

Hilfe bei blockierter IP-Adresse

Die Fehlerseite wird angezeigt, wenn Sie entweder eine ungültige Adresse (URL) ausgewählt haben oder von einer IP-Adresse aus zugreifen, welche Sie von Ihrem Internet-Service-Provider erhalten haben und welche für einen Zugriff auf unsere UniCredit Bank Services gesperrt ist.

Um sicherzustellen, dass Sie keine ungültige Adresse ausgewählt haben, rufen Sie bitte den Login für das Online Banking über unsere Homepage <https://www.hypovereinsbank.de> auf.

Wenn Sie die Meldung weiterhin erhalten, ist der Zugang Ihrer IP-Adresse aufgrund von Sicherheitsmaßnahmen der UniCredit gesperrt. Ursache dafür kann ein sicherheitsrelevanter Vorfall mit der von Ihnen genutzten IP-Adresse sein. Diese IP-Adresse bekommen Sie von Ihrem Internet-Service-Provider zugewiesen. Bei Vergabe von dynamischen IP-Adressen kann dieser Vorfall von einem früheren Nutzer herrühren.

Wie löse ich das Problem Schritt für Schritt?

1. Neustart des Routers

Zunächst wird ein Neustart des Routers empfohlen, da über diesen Vorgang ein Wechsel der IP-Adresse erwirkt werden kann. Versuchen Sie nach dem Neustart bitte nochmals, auf unser HVB Online Banking zuzugreifen. Sollte diese Maßnahme nicht zum gewünschten Erfolg führen, folgen Sie bitte den weiteren Anweisungen.

2. Überprüfen Ihrer IP-Adresse über das Internet-Sicherheitsunternehmen „Akamai“

Rufen Sie die URL <https://www.akamai.com/us/en/clientrep-lookup> auf und bestätigen Sie, dass Sie kein Roboter sind. Klicken Sie anschließend auf das Feld „Go“.

Überprüfen Sie hier, ob die IP-Adresse blockiert ist.

Auf dieser Seite finden Sie Informationen über mögliche Gründe, warum Ihrer IP-Adresse blockiert sein könnte.

Frequently Asked Questions

Why is Akamai blocking me?

Akamai does not block users from accessing our customers' websites. However, our customers can use tools and policies which may in turn block you (the end user). Our customers use these tools to protect them and you from malicious actors on the internet. Some common reasons could include:

- Explicit IP blocking / blacklisting
- Location-based blacklisting
- Rule-based blocking (i.e. web application firewall protections)
- Reputation-based blocking
- HTTP request rate controls (e.g. DoS protections)

The following activities may trigger application security controls:

- Web application layer attacks such as: SQL Injection, Cross-Site Scripting, Local File Inclusion, Remote Command Execution, Remote File Inclusion, etc.
- Volumetric attacks or similar high rate HTTP traffic
- Web content scraping, data mining, web content indexing and similar automated web activities
- Web vulnerability scanning using automated tools

Your reputation follows you. If your IP is identified as behaving poorly on one site, you may be blocked on other websites. A first step in troubleshooting may be to determine whether your IP Address is performing one of the activities listed above that could affect your reputation.

Why is my IP Address assigned bad reputation?

Client Reputation leverages advanced algorithms to compute a risk score based on prior behavior as observed over the Akamai network. An IP address is assigned with bad reputation when Akamai observes malicious activity originating from this IP address.

Where can I find more information on Client Reputation?

Additional information on Client Reputation can be found at: <https://www.akamai.com/solutions/security>

- Für weitere Fragen und Unterstützung steht Ihnen unser Onlineservice zur Verfügung. Bitte wenden Sie sich unter Anführung der SupportID aus dem Sperrbildschirm an 089/378-48888 bzw. onlineservice@unicredit.de.