

Konfigurieren der 802.1X-Komponenteneinstellungen auf einem Wireless Access Point

Ziel

Der 802.1X-Standard wurde entwickelt, um die Sicherheit in Layer 2 des OSI-Modells (Open System Interconnection) 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.

Die Konfiguration der 802.1X-Komponenteneinstellungen auf Ihrem Wireless Access Point (WAP) ist hilfreich, um autorisierten Geräten hinter Ihrem WAP den Zugriff auf das Netzwerk und die Ressourcen zu ermöglichen. Gleichzeitig wird dem Netzwerk eine Sicherheitsebene hinzugefügt.

In diesem Artikel erfahren Sie, wie Sie die 802.1X-Komponenteneinstellungen auf Ihrem Wireless Access Point konfigurieren.

Anwendbare Geräte

- WAP100-Serie
- WAP300-Serie
- WAP500-Serie

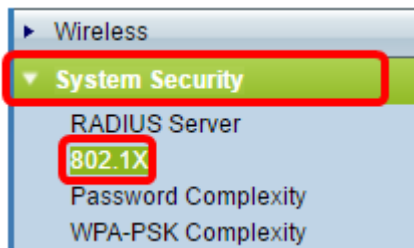
Softwareversion

- 1.0.1.2 - WAP150, WAP361
- 1.0.6.2 - WAP121, WAP321
- 1.0.2.2 - WAP131, WAP351
- 1.2.1.3 - WAP551, WAP561, WAP371
- 1.0.0.17 - WAP571, WAP571E

Konfigurieren der 802.1X-Komponenteneinstellungen auf einem WAP

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Access Points an, und wählen Sie **System Security>802.1X** aus.

Hinweis: Das webbasierte Menü des Dienstprogramms kann je nach Modell des WAP variieren. Die folgenden Bilder stammen aus dem WAP361.



Hinweis: Wenn Sie andere WAP-Modelle verwenden, wählen Sie **System Security > 802.1X Supplicant (Systemsicherheit > 802.1X-Komponente)** aus, und fahren Sie mit [Schritt 3](#) fort.

Schritt 2: Aktivieren Sie das Kontrollkästchen der Anschlussnummer, die konfiguriert werden soll, und klicken Sie dann auf **Bearbeiten**.

The screenshot shows the 'Port Table' configuration page. It contains a table with columns for 'Port No.', 'Enable', and 'Role'. The first row (Port No. 0) is highlighted in green, and its 'Enable' checkbox is checked and circled in red. Below the table is an 'Edit' button, also circled in red.

| Port No. | Enable | Role | |
|----------|-------------------------------------|------------|--------------|
| 0 | <input checked="" type="checkbox"/> | Supplicant | Show Details |
| 1 | <input type="checkbox"/> | Supplicant | Show Details |
| 2 | <input type="checkbox"/> | Supplicant | Show Details |
| 3 | <input type="checkbox"/> | Supplicant | Show Details |
| 4 | <input type="checkbox"/> | Supplicant | Show Details |

Schritt 3: Aktivieren Sie das Kontrollkästchen **Aktivieren**, und wählen Sie dann **Supplicant** aus der Dropdown-Liste aus. Dies ist die Standardoption.

Hinweis: Bei anderen WAP-Modellen aktivieren Sie das Kontrollkästchen **Aktivieren** für den Verwaltungsmodus, und fahren Sie dann mit [Schritt 5](#) fort.

The screenshot shows the 'Port Table' configuration page. The first row (Port No. 0) is highlighted in green. Both the 'Enable' checkbox and the 'Supplicant' role in the dropdown menu are circled in red. The 'Supplicant' option is also highlighted in blue. Below the table is an 'Edit' button.

| Port No. | Enable | Role | |
|----------|-------------------------------------|------------|--------------|
| 0 | <input checked="" type="checkbox"/> | Supplicant | Show Details |
| 1 | <input type="checkbox"/> | Supplicant | Show Details |
| 2 | <input type="checkbox"/> | Supplicant | Show Details |
| 3 | <input type="checkbox"/> | Supplicant | Show Details |
| 4 | <input type="checkbox"/> | Supplicant | Show Details |

