

# Vorgehensweise: Erweiterung von Cisco Umbrella zum Schutz Ihres Wireless-Netzwerks

## Einführung

Datensicherheit ist ein Gruppenansatz in jedem Unternehmen. Die Mitarbeiter sind zumindest teilweise dafür verantwortlich, sicherzustellen, dass sie nicht betrogen werden. In der Praxis ist Sicherheit schwierig, und es ist kein Wunder, warum. Wenn die Werkzeuge der Technologie weiter ausgebaut werden, wie dies auch für die Fortschritte der Hacker der Fall ist, steigen alle Boote sozusagen mit der Flut auf. Lesen Sie weiter, wie Sie Umbrella Protection in Ihr LAN integrieren können.

## Ziel

In dieser Anleitung erfahren Sie, wie Sie die Sicherheitsplattform von Umbrella in Ihr Wireless-Netzwerk integrieren können. Bevor wir uns mit den Details zu den Zerstreungen befassen, beantworten wir einige Fragen, die Sie sich vielleicht zu Umbrella stellen.

## Anwendbare Geräte

- WAP125
- WAP581

## Softwareversion

- 1,0/1

## Anforderungen

Ein aktives Umbrella-Konto (Sie haben kein eigenes Konto? [Kostenvoranschlag anfordern](#) oder [kostenlose Testversion](#) starten)

## Was ist Umbrella?

Umbrella ist eine einfache, aber sehr effektive Cloud-Sicherheitsplattform von Cisco. Umbrella ist in der Cloud tätig und führt zahlreiche sicherheitsrelevante Services durch. Von der Bedrohung bis zur Untersuchung nach einem Ereignis. Umbrella erkennt und verhindert Angriffe über alle Ports und Protokolle hinweg.

## Wie funktioniert es?

Umbrella verwendet DNS als Hauptvektor für die Verteidigung. Wenn Benutzer eine URL in ihre Browser-Leiste eingeben und die Eingabetaste drücken, nimmt Umbrella an der Übertragung teil. Diese URL wird an den DNS-Resolver von Umbrella übergeben. Wenn eine Sicherheitswarnung mit der Domäne verknüpft ist, wird die Anforderung blockiert. Diese Telemetriedaten werden in Mikrosekunden analysiert, wodurch eine Latenz nahezu vermieden wird. Die Telemetriedaten nutzen Protokolle und Instrumente, um weltweit Milliarden von DNS-Anfragen zu verfolgen. Wenn

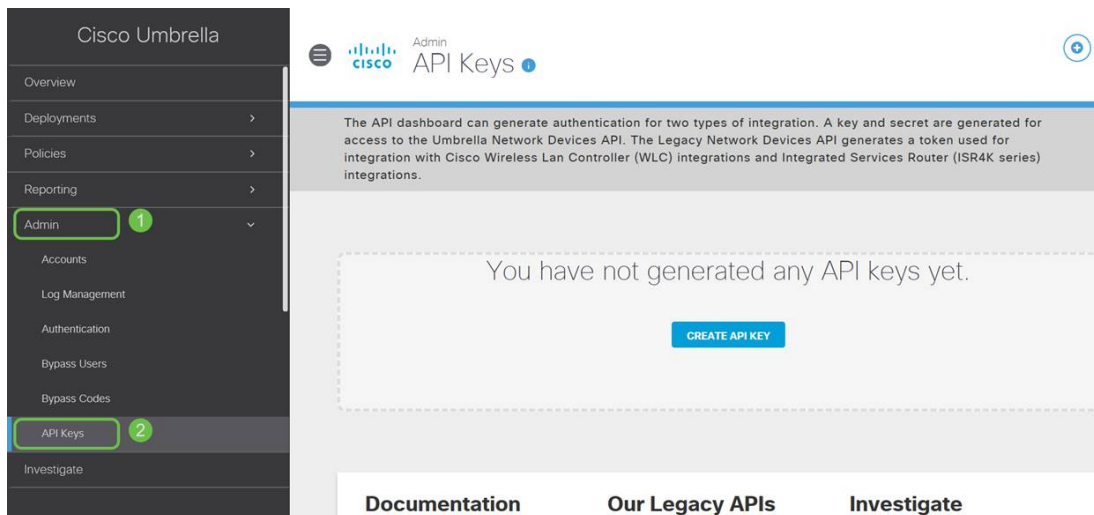
diese Daten allgegenwärtig sind, können sie weltweit korreliert werden, um schnell auf Angriffe reagieren zu können, sobald diese beginnen. Weitere Informationen finden Sie in der Datenschutzrichtlinie von Cisco - [vollständige Richtlinie](#), [Kurzfassung](#). Telemetriedaten sind Daten, die von Tools und Protokollen abgeleitet wurden.

