

Arbeitsgruppen-Bridge-Konfiguration für WAP551- und WAP561-Access Points

Ziel

In diesem Artikel wird erläutert, wie die Arbeitsgruppen-Bridge auf WAP551- und WAP561-Access Points konfiguriert wird.

Die Funktion Arbeitsgruppen-Bridge ermöglicht dem Wireless Access Point (WAP) die Überbrückung des Datenverkehrs zwischen einem Remote-Client und dem Wireless LAN, das mit dem Arbeitsgruppen-Bridge-Modus verbunden ist. Das der Remote-Schnittstelle zugeordnete WAP-Gerät wird als Access Point-Schnittstelle bezeichnet, und das dem WLAN zugeordnete Gerät wird als Infrastruktur-Schnittstelle bezeichnet. Diese Funktion wird empfohlen, wenn die WDS-Funktion nicht verwendet werden kann, da die WDS-Funktion eine bevorzugte Bridge-Lösung für den WAP551 und den WAP561 ist. Wenn die Workgroup Bridge-Funktion aktiviert ist, funktioniert die WDS Bridge-Funktion nicht. Um zu erfahren, wie die WDS Bridge konfiguriert ist, lesen Sie den Artikel *Wireless Distribution System (WDS) Bridge Configuration auf WAP551 und WAP561 Access Points*.

Anwendbare Geräte

WAP551
WAP561

Softwareversion

·v1.0.4.2

Arbeitsgruppen-Bridge konfigurieren

Hinweis: Damit Arbeitsgruppen-Bridge-Clustering aktiviert werden kann, muss dieser im WAP aktiviert sein. Wenn sie deaktiviert ist, müssen Sie die Single-Point-Einrichtung deaktivieren, die wiederum Clustering aktiviert. Alle WAP-Geräte, die an der Workgroup Bridge teilnehmen, müssen über gemeinsame Einstellungen für das Funkmodul, den IEEE 802.11-Modus, die Kanalbandbreite und den Kanal verfügen (Audio wird nicht empfohlen).

Um sicherzustellen, dass diese Einstellungen auf allen Geräten gleich sind, überprüfen Sie die Funkeinstellungen. Informationen zum Konfigurieren dieser Einstellungen finden Sie im Artikel *Funkeinstellungen auf WAP551/WAP561*.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Wireless > Work Group Bridge (Wireless > Arbeitsgruppen-Bridge)**. Die Seite *Arbeitsgruppen-Brücke* wird geöffnet:

WorkGroup Bridge

Refresh

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (+)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security: (+)

MAC Filtering:

MAC Acl Mode:

Schritt 2: Aktivieren Sie im Feld Arbeitsgruppen-Bridge-Modus die Option **Enable (Aktivieren)**, um die Funktion Arbeitsgruppen-Bridge zu aktivieren.

WorkGroup Bridge

Refresh

WorkGroup Bridge Mode: Enable

Radio Setting Per Interface

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1
 Radio 2

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

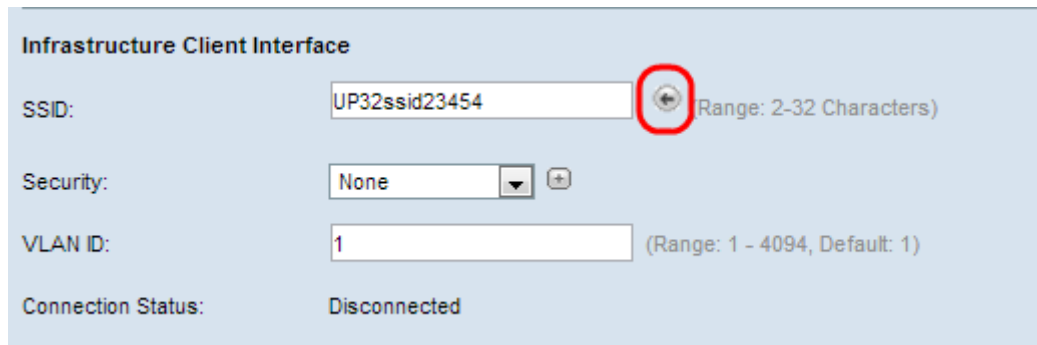
Security: (+)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Schritt 3: Dieser Schritt wird nur für WAP561 benötigt. Klicken Sie entweder auf das Optionsfeld **Radio1** oder **Radio 2**, um eine der Funkschnittstellen auszuwählen. Ignorieren Sie diesen Schritt für WAP551, der nur über eine Funkschnittstelle verfügt. Um herauszufinden, welche Funkeinheit eingerichtet ist und mit welchen Parametern die Funkeinstellungen nachgeschlagen werden. Informationen zum Konfigurieren dieser Einstellungen finden Sie im Artikel *Funkeinstellungen auf WAP551/WAP561*.

