Login 802.1x All

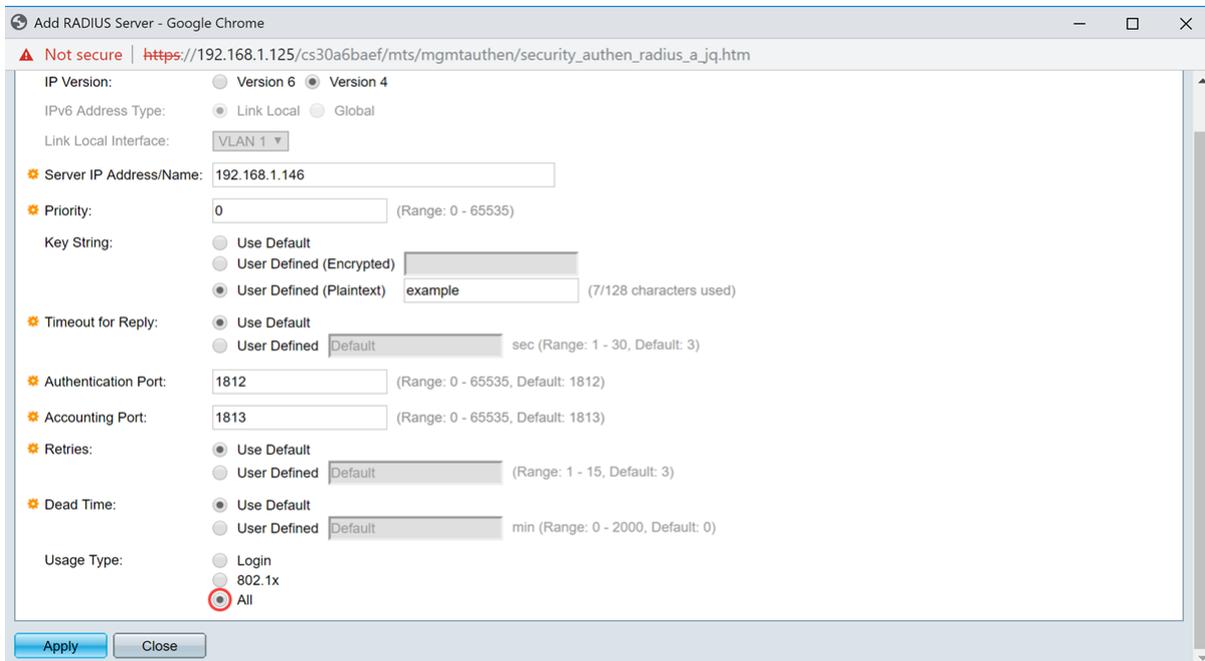
Passaggio 11. Nel campo *Usage Type*, immettere il tipo di autenticazione del server RADIUS. Le opzioni sono:

Accesso - Il server RADIUS viene utilizzato per autenticare gli utenti che richiedono di

amministrare il dispositivo.

802.1x - Il server RADIUS viene utilizzato per l'autenticazione 802.1x.

All - Il server RADIUS viene utilizzato per l'autenticazione degli utenti che richiedono l'amministrazione del dispositivo e per l'autenticazione 802.1x.



IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 characters used)

Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

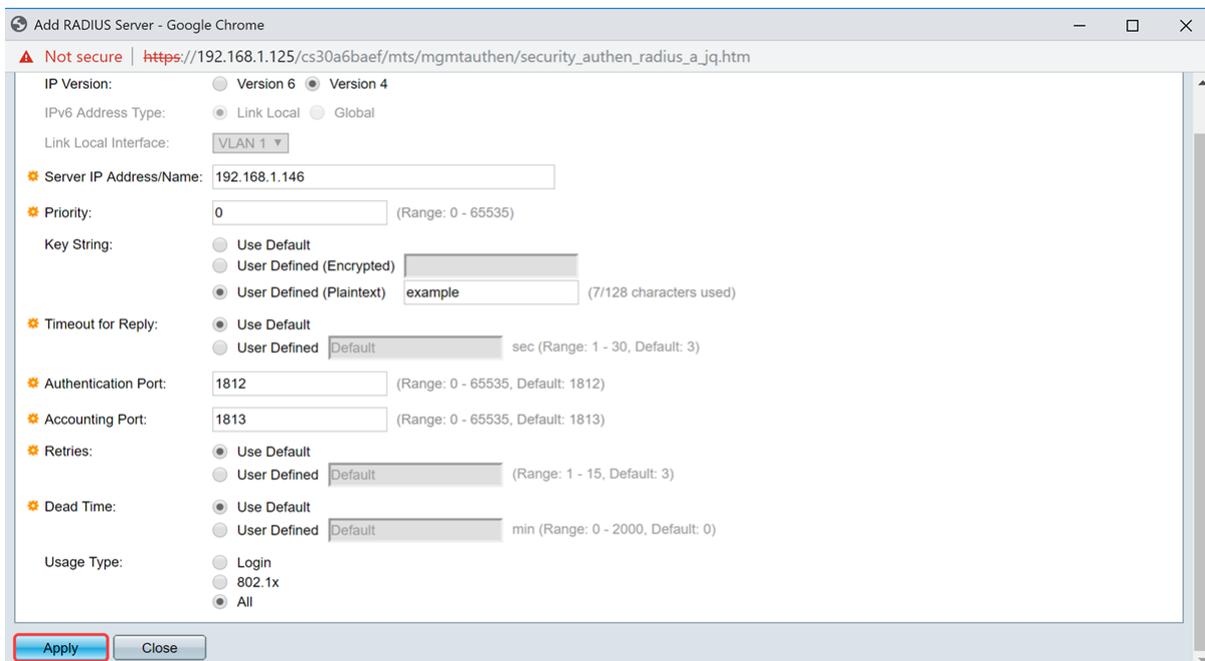
Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

Apply Close

Passaggio 12. Fare clic su **Applica**.



IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

Priority: 0 (Range: 0 - 65535)

Key String: Use Default User Defined (Encrypted) User Defined (Plaintext) example (7/128 characters used)

Timeout for Reply: Use Default User Defined Default sec (Range: 1 - 30, Default: 3)

Authentication Port: 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 1813 (Range: 0 - 65535, Default: 1813)

Retries: Use Default User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: Use Default User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type: Login 802.1x All

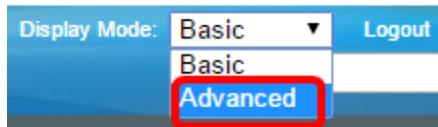
Apply Close

Configurazione delle impostazioni di autenticazione della porta 802.1x

Passaggio 1. Accedere all'utility basata sul Web dello switch, quindi selezionare **Advanced** (Avanzate) dall'elenco a discesa Display Mode (Modalità di visualizzazione).

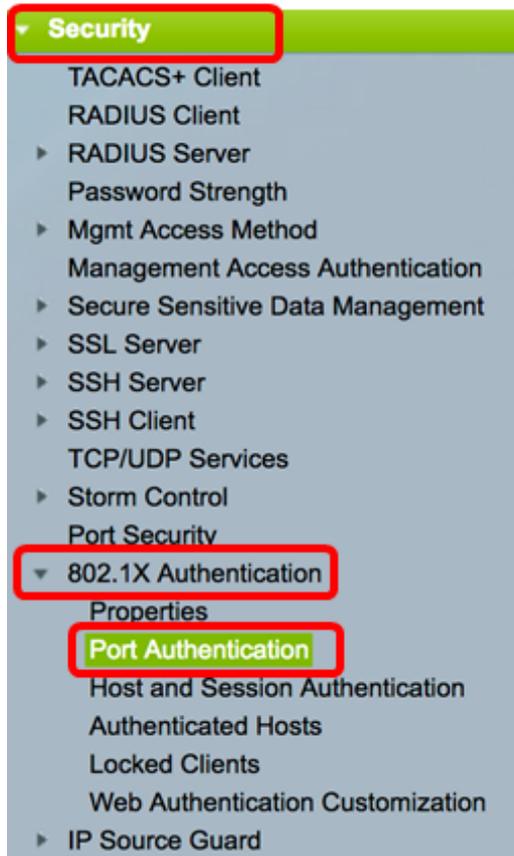
Nota: Le opzioni di menu disponibili possono variare a seconda del modello di dispositivo.

