

Konfigurieren der 802.1X-Komponenteneinstellungen auf einem WAP125 oder WAP581

Ziel

Eine Komponente ist eine der drei Rollen im 802.1X IEEE-Standard. 802.1X wurde entwickelt, um die Sicherheit in Layer 2 des OSI-Modells zu gewährleisten. Es besteht aus den folgenden Komponenten: Supplicant, Authenticator und Authentication Server. Ein Supplicant ist der Client oder die Software, der bzw. die eine Verbindung zu einem Netzwerk herstellt, um auf dessen Ressourcen zugreifen zu können. Sie muss Anmeldeinformationen oder Zertifikate bereitstellen, um eine IP-Adresse zu erhalten und Teil dieses speziellen Netzwerks zu sein. Ein Supplicant kann erst nach Authentifizierung auf die Netzwerkressourcen zugreifen.

In diesem Artikel wird beschrieben, wie der WAP125 oder WAP581 Access Point als 802.1X-Komponente konfiguriert wird.

Hinweis: Um zu erfahren, wie Sie die 802.1X-Anmeldeinformationen für Komponenten auf Ihrem Switch konfigurieren, klicken Sie [hier](#).

Anwendbare Geräte

- WAP125
- WAP581

Softwareversion

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

Konfigurieren der 802.1X-Komponente

Konfigurieren der Komponentenanmeldedaten

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm Ihres WAP an. Der Standard-Benutzername und das Kennwort lautet cisco/cisco.



Wireless Access Point

cisco

.....|

English

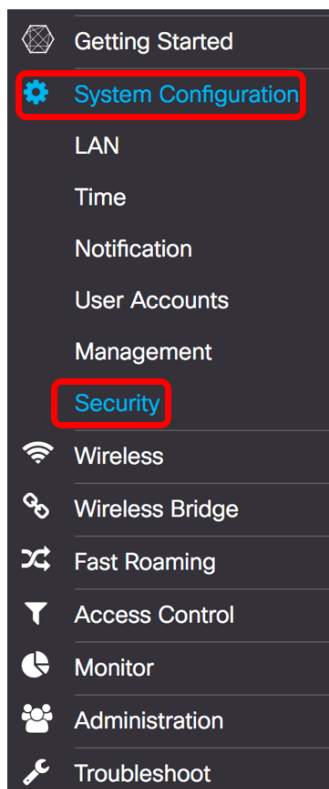
Login

©2017 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Hinweis: Wenn Sie das Kennwort bereits geändert oder ein neues Konto erstellt haben, geben Sie stattdessen Ihre neuen Anmeldeinformationen ein.

Schritt 2: Wählen Sie **Systemkonfiguration > Sicherheit** aus.



Schritt 3: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um den Verwaltungsmodus zu aktivieren. Dadurch kann der WAP als Komponente für den Authentifizierer fungieren.

