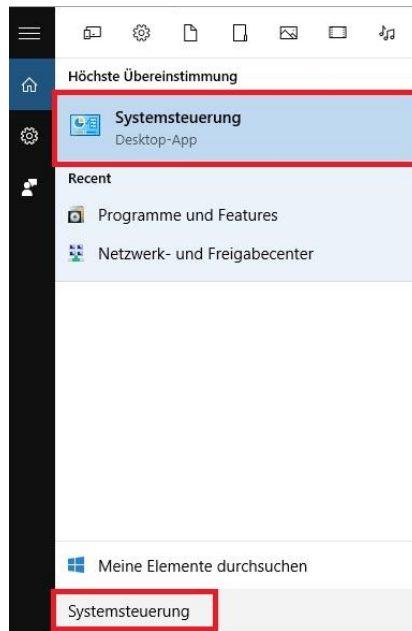


Firebird Port Freigabe - Firewall konfigurieren unter Windows 10

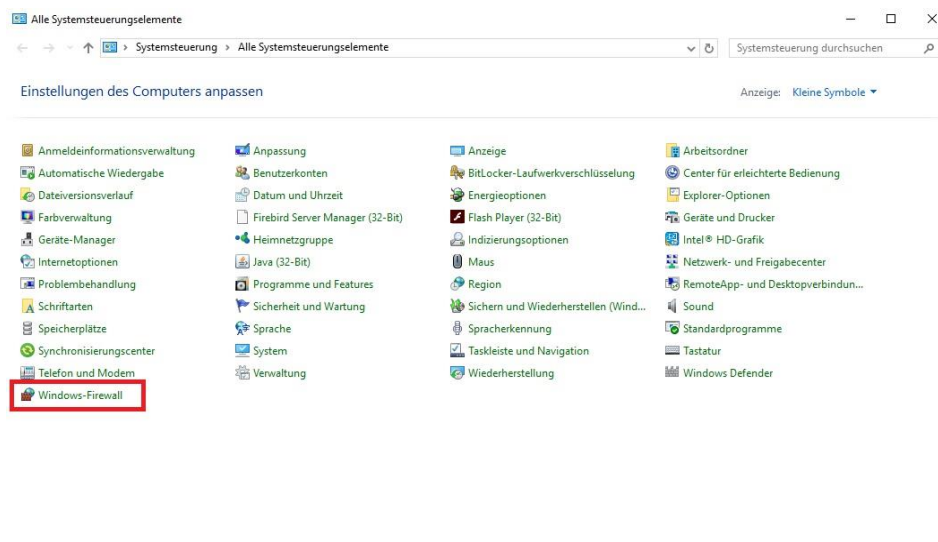
1. Klicken Sie auf das Lupen-Symbol in der Taskleiste von Windows 10.