Nell'esempio viene usato SG350X-48MP.



Nota: Se si dispone di uno switch serie Sx300 o Sx500, andare al [punto 2](#).

Passaggio 2. Scegliere **Sicurezza > Autenticazione 802.1X > Autenticazione porta**.

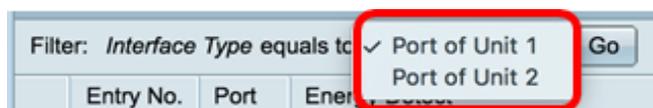


Passaggio 3. Scegliere un'interfaccia dall'elenco a discesa *Tipo interfaccia*.

Porta: dall'elenco a discesa *Interface Type* (Tipo di interfaccia), selezionare **Port** (Porta) se si desidera selezionare solo una porta.

LAG — dall'elenco a discesa *Interface Type* (Tipo di interfaccia), selezionare il LAG da configurare. Questo influisce sul gruppo di porte definite nella configurazione LAG.

Nota: Nell'esempio, viene scelto Port of Unit 1 (Porta dell'unità 1).



Nota: Se si dispone di uno switch non impilabile come uno switch serie Sx300, andare al [passo 5](#).

Passaggio 4. Fare clic su **Go** per visualizzare un elenco delle porte o dei LAG sull'interfaccia.

Port Authentication

Port Authentication Table

Filter: *Interface Type* equals to Port of Unit 1

Go

Passaggio 5. Fare clic sulla porta che si desidera configurare.

Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access	802.1x Based Authentication	MAC Based Authentication	Web Based Authentication
1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
4	GE4	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled
6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled

Nota: Nell'esempio, viene scelto GE4.

Passaggio 6. Scorrere la pagina verso il basso e fare clic su **Modifica**.

46	GE46	Port Down	Force Authorized	Disabled	Disabled
47	GE47	Port Down	Force Authorized	Disabled	Disabled
48	GE48	Port Down	Force Authorized	Disabled	Disabled
49	XG1	Authorized	Force Authorized	Disabled	Disabled
50	XG2	Port Down	Force Authorized	Disabled	Disabled
51	XG3	Port Down	Force Authorized	Disabled	Disabled
52	XG4	Authorized	Force Authorized	Disabled	Disabled

Copy Settings... Edit...

Passaggio 7. (Facoltativo) Se si desidera modificare un'altra interfaccia, scegliere dagli elenchi a discesa Unità e Porta.

Interface:

Unit 1 Port GE4

Current Port Control:

Authorized

Nota: Nell'esempio viene scelta la porta GE4 dell'unità 1.

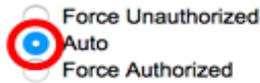
Passaggio 8. Fare clic sul pulsante di opzione corrispondente al controllo della porta desiderato nell'area di controllo della porta amministrativa. Le opzioni sono:

Force Unauthorized - Nega l'accesso all'interfaccia attivando lo stato non autorizzato sulla porta. La porta eliminerà il traffico.

Auto: la porta si sposta tra uno stato autorizzato e uno non autorizzato in base all'autenticazione del richiedente.

Force Authorized: autorizza la porta senza autenticazione. La porta inoltrerà il traffico.

Administrative Port Control:



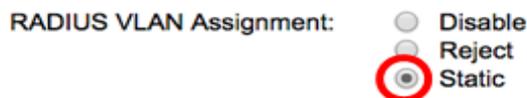
Nota: nell'esempio, viene scelto Auto.

Passaggio 9. Per configurare l'assegnazione dinamica della VLAN sulla porta selezionata, fare clic sul pulsante di opzione Assegnazione VLAN RADIUS. Le opzioni sono:

Disabilita: la funzionalità non è abilitata.

Rifiuta: se il server RADIUS autorizza il richiedente ma non fornisce una VLAN, il richiedente viene rifiutato.

Statico: se il server RADIUS autorizza il richiedente ma non fornisce una VLAN, il richiedente viene accettato.



Nota: Nell'esempio, viene scelto Static.

