

ASV

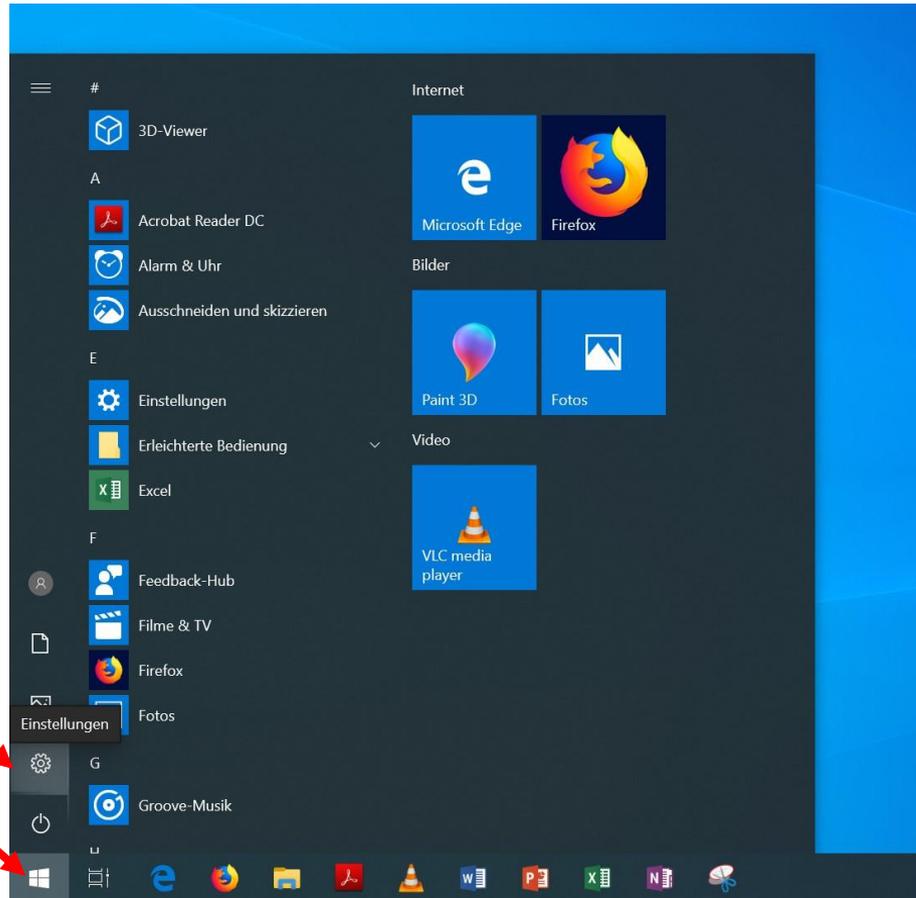
Installationsleitfaden für Förderschulen im Produktivbetrieb

Anpassungen der Windows-Firewall

Notwendigkeit:

- Befinden sich ASV-Server und –Client auf dem gleichen Rechner, besteht normalerweise keine Notwendigkeit, die Windows-Firewall anzupassen.
- Befinden sich die ASV-Clients auf anderen Rechnern, muss die Windows-Firewall aller Client-Rechner und des Server-Rechners entsprechend angepasst werden. (siehe folgende Anleitung)
- Befindet sich der ASV-Server in einem anderen Netzwerk, kann eine zusätzliche Anpassung der Firewalls in weiteren Geräten (z.B. Routern ...) notwendig sein.

1



Das Startmenü (Windows-Symbol)
öffnen und Einstellungen aufrufen.