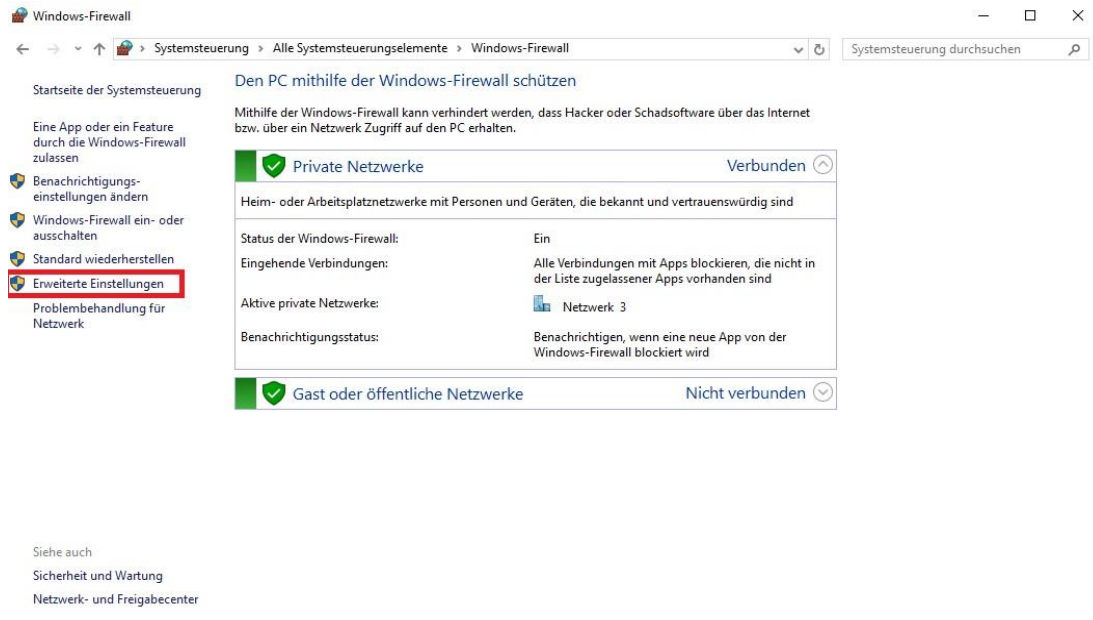
2. Geben Sie in das Suchfeld „Systemsteuerung“ ein und klicken Sie auf die sogenannte „Desktop-App“.



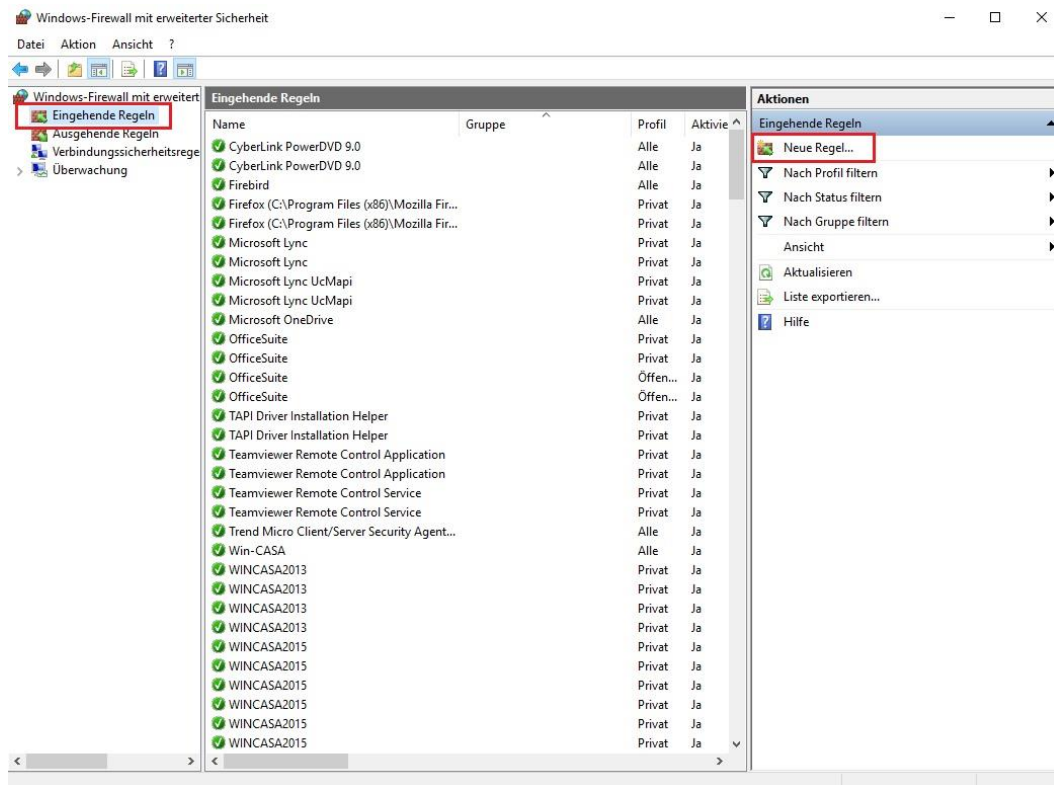
3. Klicken Sie im nachfolgenden Fenster auf „Windows-Firewall“.