Passaggio 10. Selezionare **Enable** nella casella di controllo VLAN guest per abilitare la VLAN guest per le porte non autorizzate. Con la VLAN guest, la porta non autorizzata si unisce automaticamente alla VLAN scelta nell'area dell'ID della VLAN guest nelle proprietà 802.1.

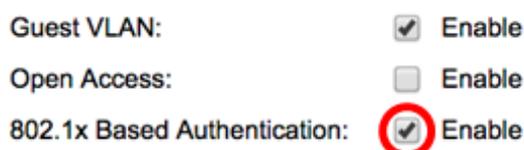


Passaggio 11. (Facoltativo) Selezionare la casella di controllo **Abilita** accesso aperto per abilitare l'accesso aperto. Open Access consente di comprendere i problemi di configurazione degli host che si connettono alla rete, di monitorare le situazioni critiche e di risolverli.

Nota: Quando Open Access è abilitato su un'interfaccia, lo switch considera tutti gli errori ricevuti da un server RADIUS come operazioni riuscite e consente l'accesso alla rete per le stazioni connesse alle interfacce, indipendentemente dai risultati dell'autenticazione. In questo esempio Open Access è disattivato.



Passaggio 12. Selezionare la casella di controllo **Abilita** autenticazione basata su 802.1x per abilitare l'autenticazione 802.1X sulla porta.



Passaggio 13. Selezionare la casella di controllo **Abilita** autenticazione basata su MAC per abilitare l'autenticazione della porta in base all'indirizzo MAC supplicant. Sulla porta è possibile usare solo otto autenticazioni basate su MAC.

Nota: Affinché l'autenticazione MAC abbia esito positivo, il nome utente e la password del server RADIUS devono essere l'indirizzo MAC del richiedente. L'indirizzo MAC deve essere in lettere minuscole e immesso senza . o - separatori (ad esempio 0020aa00bbcc).

802.1x Based Authentication: Enable
MAC Based Authentication: Enable

Nota: In questo esempio, l'autenticazione basata su MAC è disabilitata.

Passaggio 14. Selezionare la casella di controllo **Abilita** autenticazione basata sul Web per abilitare l'autenticazione basata sul Web sullo switch. In questo esempio, l'autenticazione basata sul Web è disabilitata.

802.1x Based Authentication: Enable
MAC Based Authentication: Enable
Web Based Authentication: Enable

Nota: In questo esempio, l'autenticazione basata sul Web è disabilitata.

Passaggio 15. (Facoltativo) Selezionare la casella di controllo **Abilita** riautenticazione periodica per forzare la riautenticazione della porta dopo un determinato periodo di tempo. Questa ora è definita nel campo *Periodo di riautenticazione*.

Web Based Authentication: Enable
Periodic Reauthentication: Enable

Nota: In questo esempio, è attivata la riautenticazione punto.

Passaggio 16. (Facoltativo) Immettere un valore nel campo *Periodo riautenticazione*. Questo valore rappresenta il numero di secondi prima che l'interfaccia autentichi nuovamente la porta. Il valore predefinito è 3600 secondi e l'intervallo è compreso tra 300 e 4294967295 secondi.

Periodic Reauthentication: Enable
Reauthentication Period: sec

Nota: Nell'esempio, è configurato 6000 secondi.

Passaggio 17. (Facoltativo) Selezionare la casella di controllo **Abilita** riautenticazione immediata per forzare una riautenticazione immediata della porta. In questo esempio, la riautenticazione immediata è disabilitata.

Periodic Reauthentication: Enable

Reauthentication Period: sec

Reauthenticate Now:

Authenticator State: Force Authorized

Nell'area Stato autenticatore viene visualizzato lo stato di autorizzazione della porta.

Passaggio 18. (Facoltativo) Selezionare la casella di controllo **Abilita** intervallo di tempo per abilitare un limite di tempo per l'autorizzazione della porta.

Time Range: Enable

Time Range Name: [Edit](#)

Nota: Nell'esempio, l'opzione Intervallo di tempo è abilitata. Se si preferisce saltare questa funzione, andare al [passo 20](#).

Passaggio 19. (Facoltativo) Dall'elenco a discesa Nome intervallo di tempo, scegliere un intervallo di tempo da utilizzare.

