

Sykasoft Firewall Server konfigurieren

In dieser Anleitung zeigen wir Ihnen Schritt für Schritt, wie Sie die **Windows Defender Firewall** so konfigurieren, dass Ihre Arbeitsplatzrechner reibungslos eine Verbindung zu einem zentralen Server herstellen können. Dabei gehen wir besonders auf die Freigabe bestimmter Programme und Dienste ein, die für den Zugriff auf einen Microsoft SQL Server erforderlich sind.

Die Windows Defender Firewall ist ein integraler Bestandteil des Windows-Betriebssystems und dient in erster Linie dem Schutz vor unbefugtem Zugriff von außen. Sie filtert Datenverkehr basierend auf vordefinierten Regeln und kann so gefährliche oder unerwünschte Verbindungen blockieren. Eine falsch konfigurierte Firewall kann jedoch auch berechtigte interne Verbindungen verhindern – beispielsweise von einem Arbeitsplatz zu einem Server im selben Netzwerk.

Schritt 1: Öffnen der Windows Defender Firewall	. 2
Schritt 2: Zulassen von Anwendungen durch die Windows Defender Firewall	. 3
Schritt 3: Anwendungen und Dienste für die Kommunikation durch die Firewall freigeben	.4

sykasoft GmbH Schleehofstraße 16, D-97209 Veitshöchheim Telefon +49 93129914-0 Telefax +49 93129914-30 info@sykasoft.de, www.sykasoft.de

Schritt 1: Öffnen der Windows Defender Firewall

Zunächst öffnen Sie die Windows Defender Firewall. Gehen Sie dazu folgendermaßen vor:

- 1. Klicken Sie unten links auf das **Suchfeld** in der Taskleiste (alternativ drücken Sie die **Windows-Taste** auf Ihrer Tastatur).
- 2. Geben Sie dort "Windows Defender Firewall" ein.
- 3. Wählen Sie anschließend den Eintrag **"Windows Defender Firewall"** aus den Suchergebnissen aus, um die Anwendung zu starten.

Sobald sich das Fenster geöffnet hat, können Sie mit den weiteren Schritten zur Einrichtung der Firewall-Regeln fortfahren, um den Zugriff Ihrer Arbeitsstationen auf den Server zu ermöglichen.

Suchen Apps Dokumente Web	Mehr 🔫					
Höchste Übereinstimmung						
Windows Defender Firewall mit erweiterter Sicherheit System						
Einstellungen						
Windows Defender Firewall	>					
Firewall- & Netzwerkschutz	>					
💣 Firewallstatus überprüfen	>					
Windows-Sicherheit	>					
Web durchsuchen						
🐖 Firewall	>					
	>					
℅ firewall kostenios	>					
$\mathcal P$ firewall ausschalten	>					
	>					
Dokumente - Dieser PC (1+)						

Schritt 2: Zulassen von Anwendungen durch die Windows Defender Firewall

Nachdem Sie die Windows Defender Firewall geöffnet haben, navigieren Sie nun zu den Einstellungen, mit denen Sie festlegen können, welche Programme und Dienste durch die Firewall kommunizieren dürfen.

Gehen Sie dabei wie folgt vor:

 Klicken Sie im linken Menü des Firewall-Fensters auf den Punkt "Eine App oder ein Feature durch die Windows Defender Firewall zulassen".

– Dieser Menüpunkt befindet sich in der Regel im linken Bereich des Fensters unterhalb der allgemeinen Firewall-Übersicht.

- 2. Es öffnet sich nun ein neues Fenster mit dem Titel "Zugelassene Apps".
 Hier sehen Sie eine Liste aller Programme und Dienste, die bereits für die Kommunikation durch die Firewall freigegeben wurden.
 – In dieser Liste können Sie sowohl private als auch öffentliche Netzwerkzugriffe einzeln konfigurieren.
- 3. Um Änderungen vornehmen zu können, klicken Sie zunächst oben rechts auf die Schaltfläche **"Einstellungen ändern"**.

– Möglicherweise erscheint eine Sicherheitsabfrage der Benutzerkontensteuerung, die Sie mit **"Ja"** bestätigen müssen.

Prindows Defender Firewall 🚽 🕐 🤺 🍻 🔹 Systemsteuerung 🔉 System und Sicherheit 🕉 Windows Defender Firewall Den PC mithilfe der Windows Defender Firewall schützen Startseite der Systemsteuerung Mithilfe der Windows Defender Firewall kann verhindert werden, dass Hacker oder Schadsoftware über das Eine App oder ein Feature Internet bzw. über ein Netzwerk Zugriff auf den PC erhalten. durch die Windows Defender Firewall zulassen 🤝 Domänennetzwerke Verbunden 🔿 Benachrichtigungseinstellungen ändern Netzwerke am Arbeitsplatz, die zu einer Domäne gehören Windows Defender Firewall ein- oder ausschalten Windows Defender Firewall-Zustand: Fin Standard wiederherstellen Eingehende Verbindungen: Alle Verbindungen mit Apps blockieren, die nicht in der Liste zugelassener Apps vorhanden sind 😌 Erweiterte Einstellungen Aktive Domänennetzwerke: syka.local Problembehandlung für Netzwerk Benachrichtigungsstatus: Benachrichtigen, wenn eine neue App von der Windows Defender Firewall blockiert wird Private Netzwerke Nicht verbunden 📀 🗸 Gast oder öffentliche Netzwerke Nicht verbunden

Kommunikation von Apps durch die Windows Defender Firewall zulassen

Klicken Sie zum Hinzufügen, Ändern oder Entfernen zugelassener Apps und Ports auf "Einstellungen ändern".