4. Klicken Sie links auf „Erweiterte Einstellungen“:



5. Als Erstes muss links „Eingehende Regeln“ gewählt werden, dann „Neue Regel“:



6. Setzen Sie den Punkt bei „Port“:

Assistent für neue eingehende Regel

Regeltyp

Wählen Sie den Typ der zu erstellenden Firewallregel aus.

Schritte:

- Regeltyp
- Protokolle und Ports
- Aktion
- Profil
- Name

Welchen Regeltyp möchten Sie erstellen?

Programm
Regel, die die Verbindungen für ein Programm steuert.

Port
Regel, die die Verbindungen für einen TCP- oder UDP-Port steuert.

Vordefiniert:
"Auf Gerät abspielen"-Funktionalität
Regel, die die Verbindungen für einen Windows-Vorgang steuert.

Benutzerdefiniert
Benutzerdefinierte Regel

< Zurück Weiter > Abbrechen

7. Setzen Sie den Punkt bei „TCP“ und „Bestimmte lokale Ports“ und tragen Sie den Port „3050“ ein:

Assistent für neue eingehende Regel

Protokolle und Ports

Geben Sie die Protokolle und Ports an, für die diese Regel gilt.

Schritte:

- Regeltyp
- Protokolle und Ports
- Aktion
- Profil
- Name

Betrifft diese Regel TCP oder UDP?

TCP

UDP

Gilt diese Regel für alle lokalen Ports oder für bestimmte lokale Ports?

Alle lokalen Ports

Bestimmte lokale Ports: 3050
Beispiel: 80, 443, 5000-5010

< Zurück Weiter > Abbrechen

8. Setzen Sie den Punkt bei „Verbindung zulassen“:

Assistent für neue eingehende Regel ×

Aktion

Legen Sie die Aktion fest, die ausgeführt werden soll, wenn eine Verbindung die in der Regel angegebenen Bedingungen erfüllt.

Schritte:

- Regeltyp
- Protokolle und Ports
- **Aktion**
- Profil
- Name

Welche Aktion soll durchgeführt werden, wenn eine Verbindung die angegebenen Bedingungen erfüllt?

Verbindung zulassen
 Dies umfasst sowohl mit IPsec geschützte als auch nicht mit IPsec geschützte Verbindungen.

Verbindung zulassen, wenn sie sicher ist
 Dies umfasst nur mithilfe von IPsec authentifizierte Verbindungen. Die Verbindungen werden mit den Einstellungen in den IPsec-Eigenschaften und -regeln im Knoten "Verbindungssicherheitsregel" gesichert.

Verbindung blockieren

9. „Domäne“, „Privat“ und „Öffentlich“ bleibt angehakt:

Assistent für neue eingehende Regel ×

Profil

Geben Sie die Profile an, für die diese Regel zutrifft.

Schritte:

- Regeltyp
- Protokolle und Ports
- Aktion
- **Profil**
- Name

Wann wird diese Regel angewendet?

Domäne
 Wird angewendet, wenn ein Computer mit der Firmendomäne verbunden ist.

Privat
 Wird angewendet, wenn ein Computer mit einem privaten Netzwerk (z. B. zu Hause oder am Arbeitsplatz) verbunden ist.

Öffentlich
 Wird angewendet, wenn ein Computer mit einem öffentlichen Netzwerk verbunden ist.

10. Tragen Sie als Name „Firebird“ ein und beenden diesen Assistenten mit „Fertig stellen“:

Assistent für neue eingehende Regel

Name

Geben Sie den Namen und die Beschreibung dieser Regel an.

Schritte:

- Regeltyp
- Protokolle und Ports
- Aktion
- Profil
- Name

Name:
Firebird

Beschreibung (optional):

< Zurück Fertig stellen Abbrechen

11. Starten Sie dann Ihren Computer neu.