Time Range: Enable

Time Range Name: Dayshift NightShift [Edit](#)

Maximum WBA Login Attempts:

Nota: Nell'esempio, viene scelto Dayshift.

Passaggio 20. Nell'area Numero massimo di tentativi di login WBA, fare clic su Infinito per nessun limite o su Definito dall'utente per impostare un limite. Se si sceglie Definito dall'utente, immettere il numero massimo di tentativi di accesso consentiti per l'autenticazione basata sul Web.

Maximum WBA Login Attempts: Infinite User Defined

Nota: Nell'esempio viene scelto Infinito.

Passaggio 21. Nell'area Periodo massimo silenzio WBA, fare clic su Infinito per nessun limite o su Definito da utente per impostare un limite. Se si sceglie Definito dall'utente, immettere la durata massima del periodo di inattività per l'autenticazione basata sul Web consentita per l'interfaccia.

Maximum WBA Silence Period: Infinite User Defined sec

Nota: Nell'esempio viene scelto Infinito.

Passaggio 2. Nell'area Numero massimo host, fare clic su Infinito per nessun limite o su Definito dall'utente per impostare un limite. Se si sceglie Definito dall'utente, immettere il numero massimo di host autorizzati consentiti sull'interfaccia.

Max Hosts:

Infinite
 User Defined

Nota: Impostare questo valore su 1 per simulare la modalità host singolo per l'autenticazione basata sul Web in modalità multisessione. Nell'esempio viene scelto Infinito.

Passaggio 23. Nel campo *Quiet Period* (Periodo di inattività), immettere il periodo di tempo durante il quale lo switch rimane in stato di inattività dopo uno scambio di autenticazione non riuscito. Quando lo switch è in modalità non interattiva, non è in ascolto di nuove richieste di autenticazione da parte del client. Il valore predefinito è 60 secondi e l'intervallo è compreso tra 1 e 65535 secondi.

Quiet Period:

Nota: In questo esempio, il periodo di attesa è impostato su 120 secondi.

Passaggio 24. Nel campo *Nuovo invio di EAP*, immettere il tempo di attesa del commutatore per un messaggio di risposta dal supplicant prima di inviare nuovamente una richiesta. Il valore predefinito è 30 secondi e l'intervallo è compreso tra 1 e 65535 secondi.

Quiet Period:
Resending EAP:

Nota: In questo esempio, il valore EAP per il rinvio è impostato su 60 secondi.

Passaggio 25. Nel campo *Numero massimo di richieste EAP*, immettere il numero massimo di richieste EAP che possono essere inviate. EAP è un metodo di autenticazione utilizzato in 802.1X che fornisce lo scambio di informazioni di autenticazione tra lo switch e il client. In questo caso, le richieste EAP vengono inviate al client per l'autenticazione. Il client deve quindi rispondere e corrispondere alle informazioni di autenticazione. Se il client non risponde, viene impostata un'altra richiesta EAP in base al valore EAP di rinvio e il processo di autenticazione viene riavviato. Il valore predefinito è 2 e l'intervallo è compreso tra 1 e 10.

Quiet Period:
Resending EAP:
Max EAP Requests:

Nota: Nell'esempio viene utilizzato il valore predefinito 2.

Passaggio 26. Nel campo *Timeout supplicant*, immettere l'intervallo di tempo che deve trascorrere prima che le richieste EAP vengano inviate al supplicant. Il valore predefinito è 30 secondi e l'intervallo è compreso tra 1 e 65535 secondi.

Max EAP Requests: (Rar)
Supplicant Timeout: sec

Nota: Nell'esempio, il timeout del supplicant è impostato su 60 secondi.

Passaggio 27. Nel campo *Server Timeout* (Timeout server), immettere il tempo che deve trascorrere prima che lo switch invii nuovamente una richiesta al server RADIUS. Il valore predefinito è 30 secondi e l'intervallo è compreso tra 1 e 65535 secondi.