Um es in einer Metapher zusammenzufassen: Stellen Sie sich vor, Sie sind auf einer Party. Auf dieser Party ist jeder auf seinem Telefon surfen im Internet. Das stille Gruppenschweigen wird von den ParteichefInnen gestoppt, die auf ihren Bildschirmen wegschlagen. [Es ist keine tolle Party](#), aber während Sie auf Ihrem eigenen Telefon sehen Sie einen Hyperlink zu einem kitten GIF, das scheint unwiderstehlich. Sie sind sich jedoch nicht sicher, ob Sie darauf tippen oder nicht, da die URL fragwürdig erscheint. Bevor Sie also auf den Hyperlink tippen, rufen Sie den Rest der Partei an: "Ist dieser Link schädlich?" Wenn eine andere Person auf der Party den Link besucht und entdeckt hätte, dass es ein Betrug war, würden sie zurückrufen: "Ja, das habe ich getan, und das ist ein Betrug!" Sie danken dieser Person, dass sie Sie rettet hat, und setzen Ihre Suche nach Bildern süßer Tiere in Stille fort. Bei der Skala von Cisco werden Sicherheitsüberprüfungen für Anfragen und Rückrufe Millionen Mal pro Sekunde durchgeführt.

## Klingt großartig, wie können wir das aufheben?

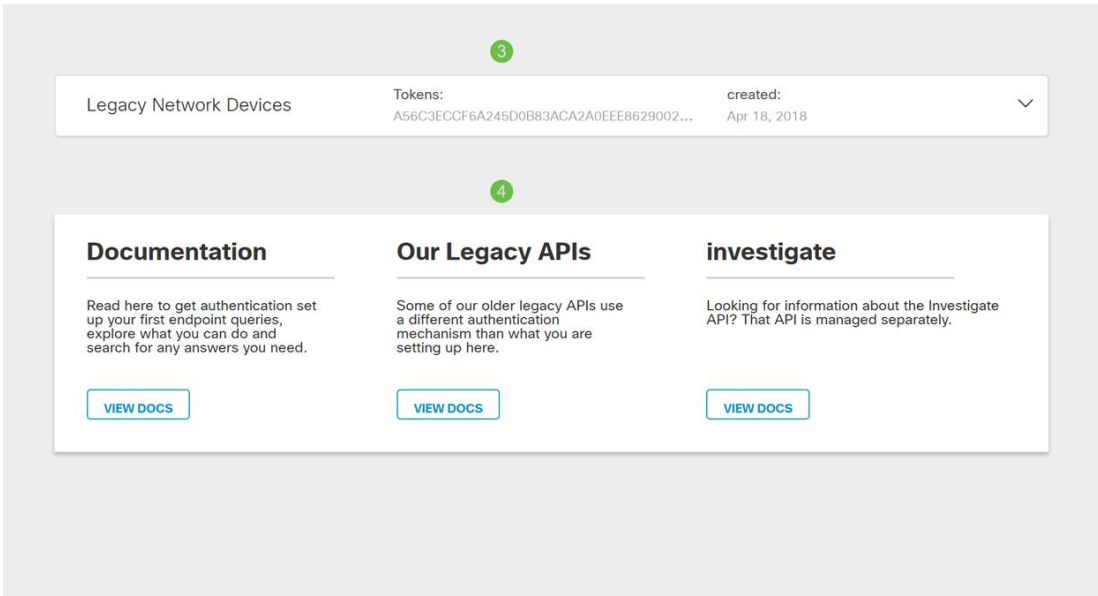
Beginnen Sie bei der Navigation in diesem Leitfaden mit der Abfrage des API-Schlüssels und des Geheimschlüssels im Umbrella Account Dashboard. Anschließend melden wir uns bei Ihrem WAP-Gerät an, um die API und den geheimen Schlüssel hinzuzufügen. Wenn Probleme auftreten, [finden Sie hier Dokumentation](#) und [hier die Support-Optionen für Umbrella](#).