Schritt 4: Klicken Sie auf den Link **Details anzeigen**, um die Einstellungen zu bearbeiten.

| Port Table | | | | |
|-------------------------------------|----------|-------------------------------------|--------------|--------------|
| | Port No. | Enable | Role | |
| <input checked="" type="checkbox"/> | 0 | <input checked="" type="checkbox"/> | Supplicant ▼ | Show Details |
| <input type="checkbox"/> | 1 | <input type="checkbox"/> | Supplicant ▼ | Show Details |
| <input type="checkbox"/> | 2 | <input type="checkbox"/> | Supplicant ▼ | Show Details |
| <input type="checkbox"/> | 3 | <input type="checkbox"/> | Supplicant ▼ | Show Details |
| <input type="checkbox"/> | 4 | <input type="checkbox"/> | Supplicant ▼ | Show Details |

Edit

Schritt 5: Wählen Sie in der Dropdown-Liste EAP Method (EAP-Methode) den entsprechenden Typ der Extensible Authentication Protocol (EAP)-Methode aus.

EAP Method: (Range: 1 - 64 Characters)

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Folgende Optionen stehen zur Verfügung:

- MD5 — MD5 ist ein Algorithmus, der verwendet wird, um Daten jeder Größe in 128 Bit zu verschlüsseln. Der MD5-Algorithmus verwendet ein öffentliches Kryptosystem, um Daten zu verschlüsseln.
- PEAP - Protected Extensible Authentication Protocol (PEAP) authentifiziert Wireless Local Area Network (LAN)-Clients mithilfe digitaler Zertifikate, die vom Server ausgegeben werden. Hierzu wird ein verschlüsselter SSL- (Secure Sockets Layer)- oder TLS-Tunnel zwischen dem Client und dem Authentifizierungsserver erstellt.
- TLS - 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.

Schritt 6: Geben Sie Ihren bevorzugten Benutzernamen in das Feld *Benutzername* ein. Dies wird bei der Beantwortung eines 802.1X-Authentifizierers verwendet. Sie kann bis zu 64 Zeichen lang sein und Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen außer doppelten Anführungszeichen enthalten.

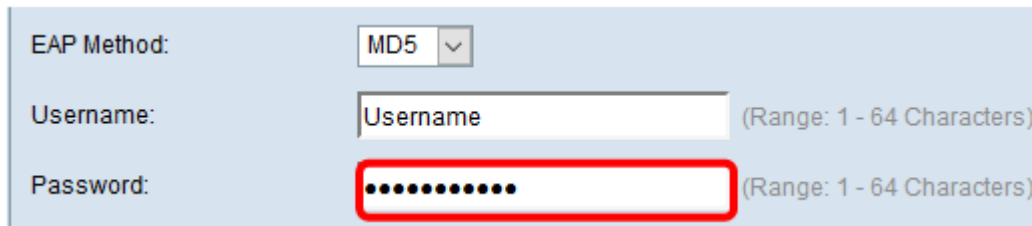
EAP Method:

Username: (Range: 1 - 64 Characters)

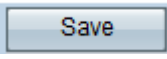
Password: (Range: 1 - 64 Characters)

Schritt 7: Geben Sie Ihr bevorzugtes Kennwort in das Feld *Kennwort* ein. Dieses MD5-

Kennwort wird bei der Beantwortung eines 802.1X-Authentifizierers verwendet. Das Kennwort kann bis zu 64 Zeichen lang sein und Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen außer Anführungszeichen enthalten.



The screenshot shows a configuration form for EAP. It includes a dropdown menu for 'EAP Method' set to 'MD5', a text input field for 'Username' with a '(Range: 1 - 64 Characters)' note, and a password input field with masked characters and a '(Range: 1 - 64 Characters)' note. The password field is highlighted with a red rectangle.