Schritt 4: Geben Sie im Feld SSID (SSID) den Namen Service Set Identifier (SSID) für die Infrastruktur-Client-Schnittstelle oder den Upstream Access Point (AP) ein.



Infrastructure Client Interface

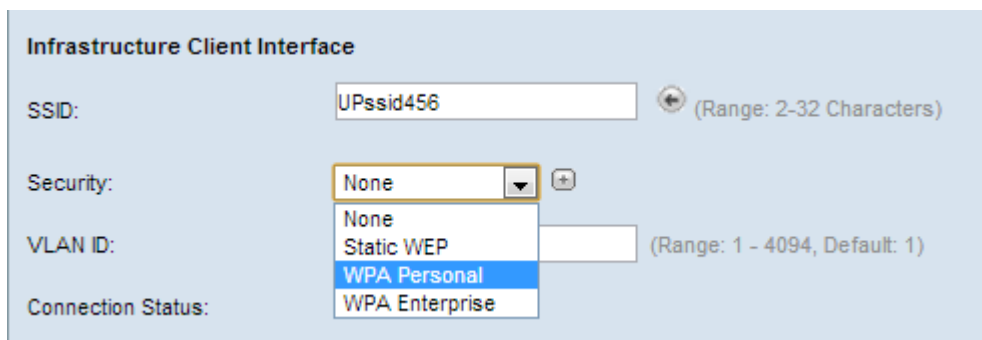
SSID: (Range: 2-32 Characters)

Security: (None)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Tipp: Sie können auch auf das **Pfeilsymbol** neben dem SSID-Feld klicken, um nach ähnlichen benachbarten SSIDs zu suchen. Diese Funktion ist nur aktiviert, wenn die AP-Erkennung in der Erkennung nicht autorisierter APs aktiviert ist (standardmäßig deaktiviert). Lesen Sie den Artikel *Rogue Access Point (AP) Detection auf WAP561 und WAP551*, um die Erkennung nicht autorisierter APs zu aktivieren.



Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (None, Static WEP, WPA Personal, WPA Enterprise)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Schritt 5: Wählen Sie aus der Dropdown-Liste im Feld Sicherheit im Abschnitt Infrastruktur-Client-Schnittstelle den Sicherheitstyp aus, der als Client-Station auf dem Upstream-WAP-Gerät (Infrastruktur-Client-Schnittstelle) authentifiziert werden soll. Die möglichen Optionen sind nachfolgend aufgeführt.

·Keine - Offen oder keine Sicherheit. Dies ist der Standardwert. Wenn Sie diese Option wählen, fahren Sie mit dem Abschnitt *VLAN-ID und Access Point-Schnittstelle konfigurieren fort*.

·[Static WEP](#) - Static WEP ist die minimale Sicherheit und kann bis zu 4 Schlüssel mit einer Länge von 64 bis 128 Bit unterstützen. In allen Knoten muss derselbe Schlüssel verwendet werden.

·[WPA Personal](#): WPA Personal ist im Vergleich zu WEP fortgeschrittener und unterstützt Schlüssel mit einer Länge von 8 bis 63 Zeichen. Die Verschlüsselungsmethode ist RC4 für WPA und Advanced Encryption Standard (AES) für WPA2. WPA2 wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard verfügt.