☛ Max EAP Requests:	<input type="text" value="2"/>	(Range: 1 - 10, Default: 2)
☛ Supplicant Timeout:	<input type="text" value="60"/>	sec (Range: 1 - 65535, Default: 30)
☛ Server Timeout:	<input type="text" value="60"/>	sec (Range: 1 - 65535, Default: 30)

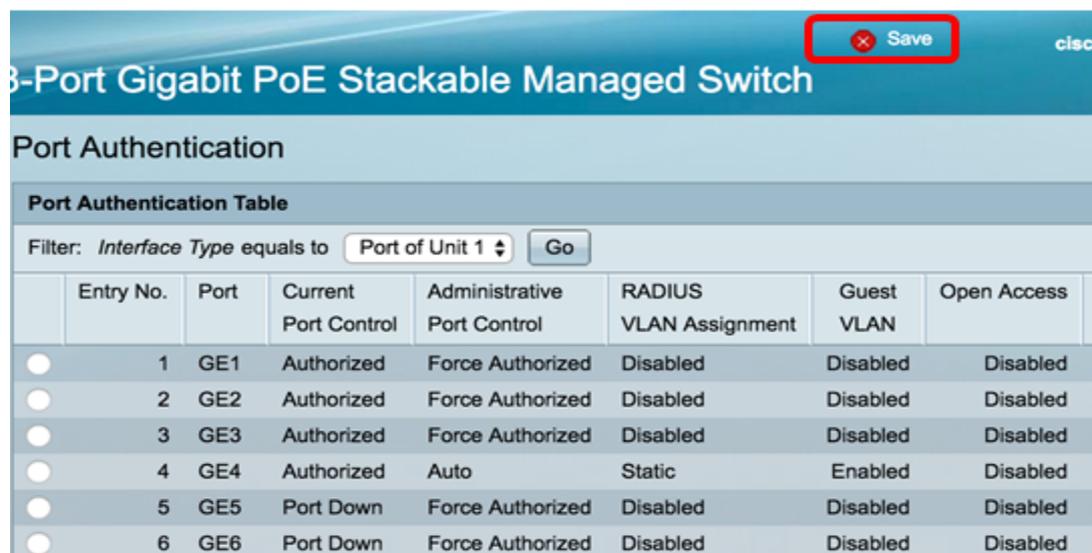
Nota: In questo esempio, il timeout del server è impostato su 60 secondi.

Passaggio 28. Fare clic su **Apply** (Applica), quindi su **Close** (Chiudi).

Interface:	Unit <input type="text" value="1"/>	Port <input type="text" value="GE4"/>
Current Port Control:	Unauthorized	
Administrative Port Control:	<input type="radio"/> Force Unauthorized <input checked="" type="radio"/> Auto <input type="radio"/> Force Authorized	
RADIUS VLAN Assignment:	<input type="radio"/> Disable <input type="radio"/> Reject <input checked="" type="radio"/> Static	
Guest VLAN:	<input checked="" type="checkbox"/> Enable	
Open Access:	<input type="checkbox"/> Enable	
802.1x Based Authentication:	<input checked="" type="checkbox"/> Enable	
MAC Based Authentication:	<input type="checkbox"/> Enable	
Web Based Authentication:	<input type="checkbox"/> Enable	
Periodic Reauthentication:	<input checked="" type="checkbox"/> Enable	
☛ Reauthentication Period:	<input type="text" value="6000"/>	sec (Range: 300 - 4294967295, Default: 3600)
Reauthenticate Now:	<input type="checkbox"/>	
Authenticator State:	Connecting	
Time Range:	<input type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="Dayshift"/> Edit	
☛ Maximum WBA Login Attempts:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text" value=""/> (Range: 3 - 10)	
☛ Maximum WBA Silence Period:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text" value=""/> sec (Range: 60 - 65535)	
☛ Max Hosts:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text" value=""/> sec (Range: 1 - 4294967295)	
☛ Quiet Period:	<input type="text" value="120"/>	sec (Range: 10 - 65535, Default: 60)
☛ Resending EAP:	<input type="text" value="60"/>	sec (Range: 30 - 65535, Default: 30)
☛ Max EAP Requests:	<input type="text" value="2"/>	(Range: 1 - 10, Default: 2)
☛ Supplicant Timeout:	<input type="text" value="60"/>	sec (Range: 1 - 65535, Default: 30)
☛ Server Timeout:	<input type="text" value="60"/>	sec (Range: 1 - 65535, Default: 30)

Passaggio 29. (Facoltativo) Fare clic su **Salva** per salvare le impostazioni nel file della

configurazione di avvio.