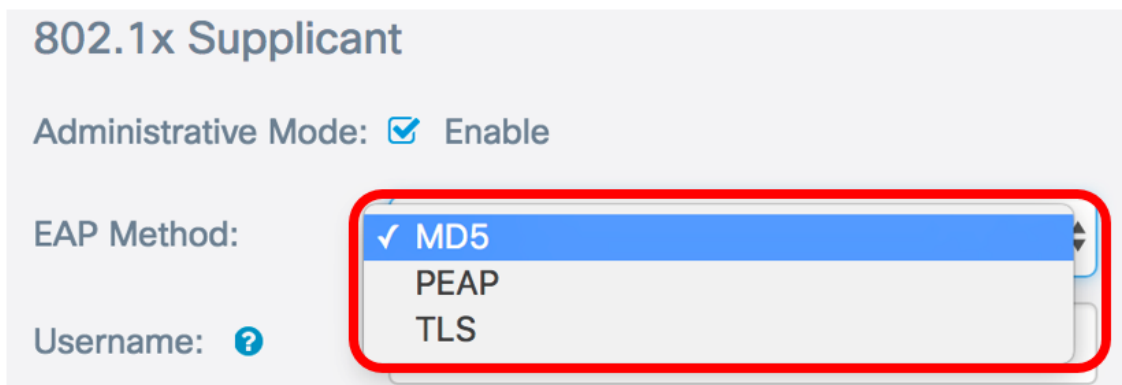
802.1x Supplicant

Administrative Mode: Enable

Schritt 4: Wählen Sie den entsprechenden Typ der Extensible Authentication Protocol (EAP)-Methode aus, der zur Verschlüsselung von Benutzernamen und Kennwörtern aus der Dropdown-Liste *EAP Method* verwendet wird. Folgende Optionen stehen zur Verfügung:

- MD5 - Verwendet eine 128-Bit-Verschlüsselungsmethode. Der MD5-Algorithmus verwendet zur Verschlüsselung von Daten ein öffentliches Kryptosystem.
- PEAP - Protected Extensible Authentication Protocol (PEAP) authentifiziert WLAN-Clients mithilfe von digitalen Zertifikaten, die vom Server ausgegeben werden, indem ein verschlüsselter SSL/TLS-Tunnel zwischen dem Client und dem Authentifizierungsserver erstellt wird.
- TLS - Transport Layer Security (TLS) ist ein Protokoll, das Sicherheit und Datenintegrität für die Kommunikation über das Internet bietet. Es wird sichergestellt, dass keine Manipulationen von Drittanbietern an der ursprünglichen Nachricht auftreten.

Hinweis: In diesem Beispiel wird MD5 verwendet.



802.1x Supplicant

Administrative Mode: Enable

EAP Method:

Username:

Schritt 5: Geben Sie im Feld *Benutzername* einen Benutzernamen ein. Dies ist der Benutzername, der auf dem Authentifizierer konfiguriert wurde und für die Antwort auf den 802.1X-Authentifizierer verwendet wird. Sie kann ein bis 64 Zeichen lang sein und Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen außer doppelten Anführungszeichen enthalten.

Hinweis: In diesem Beispiel wird UserAccess_1 verwendet.

802.1x Supplicant

Administrative Mode: Enable

EAP Method: MD5

Username:

Schritt 6: Geben Sie im Feld *Kennwort* ein Kennwort ein, das dem Benutzernamen zugeordnet ist. Dieses MD5-Kennwort wird zur Reaktion auf den 802.1X-Authentifizierer verwendet. Das Kennwort kann ein bis 64 Zeichen lang sein und kann Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen außer Anführungszeichen enthalten.

802.1x Supplicant

Administrative Mode: Enable

EAP Method: MD5

Username:

Password:

Schritt 7: Klicken Sie auf die Schaltfläche **Speichern**, um die konfigurierten Einstellungen zu speichern.

Security

Save

802.1x Supplicant

Administrative Mode: Enable

EAP Method: MD5

Username:

Password:

Sie sollten jetzt die 802.1X Supplicant-Einstellungen auf dem WAP konfiguriert haben.

Hochladen der Zertifikatsdatei

Schritt 1: Wählen Sie aus der Übertragungsmethode eine Methode aus, die der WAP zum Abrufen des SSL-Zertifikats verwenden wird. Das SSL-Zertifikat ist ein digital signiertes Zertifikat von einer Zertifizierungsstelle, das dem Webbrowser eine sichere Kommunikation mit dem Webserver ermöglicht. Folgende Optionen stehen zur Verfügung:

- HTTP - Das Zertifikat wird über das Hyper Text Transfer Protocol (HTTP) oder den Browser hochgeladen.
- TFTP - Das Zertifikat wird über einen TFTP-Server (Trivial File Transfer Protocol) hochgeladen. Wenn Sie diese Option auswählen, fahren Sie mit [Schritt 3 fort](#). Sie müssen den Dateinamen und die TFTP-Adresse eingeben.

Hinweis: In diesem Beispiel wird HTTP ausgewählt.