·[WPA Enterprise](#): WPA Enterprise ist die fortschrittlichste und empfohlene

Sicherheitslösung. Es verwendet Protected Extensible Authentication Protocol (PEAP), in dem jeder Wireless-Benutzer unter WAP mit individuellen Benutzernamen und Kennwörtern autorisiert ist, die sogar AES-Verschlüsselungsstandards unterstützen können. Zusätzlich zu PEAP wird auch Transport Layer Security (TLS) verwendet, bei dem jeder Benutzer ein zusätzliches Zertifikat bereitstellen muss, um Zugriff zu erhalten. Die Verschlüsselungsmethode ist RC4 für WPA und Advanced Encryption Standard (AES) für WPA2.

Hinweis: Je nach Wahl des IEEE 802.11-Modus kann die Verfügbarkeit der oben genannten Optionen variieren.

Schritt 6: Klicken Sie auf die Option, die Sie in Schritt 5 ausgewählt haben, und folgen Sie den entsprechenden Anweisungen. Wenn Sie None (Keine) auswählen, müssen Sie keine dieser Prozeduren konfigurieren.

The screenshot shows a configuration page with two main sections: 'Infrastructure Client Interface' and 'Access Point Interface'.
Infrastructure Client Interface:
- SSID: Infrastructure Client SSID (Range: 2-32 Characters)
- Security: None (dropdown menu with a plus icon)
- VLAN ID: 102 (Range: 1 - 4094, Default: 1)
- Connection Status: Disconnected
Access Point Interface:
- Status: Enable
- SSID: Access Point SSID (Range: 2-32 Characters)
- SSID Broadcast: Enable
- Security: None (dropdown menu with a plus icon)
- MAC Filtering: Local (dropdown menu)
- MAC Acl Mode: Accept (dropdown menu)
- VLAN ID: 1 (Range: 1 - 4094, Default: 1)
At the bottom left, there is a 'Save' button.

Schritt 7: Geben Sie im Feld VLAN ID (VLAN-ID) die VLAN-ID für die Infrastruktur-Client-Schnittstelle ein.

Schritt 8: Aktivieren Sie im Feld Status die Option **Aktivieren**, um das Bridging auf der Access Point-Schnittstelle zu aktivieren.

Schritt 9: Geben Sie im Feld SSID (SSID) den Namen Service Set Identifier (SSID) für die Schnittstelle des Access Points ein.

Schritt 10: (Optional) Wenn die Downstream-SSID (Access Point Interface SSID) gesendet werden soll, aktivieren Sie im Feld SSID Broadcast die Option **Enable (Aktivieren)**. Es ist standardmäßig aktiviert.

Schritt 11: Wählen Sie in der Dropdown-Liste Security (Sicherheit) den Sicherheitstyp aus, um nachgeschaltete Client-Stationen am WAP-Gerät (Access Point Interface) zu authentifizieren. Mögliche Werte sind:

- Keine - Offen oder keine Sicherheit. Dies ist der Standardwert. Wenn Sie diese Option wählen, überspringen Sie die Schritte 12 bis 15. Fahren Sie mit Schritt 16 fort.
- Static WEP - Static WEP ist die minimale Sicherheit und kann bis zu 4 Schlüssel mit einer Länge von 64 bis 128 Bit unterstützen. Befolgen Sie den Abschnitt [Static WEP konfigurieren](#). Fahren Sie mit Schritt 16 fort.
- WPA Personal - WPA Personal ist im Vergleich zu WEP fortgeschrittener und unterstützt Schlüssel mit einer Länge von 8 bis 63 Zeichen. Die Verschlüsselungsmethode ist entweder Temporal Key Integrity Protocol (TKIP) oder Counter Cipher Mode mit Block Chaining Message Authentication Code Protocol (CCMP). WPA2 mit CCMP wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard, Advanced Encryption Standard (AES), verfügt, als das TKIP, das nur einen 64-Bit-RC4-Standard verwendet.