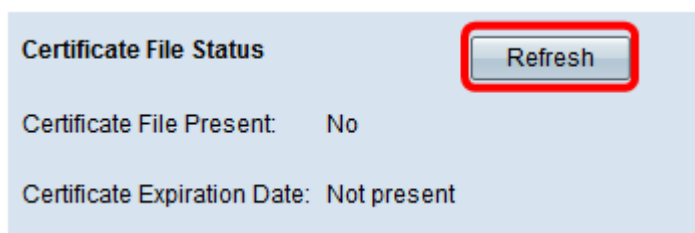
Schritt 8: Klicken Sie auf die  Schaltfläche.

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

Zertifikatsdateieinstellungen anzeigen

Im Bereich Status der Zertifikatsdatei wird angezeigt, ob die Zertifikatsdatei vorhanden ist oder nicht. Das SSL-Zertifikat ist ein digital signiertes Zertifikat von einer Zertifizierungsstelle, das dem Webbrowser eine sichere Kommunikation mit dem Webserver ermöglicht.

Schritt 1: Um den aktuellen Status der Zertifikatsdatei anzuzeigen, klicken Sie auf **Aktualisieren**.



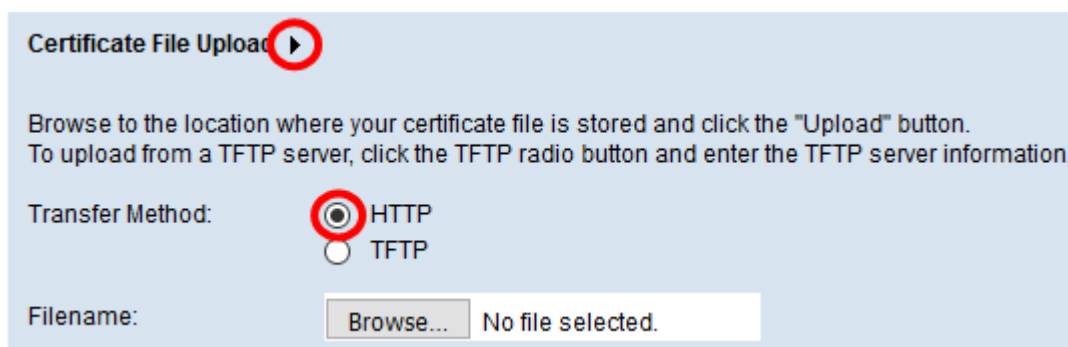
The screenshot shows the 'Certificate File Status' section. It features a 'Refresh' button highlighted with a red rectangle. Below the button, the status is shown as 'Certificate File Present: No' and 'Certificate Expiration Date: Not present'.

Der Bereich Status der Zertifikatsdatei verfügt über folgende Felder:

- Certificate File Present (Zertifikatsdatei vorhanden): Zeigt an, ob die Zertifikatsdatei vorhanden ist oder nicht.
- Ablaufdatum des Zertifikats - Zeigt das Ablaufdatum der aktuellen Zertifikatsdatei an.

Hochladen einer Zertifikatsdatei

Schritt 1: Klicken Sie auf den Pfeil neben "Zertifikatsdatei hochladen", und wählen Sie dann das gewünschte Optionsfeld aus der Übertragungsmethode aus.



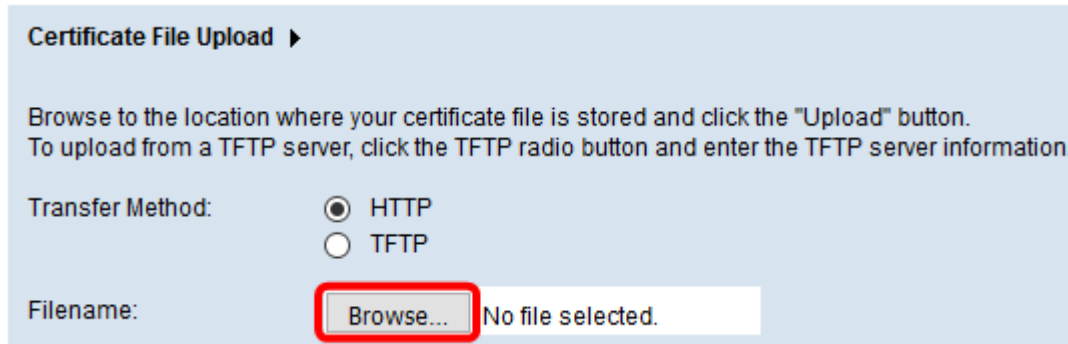
The screenshot shows the 'Certificate File Upload' section. It includes a play button icon, instructions to browse for the certificate file or use TFTP, and a 'Transfer Method' section with radio buttons for 'HTTP' (selected) and 'TFTP'. A 'Filename' field with a 'Browse...' button and 'No file selected.' text is also visible.