Schritt 1: Wenn Sie sich bei Ihrem Umbrella Account angemeldet haben, klicken Sie im *Dashboard*-Bildschirm auf **Admin > API Keys (Admin > API-Schlüssel)**.

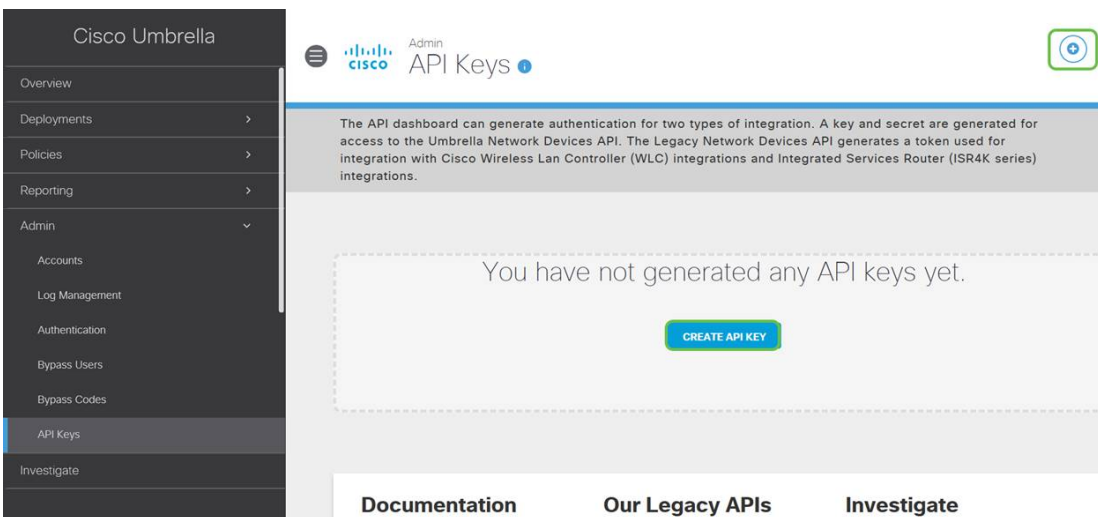


### Bildschirm "Anatomy of the API Keys" -

1. *API-Schlüssel hinzufügen* - Initiiert die Erstellung eines neuen Schlüssels für die Verwendung mit der Umbrella API.
2. *Zusätzliche Informationen*: Hierfür wird eine Erklärung nach unten bzw. nach oben angezeigt.
3. *Token Well* - Enthält alle Schlüssel und Token, die von diesem Konto erstellt wurden. (Fügt nach dem Erstellen eines Schlüssels ein)
4. *Support-Dokumente* - Links zu Dokumentationen auf der übergeordneten Website zu den Themen in den einzelnen Abschnitten.



Schritt 2: Klicken Sie in der rechten oberen Ecke auf die Schaltfläche **API-Schlüssel hinzufügen**, oder klicken Sie auf die Schaltfläche **API-Schlüssel erstellen**. Beide funktionieren gleich.



Schritt 3: Wählen Sie **Umbrella Network Devices** und klicken Sie dann auf die Schaltfläche **Create (Erstellen)**.

## What should this API do?

Choose the API that you would like to use.

1



### Umbrella Network Devices

To be used to integrate Umbrella-enabled hardware with your organization. In addition, allows you to create, update, list and delete identities in Umbrella.



### Legacy Network Devices

A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.