The screenshot shows the 'Access Point Interface' configuration page. The 'Status' is set to 'Enable'. The 'SSID' is 'Access Point SSID' with a range of 2-32 characters. 'SSID Broadcast' is 'Enable'. 'Security' is set to 'WPA Personal'. A sub-section for WPA settings is expanded, showing 'WPA Versions' with 'WPA' and 'WPA2' checked, 'Cipher Suites' with 'TKIP' and 'CCMP (AES)' checked, a 'Key' field with 8 dots, and a 'Broadcast Key Refresh Rate' of 300. Below this, 'MAC Filtering' is 'Disabled', 'MAC Acl Mode' is 'Deny', and 'VLAN ID' is '1'.

Zeitgeber: Führen Sie die Schritte 12 bis 15 nur aus, wenn Sie in Schritt 11 WPA Personal ausgewählt haben.

Schritt 12: Aktivieren Sie die entsprechenden Kontrollkästchen, um die WPA-Version auszuwählen. Sie können sowohl WPA als auch WPA2 in verschiedenen WPA-Clients auswählen, die unterschiedliche WPA-Versionen haben.

Schritt 13: Aktivieren Sie die entsprechenden Kontrollkästchen, um die Verschlüsselungssuiten auszuwählen. Sie wählen sowohl TKIP als auch CCMP(AES) aus.

Schritt 14: Geben Sie den gemeinsamen WPA-Schlüssel in das Feld Schlüssel ein. Der Schlüssel kann alphanumerische Zeichen, Groß- und Kleinbuchstaben und Sonderzeichen enthalten.

Schritt 15: Geben Sie im Feld "Broadcast Key Refresh Rate" (Aktualisierungsrate für Sendeschlüssel) das gewünschte Intervall für die Tastenaktualisierung ein. In diesem Intervall sollte der Gruppenschlüssel für alle WAP-Clients aktualisiert werden.

Schritt 16: Wählen Sie aus der Dropdown-Liste MAC Filtering (MAC-Filterung) den Typ der MAC-Filterung aus, die für die Access Point-Schnittstelle konfiguriert werden soll. Wenn diese Funktion aktiviert ist, wird Benutzern basierend auf der MAC-Adresse des Clients, den sie verwenden, der Zugriff auf den WAP gewährt oder verweigert. Mögliche Werte sind:

- Disabled (Deaktiviert): Alle Clients können auf das Upstream-Netzwerk zugreifen. Dies ist der Standardwert.
- Local (Lokal): Die Clients, die auf das Upstream-Netzwerk zugreifen können, sind auf die Clients beschränkt, die in einer lokal definierten MAC-Adressliste angegeben sind.
- Radius - Der Client-Satz, der auf das Upstream-Netzwerk zugreifen kann, ist auf die in einer MAC-Adressliste auf einem RADIUS-Server angegebenen Clients beschränkt.

Schritt 17: Geben Sie im Feld VLAN ID (VLAN-ID) die VLAN-ID für die Client-Schnittstelle des Access Points ein.

Hinweis: Um das Bridging von Paketen zu ermöglichen, sollte die VLAN-Konfiguration für die Access Point-Schnittstelle und die kabelgebundene Schnittstelle mit der der Infrastruktur-Client-Schnittstelle übereinstimmen.

Schritt 18: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

[Statisches WEP konfigurieren](#)

Führen Sie die folgenden Schritte aus, wenn Sie Static WEP als Authentifizierungstyp konfiguriert haben.

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security:

Transfer Key Index:

Key Length: 64 bits 128 bits

Key Type: ASCII Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: **Disconnected**

Schritt 1: Wenn Sie Static WEP (Statischer WEP) auswählen, werden einige zusätzliche Felder angezeigt. Wählen Sie aus der Dropdown-Liste im Feld Transfer Key Index (Transfer Key-Index) einen Schlüsselindex aus. Die verfügbaren Werte sind 1, 2, 3 und 4. Der Standardwert ist 2. Der Schlüsselindex ist für verschiedene WLANs unterschiedlich. Die mit einem bestimmten WLAN verbundenen Geräte müssen über denselben Schlüsselindex verfügen. Dieser Schlüssel wird zur Verschlüsselung von Daten für die Kommunikation verwendet.