Certificate File Upload

Transfer Method: HTTP TFTP

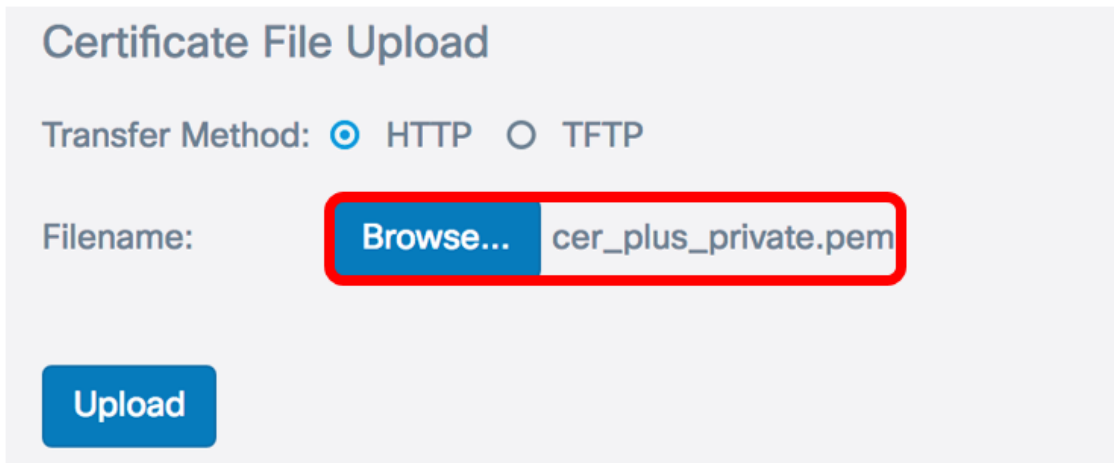
Filename: **Browse...**

Upload

HTTP-Übertragungsmethode

Schritt 2: (Optional) Wenn Sie HTTP ausgewählt haben, klicken Sie auf **Durchsuchen...** und wählen Sie das SSL-Zertifikat aus.

Hinweis: In diesem Beispiel wird cer_plus_private.pem verwendet.



Certificate File Upload

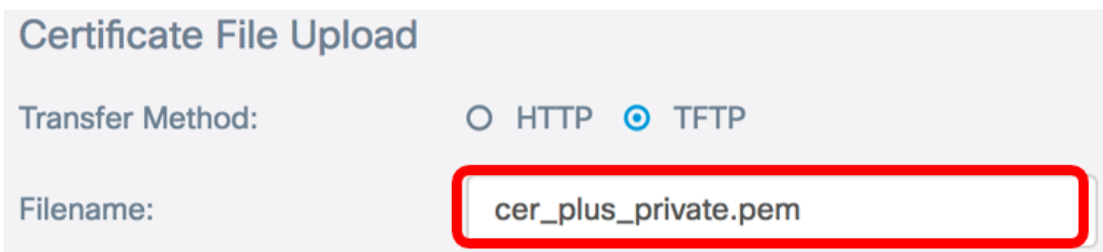
Transfer Method: HTTP TFTP

Filename: cer_plus_private.pem

TFTP-Übertragungsmethode

[Schritt 3](#): Wenn Sie in Schritt 1 TFTP ausgewählt haben, geben Sie den Namen der Datei in das Feld Dateiname ein.

Hinweis: In diesem Beispiel wird cer_plus_private.pem verwendet.



Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

Schritt 4: (Optional) Wenn TFTP als Übertragungsmethode ausgewählt ist, geben Sie die IPv4-Adresse des TFTP-Servers in das Feld *IPv4-Adresse des TFTP-Servers* ein. Dies ist der Pfad, über den der WAP das Zertifikat abrufen.

Hinweis: In diesem Beispiel wird 10.21.52.101 verwendet.



Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

Schritt 5: Klicken Sie auf **Hochladen**.

802.1x Supplicant

Administrative Mode: Enable

EAP Method:

Username:

Password:

Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

Sie sollten jetzt erfolgreich ein Zertifikat auf den WAP hochgeladen haben.