**i** You can only generate one token. Refresh your current token to get a new token.



### Umbrella Reporting

Enables API access to query for Security Events and traffic to specific Destinations

CANCEL


2


CREATE

Schritt 4: Klicken Sie auf die Schaltfläche **Kopieren** rechts neben Ihrem *Geheimschlüssel*. Eine Popup-Benachrichtigung bestätigt, dass der Schlüssel in Ihre Zwischenablage kopiert wird.

Umbrella Network Devices      Key: aae [redacted]      Created: Jul 26, 2018

The API key and secret here are used to perform API requests against your Umbrella organization, such as identity management, reporting and more. If you are using an Umbrella-integrated hardware device that uses basic authentication, this allows management of Umbrella from the device and vice versa.

**Your Key:** aae [redacted] 

**Your Secret:** 352 [redacted] 

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

Check out the [documentation](#) for step by step instructions.

**DELETE**      **REFRESH**      **CLOSE**

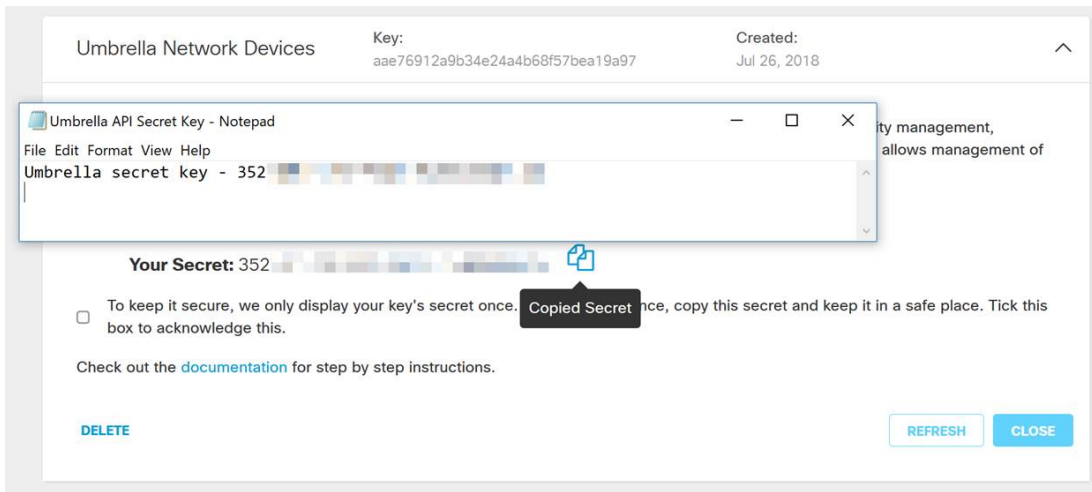
Nachdem Sie den Schlüssel und geheimen Schlüssel in einen sicheren Bereich kopiert haben, klicken Sie auf das **Kontrollkästchen**, um die Bestätigung abzuschließen, und klicken Sie dann auf die Schaltfläche **Schließen**.

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

Check out the [documentation](#) for step by step instructions.

**DELETE**      **REFRESH**      **CLOSE**

Schritt 5: Öffnen Sie einen Texteditor, z. B. Notizblock, und fügen Sie Ihren geheimen und API-Schlüssel in das Dokument ein. Bezeichnen Sie ihn als Referenz für die Zukunft. In diesem Fall ist die Bezeichnung "Umbrella secret Key". Schließen Sie den API-Schlüssel zusammen mit Ihrem geheimen Schlüssel und einer kurzen Beschreibung seiner Verwendung in derselben Textdatei an. Speichern Sie die Textdatei an einem sicheren Ort, der Ihnen später bei Bedarf leicht zugänglich ist.