Schritt 2: Wählen Sie im Feld Key Length (Schlüssellänge) entweder das Optionsfeld **64 bits** oder die Optionsschaltfläche **128 bits** aus. Gibt die Länge des verwendeten Schlüssels an.

Schritt 3: Klicken Sie entweder auf das Optionsfeld **ASCII** oder das Optionsfeld **HEX**, um den Schlüsseltyp im Feld Schlüsseltyp auszuwählen. WEP-Schlüssel sind normalerweise in Hexadezimalform.

Security: Static WEP

Transfer Key Index: 1

Key Length: 64 bits 128 bits

Key Type: ASCII Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Schritt 4: Geben Sie in den nächsten vier Feldern im Feld WEP-Schlüssel bis zu vier WEP-Schlüssel ein, die als 1, 2, 3 und 4 gekennzeichnet sind. Dies ist eine Zeichenfolge, die als Schlüssel eingegeben wird. Die Länge des Schlüssels variiert je nach Länge und Typ des Schlüssels. Die erforderliche Länge wird neben dem Feld "WEP Key" (WEP-Schlüssel) angegeben. Die WEP-Schlüsselzeichenfolgen müssen in allen WAP-Knoten (AP und Clients) übereinstimmen und an denselben Stellen im gleichen Feld angeordnet sein. Das bedeutet, wenn Zeichenfolge 1 in einem Gerät Schlüssel 1 ist, muss Zeichenfolge 1 auch auf den anderen Geräten in der Arbeitsgruppen-Bridge der Schlüssel 1 sein.

Klicken Sie [hier](#), um mit der Konfiguration fortzufahren.

WPA Personal konfigurieren

Führen Sie die folgenden Schritte aus, wenn Sie WPA Personal als Authentifizierungstyp konfiguriert haben.

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: WPA Personal

WPA Versions: WPA WPA2

Key: (Range: 8-63 Characters)

VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Schritt 1: Aktivieren Sie entweder **WPA** oder **WPA2**, um die WPA-Version auszuwählen. In der Regel wird WPA nur dann ausgewählt, wenn keiner der beteiligten WAPs WPA2 unterstützt. Andernfalls wird WPA 2 empfohlen.

Schritt 2: Geben Sie den gemeinsamen WPA-Schlüssel in das Feld Schlüssel ein. Der

Schlüssel kann alphanumerische Zeichen, Groß- und Kleinbuchstaben und Sonderzeichen enthalten.

Klicken Sie [hier](#), um mit der Konfiguration fortzufahren.

WPA-Enterprise konfigurieren

Führen Sie die folgenden Schritte aus, wenn Sie WPA Enterprise als Authentifizierungstyp konfiguriert haben.

The screenshot shows the 'Infrastructure Client Interface' configuration page. The SSID field is 'Infrastructure Client SSID' with a range of 2-32 characters. The Security dropdown is set to 'WPA Enterprise'. Under 'WPA Versions', 'WPA' is unchecked and 'WPA2' is checked. Under 'EAP Method', 'PEAP' is selected with a radio button, and 'TLS' is unselected. There are empty input fields for 'Username' and 'Password'. The 'VLAN ID' field contains '1' with a range of 1-4094 and a default of 1. The 'Connection Status' is 'Disconnected'.

Schritt 1: Wenn Sie WPA Enterprise ausgewählt haben, aktivieren Sie entweder **WPA** oder **WPA2**, um die WPA-Version auszuwählen. In der Regel wird WPA nur dann ausgewählt, wenn keiner der WAPs im Bridge-System WPA2 unterstützt. WPA 2 ist die erweiterte und empfohlene Version.

Schritt 2: Klicken Sie auf das entsprechende Optionsfeld, um zwischen den beiden EAP-Methoden zu wählen.