3-Port Gigabit PoE Stackable Managed Switch

Port Authentication

Port Authentication Table

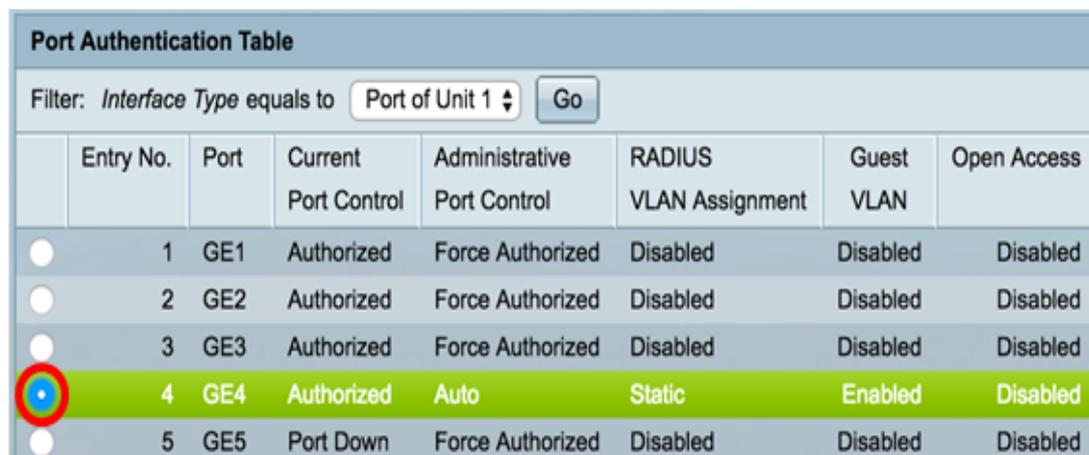
Filter: Interface Type equals to Port of Unit 1 Go

Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access	
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled

A questo punto, le impostazioni di autenticazione della porta 802.1x sullo switch sono state configurate correttamente.

Applicazione delle impostazioni di configurazione interfaccia a più interfacce

Passaggio 1. Fare clic sul pulsante di opzione dell'interfaccia a cui si desidera applicare la configurazione di autenticazione a più interfacce.



Port Authentication Table

Filter: Interface Type equals to Port of Unit 1 Go

Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access	
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input checked="" type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled

Nota: Nell'esempio, viene scelto GE4.

Passaggio 2. Scorrere verso il basso e fare clic su **Copia impostazioni**.

<input type="radio"/>	43	GE43	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	44	GE44	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	45	GE45	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	47	GE47	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	48	GE48	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled

Copy Settings... Edit...

Passaggio 3. Nel campo *a*, immettere l'intervallo di interfacce a cui applicare la configurazione dell'interfaccia scelta. È possibile utilizzare i numeri di interfaccia o il nome delle interfacce come input. È possibile immettere le interfacce separate da una virgola (ad esempio 1, 3, 5 o GE1, GE3, GE5) oppure immettere un intervallo di interfacce (ad esempio 1-5 o GE1-GE5).

Copy configuration from entry 4 (GE4)

to: (Example: 1,3,5-10 or: GE1,GE3-XG4)

Nota: Nell'esempio, le impostazioni di configurazione verranno applicate alle porte da 47 a 48.

Passaggio 4. Fare clic su **Apply (Applica)**, quindi su **Close (Chiudi)**.

Copy configuration from entry 4 (GE4)

to: (Example: 1,3,5-10 or: GE1,GE3-XG4)

Apply Close

L'immagine seguente mostra le modifiche apportate dopo la configurazione.

Port Authentication Table

Filter: *Interface Type* equals to

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled

<input type="radio"/>	45	GE45	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	47	GE47	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	48	GE48	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled	Disabled

A questo punto, le impostazioni di autenticazione 802.1x di una porta dovrebbero essere copiate correttamente e applicate ad altre porte dello switch.