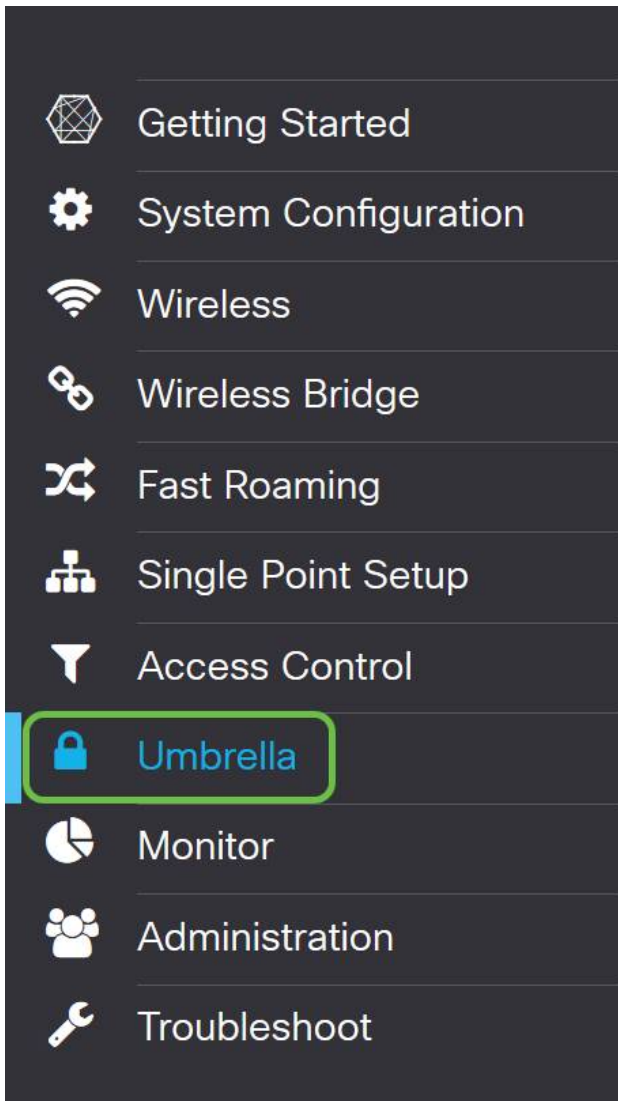
**Wichtiger Hinweis:** Wenn Sie den geheimen Schlüssel verlieren oder versehentlich löschen, gibt es keine Funktion oder Support-Nummer, um diesen Schlüssel abzurufen. [Halte es geheim, halte es sicher](#). Wenn der Schlüssel verloren geht, müssen Sie den Schlüssel löschen und den API-Schlüssel mit jedem WAP-Gerät, das Sie mit Umbrella schützen möchten, erneut autorisieren.

**Best Practice:** Bewahren Sie nur eine *einzelne* Kopie dieses Dokuments auf einem Gerät wie einem USB-Stick auf, auf den von einem Netzwerk aus nicht zugegriffen werden kann.

## Konfigurieren von Umbrella auf Ihrem WAP-Gerät

Nachdem wir API-Schlüssel in Umbrella erstellt haben, werden wir diese Schlüssel auf unseren WAP-Geräten installieren. In unserem Fall verwenden wir einen WAP581.

Schritt 1: Nach der Anmeldung bei Ihrem WAP-Gerät, klicken Sie auf **Umbrella** im Sidebar-Menü.



Schritt 2: Der Bildschirm Umbrella ist einfach, aber es gibt zwei Felder, die Sie hier definieren sollten:

- *Lokale Domänen für die Umgehung*: Dieses Feld enthält Ihre internen Domänen, die Sie vom Umbrella-Service ausschließen möchten.
- *DNSCrypt* - Sichert die Übertragung von Paketen zwischen dem DNS-Client und dem DNS-Resolver. Diese Funktion ist standardmäßig aktiviert. Wenn Sie diese Funktion deaktivieren, wird die Sicherheit Ihres Netzwerks beeinträchtigt.

The screenshot shows the Cisco Umbrella configuration interface for a device named WAP581-WAP581. At the top, there is a navigation bar with the Cisco logo, the device name, and a language dropdown set to 'English'. Below the navigation bar, the title 'Umbrella' is displayed on the left, and 'Save' and 'Cancel' buttons are on the right. The main content area contains the following configuration options:

- Enable:** A checkbox that is currently unchecked.
- API Key:** A text input field with a help icon.
- Secret:** A text input field with a help icon.
- Local Domains to Bypass (optional):** A text input field containing the placeholder text 'Multiple inputs separated by comma'.
- Device Tag (optional):** A text input field containing the value 'WAP581'.
- DNSCrypt:** A checkbox labeled 'Enable' that is currently unchecked.
- Registration Status:** A label with no associated input field.