Welche Risiken bestehen, wenn die Kommunikation einer App zugelassen wird?

lame	Domäne	Privat	Öffentlich	1
SQL Browser Service EXE	\checkmark			
SQL Server Windows NT - 64 Bit				
✓ Starten		\checkmark	\checkmark	
✓ teams.exe				
✓ TeamViewer			\checkmark	
Teamviewer Remote Control Application				
Teamviewer Remote Control Service				
Tragbare Drahtlosgeräte				
🗹 Übermittlungsoptimierung		\checkmark	\checkmark	
Überwachung für virtuelle Computer				
☑ UX.Client.ST		\checkmark	\checkmark	
Veeam Networking		✓	✓	

Andere App zulassen...

🗣 Einstellungen ändern

Schritt 3: Anwendungen und Dienste für die Kommunikation durch die Firewall freigeben

In diesem Bereich haben Sie nun die Möglichkeit, gezielt festzulegen, welche Anwendungen und Dienste durch die Windows Defender Firewall kommunizieren dürfen. Dies ist besonders wichtig, wenn bestimmte Programme oder Serverdienste von anderen Rechnern im Netzwerk – in diesem Fall von den Arbeitsplätzen – erreichbar sein müssen.

Gerade in einer Server-Client-Umgebung, in der beispielsweise ein SQL-Server auf dem Server läuft, ist es unerlässlich, die dazugehörigen Dienste freizugeben. Andernfalls kann keine Verbindung vom Arbeitsplatzrechner zum Server hergestellt werden, da die Firewall den Datenverkehr blockiert.

Vorgehensweise:

1. Anwendung in der Liste suchen:

Überprüfen Sie zunächst, ob die benötigten Anwendungen bereits in der Liste der zugelassenen Programme vorhanden sind. Sollte dies nicht der Fall sein, können Sie sie manuell hinzufügen.

2. Anwendung manuell hinzufügen:

- a. Klicken Sie auf "Andere App zulassen …" (unten im Fenster).
- b. Wählen Sie anschließend den Button **"Durchsuchen …"**, um zur entsprechenden Datei zu navigieren.

3. Folgende Dienste müssen freigegeben werden:

Damit die Arbeitsplätze eine Verbindung zur SQL Server-Datenbank auf dem Server herstellen können, müssen Sie die folgenden ausführbaren Dateien manuell hinzufügen und sowohl für **private** als auch **öffentliche Netzwerke** freigeben:

a. SQL Server-Dienst:

C:\Program Files\Microsoft SQL

Server\MSSQL12.SYKA2014\MSSQL\Binn\sqlservr.exe

– Dies ist die zentrale Dienstdatei für die SQL Server-Instanz, die für den Datenbankbetrieb zuständig ist.

App hinzuf	ügen				×
Wählen Sie "Durchsuche klicken Sie a Apps:	die hinzuzufügende en", um nach einer n nschließend auf "OK	App aus, o hicht aufge (".	oder klicken Sie a listeten App zu s	uf uchen, und	
SQL Se	rver Windows NT - (64 Bit			
Pfad:	C:\Program Files\	/licrosoft S	QL Server 🕅 📘	Durchsuchen	
Welche Risike	en bestehen beim Au	ufheben de	er Blockierung eir	er App?	
Sie können auswählen, welchen Netzwerktypen diese App hinzugefügt wird.					
Netzv	verktypen		Hinzufügen	Abbreche	n

b. SQL Server Browser-Dienst:

C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe – Dieser Dienst ermöglicht es Client-Rechnern, die verfügbare(n) SQL Server-Instanz(en) im Netzwerk zu erkennen und sich mit ihnen zu verbinden.

App hinzufügen	×				
Wählen Sie die hinzuzufügende App aus, oder klicken Sie auf "Durchsuchen", um nach einer nicht aufgelisteten App zu suchen, und klicken Sie anschließend auf "OK".					
Apps:					
SQL Browser Service EXE					
Pfad: C:\Program Files (x86)\Microsoft SQL Sei Durchsuchen					
Welche Risiken bestehen beim Aufheben der Blockierung einer App?					
Sie können auswählen, welchen Netzwerktypen diese App hinzugefügt wird.					
Netzwerktypen Hinzufügen Abbreche	n				

4. Nach dem Hinzufügen:

- a. Stellen Sie sicher, dass beide Programme in der Liste aktiviert sind.
- b. Setzen Sie sowohl das H\u00e4kchen f\u00fcr das private als auch f\u00fcr das \u00f6ffentliche Netzwerk, falls Ihre Umgebung dies erfordert (z. B. in gemischten Netzwerken oder bei wechselnden Verbindungen).
- c. Klicken Sie abschließend auf "OK", um die Änderungen zu übernehmen.