·PEAP - Protected EAP. Sie stützt sich auf TLS, vermeidet jedoch die Installation digitaler Zertifikate auf jedem Client. Stattdessen wird die Authentifizierung über einen Benutzernamen und ein Kennwort ermöglicht. Führen Sie die Schritte 3 bis 5 aus.

·TLS - Authentifizierung durch Austausch digitaler Zertifikate. Erfordert die Durchführung der Schritte 3 bis 7.

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security:

WPA Versions: WPA WPA2

EAP Method: PEAP TLS

Username:

Password:

VLAN ID: (Range: 1 - 4094, Default: 1)

Schritt 3: Unabhängig von der in Schritt 1 gewählten Methode geben Sie im Feld Benutzername einen Benutzernamen ein.

Schritt 4: Unabhängig von der in Schritt 1 gewählten Methode geben Sie im Feld Kennwort ein Kennwort ein.

Schritt 5: Wenn Sie PEAP ausgewählt haben, klicken Sie [hier](#), um mit der Konfiguration fortzufahren. Wenn Sie TLS ausgewählt haben, fahren Sie mit Schritt 6 fort.

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security:

WPA Versions: WPA WPA2

EAP Method: PEAP TLS

Identity:

Private Key:

Certificate File Present:

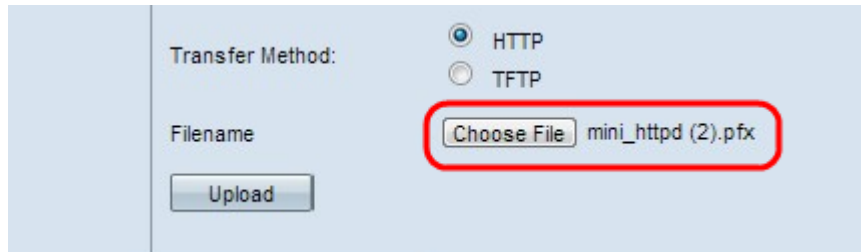
Certificate Expiration Date:

Transfer Method: HTTP TFTP

Certificate File: No file chosen

Schritt 6: Wenn Sie TLS ausgewählt haben, klicken Sie entweder auf das **HTTP**- oder das **TFTP**-Optionsfeld, um zwischen den beiden Übertragungsmodi auszuwählen, um eine Zertifikatsdatei für die TLS-Authentifizierung herunterzuladen.


·HTTP - Herunterladen über einen Webserver oder PC.



The screenshot shows a configuration panel for the HTTP transfer method. Under 'Transfer Method:', the 'HTTP' radio button is selected. Below this, the 'Filename' field contains 'mini_httpd (2).pfx' and is highlighted with a red rounded rectangle. To the left of the filename is a 'Choose File' button. At the bottom of the panel is an 'Upload' button.

- Datei auswählen - Wählen Sie eine Zertifikatsdatei aus. Es muss sich um eine Zertifikatsstypdatei mit den Erweiterungen .pem, .pfx usw. handeln. Andernfalls kann der Upload der Datei nicht erfolgreich sein.

·TFTP — Download von einem Dateiserver. Es müssen Schritte durchgeführt werden.



The screenshot shows a configuration panel for the TFTP transfer method. Under 'Transfer Method:', the 'TFTP' radio button is selected. Below this, the 'Filename' field contains 'mini_httpd.pem'. Below the filename field is the 'TFTP Server IPv4 Address' field, which contains '192.168.1.20'. At the bottom of the panel is an 'Upload' button.

- Dateiname: Geben Sie den Namen der Zertifikatsdatei im Feld Dateiname ein.

- TFTP Server IPv4 Address (IPv4-Adresse des TFTP-Servers) - Geben Sie die IP-Adresse des TFTP-Servers ein.

Hinweis: Das Feld "Transfer von Zertifikatsdateien" zeigt an, ob ein Zertifikat im WAP vorhanden ist, und das Feld "Ablaufdatum für Zertifikate" zeigt das Ablaufdatum dieses Zertifikats.

Schritt 7: Klicken Sie auf **Hochladen**.

Klicken Sie [hier](#), um mit der Konfiguration fortzufahren.