### Schritt 3: API und Geheimschlüssel in die entsprechenden Felder einfügen

Umbrella

Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.  
With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.  
This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt:  Enable

Registration Status:

### Schritt 4: Stellen Sie sicher, dass die Kontrollkästchen für **Aktivieren** und **DNSCrypt** in den Aktivierungsstatus geändert werden.

Umbrella

Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.  
With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.  
This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt:  Enable

Registration Status:

**Hinweis:** DNSCrypt sichert die DNS-Kommunikation zwischen einem DNS-Client und einem DNS-Resolver. Die Standardeinstellung ist aktiviert.

### Schritt 5: (Optional) Geben Sie die lokalen Domänen ein, die Umbrella über den DNS-Auflösungsprozess erlauben soll.

Umbrella

Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.  
With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.  
This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt:  Enable

Registration Status:

**Hinweis:** Dies ist für alle Intranet-Domänen und geteilten DNS-Domänen erforderlich. Wenn für Ihr Netzwerk die Verwendung von lokalen Domänen für das Routing erforderlich ist, müssen Sie sich an den Umbrella Support wenden, um diese Funktion in Betrieb zu nehmen. Die meisten Benutzer müssen diese Option nicht verwenden.

Schritt 6: Wenn Sie mit den Änderungen zufrieden sind oder Ihre eigenen *lokalen Domänen zu Bypass* hinzugefügt haben, klicken Sie auf die **Save**-Schaltfläche in der oberen rechten Ecke.



Schritt 7: Nach Abschluss der Änderungen wird das Feld "Registrierungsstatus" in "Erfolgreich" angezeigt.

The image shows a configuration form with several fields. The 'Enable' checkbox is checked. The 'API Key' field contains 'aae' followed by a masked area. The 'Secret' field contains '352' followed by a masked area. The 'Local Domains to Bypass (optional)' field contains the text 'Multiple inputs separated by comma'. The 'Device Tag (optional)' field contains 'WAP581'. The 'DNSCrypt' checkbox is checked and labeled 'Enable'. At the bottom, the 'Registration Status' field is highlighted with a green border and contains the text 'Successful'.

## Bestätigen, dass alles am richtigen Ort ist


Herzlichen Glückwunsch! Sie sind jetzt geschützt Umbrella von Cisco. Oder sind Sie es? Cisco hat eine Website erstellt, auf der diese Daten so schnell wie möglich beim Laden der Seite ermittelt werden können. [Klicken Sie hier](#), oder geben Sie <https://InternetBadGuys.com> in die Browserleiste ein.

Wenn Umbrella richtig konfiguriert ist, werden Sie von einem Bildschirm ähnlich wie diesem begrüßt werden!



SECURITY THREAT DETECTED AND B... X

sinkhole-umbrella.cisco.com/?client\_ip=...&type=phish&url=uggc...



### SECURITY THREAT DETECTED AND BLOCKED

Based on Cisco Umbrella security threat information, access to the web site **Not\_Found** has been blocked to prevent an attack on your browser.

Malware protection has shifted from the endpoint, deeper into the network, in order to cater to a growing number and variety of devices. In order to offer the most effective protection to computing assets on the Cisco network, Infosec, Cisco IT, and the Security Business Group have jointly rolled out Umbrella protection for Cisco's corporate DNS infrastructure. This service will block access to hostnames that are known bad and has been deployed to prevent malicious actors from serving malware or content otherwise harmful to users of the Cisco corporate network.

If you believe this page should not be blocked, [open a case](#) providing the following information:

- Text or screenshot of the corresponding debug information below
- Business justification for use of the website

**Block Reason: Umbrella DNS Block**

Date: July 26, 2018  
Time: 22:58:17  
Host Requested: Not\_Found  
URL Requested: Not\_Found  
Client IP address: ...  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0  
Request Method: GET

Sehen Sie sich ein Video zu diesem Artikel an..

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)