Beim Hochladen der Datei gibt es zwei Übertragungsmethoden:

- Hypertext Transfer Protocol (HTTP)
- Trivial File Transfer Protocol (TFTP)

Hinweis: In diesem Beispiel wird HTTP ausgewählt.

Schritt 2: (Optional) Wenn HTTP ausgewählt ist, klicken Sie auf **Durchsuchen**, um die Zertifikatsdatei von Ihrem Computer auszuwählen, und fahren Sie dann mit [Schritt 5 fort](#).



Certificate File Upload ▶

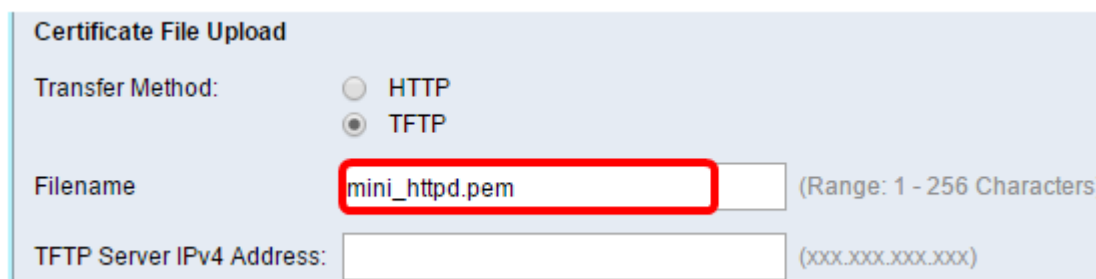
Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Transfer Method: HTTP
 TFTP

Filename: No file selected.

Schritt 3: (Optional) Wenn Sie in Schritt 1 TFTP ausgewählt haben, geben Sie den Namen der Zertifikatsdatei in das Feld *Dateiname ein*. Der TFTP-Server dient zum automatischen Übertragen von Boot-Dateien innerhalb von Geräten und ist sehr einfach.

Hinweis: In diesem Beispiel wird *mini_httpd.pem* als Dateiname verwendet.



Certificate File Upload

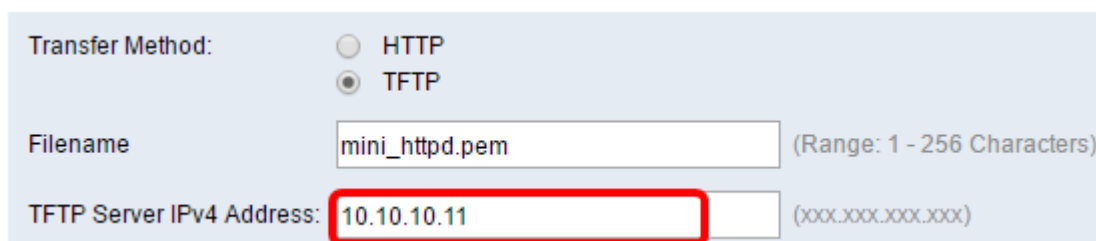
Transfer Method: HTTP
 TFTP

Filename (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

Schritt 4: Geben Sie die IP-Adresse des TFTP-Servers in das Feld *IPv4-Adresse des TFTP-Servers ein*.

Hinweis: In diesem Beispiel wird 10.10.10.11 als IPv4-Adresse des TFTP-Servers verwendet.



Transfer Method: HTTP
 TFTP

Filename (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

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

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

Hinweis: Wenn Sie andere WAP-Modelle verwenden, klicken Sie auf **Hochladen**.

Schritt 6: Klicken Sie auf die Schaltfläche, um die Einstellungen zu speichern.

Sie sollten jetzt eine Zertifikatsdatei erfolgreich auf Ihren WAP hochgeladen haben.