2

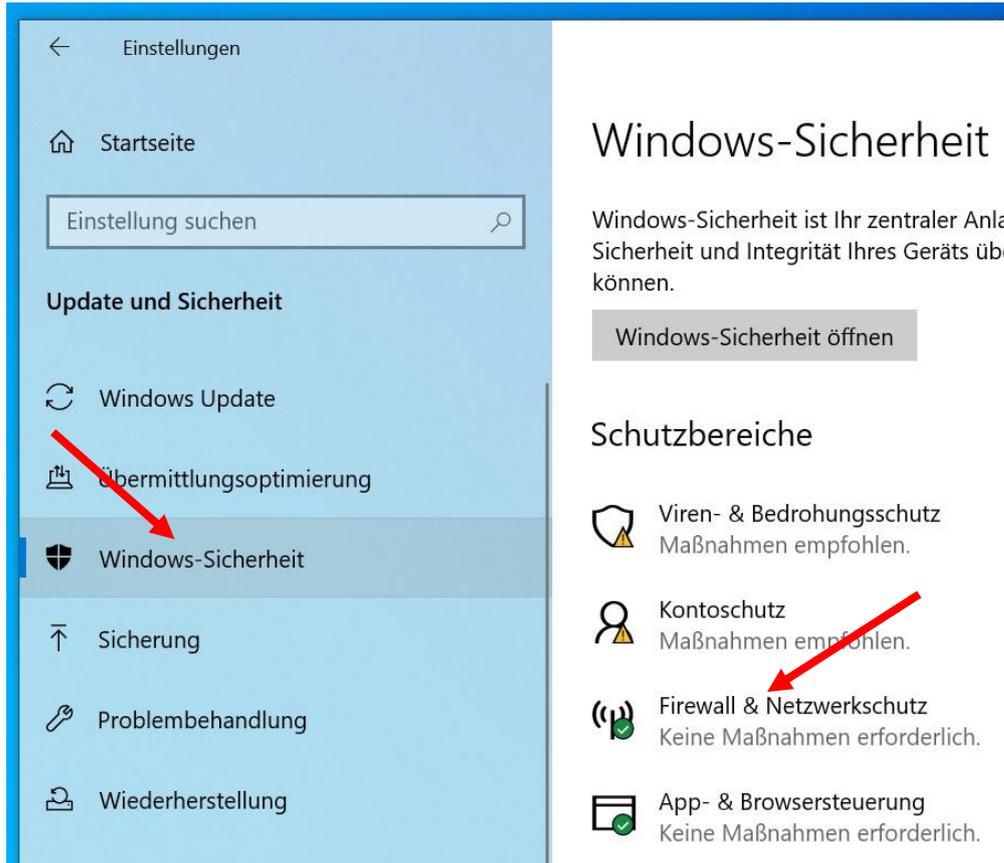
Einstellungen

- 
Personalisierung
 Hintergrund, Sperrbildschirm, Farben
- 
Apps
 Deinstallieren, Standardwerte, optionale Funktionen
- 
Konten
 Ihre Konten, E-Mail-Adresse, Synchronisieren, Arbeit, Familie
- 
Zeit und Sprache
 Spracherkennung, Region, Datum
- 
Spiele
 Spieleleiste, Aufzeichnungen, Übertragung, Spielemodus
- 
Erleichterte Bedienung
 Sprachausgabe, Bildschirmlupe, hoher Kontrast
- 
Suche
 Meine Dateien finden, Berechtigungen
- 
Cortana
 Cortana-Sprache, Berechtigungen, Benachrichtigungen
- 
Datenschutz
 Standort, Kamera, Mikrofon
- 
Update und Sicherheit
 Windows Update, Wiederherstellung, Sicherung

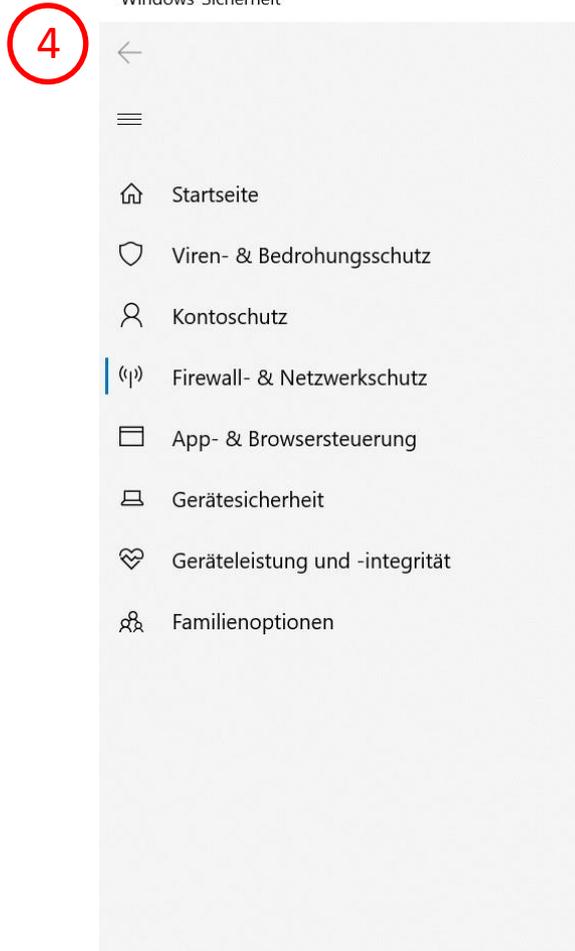
In den Einstellungen „Update und Sicherheit“ öffnen.



3



„Windows-Sicherheit“ auswählen und dann „Firewall & Netzwerkschutz“ öffnen.



Firewall- & Netzwerkschutz

Gibt an, wer und was auf Ihre Netzwerke zugreift

Domänennetzwerk

Firewall ist aktiviert.

Privates Netzwerk

Firewall ist aktiviert.

Öffentliches Netzwerk

Firewall ist aktiviert.

[Zugriff von App durch Firewall zulassen](#)

[Problembehandlung für Netzwerk und Internet](#)

[Einstellungen für Firewallbenachrichtigungen](#)

[Erweiterte Einstellungen](#)

[Standard für Firewalls wiederherstellen](#)

„Erweiterte Einstellungen“ öffnen.

5

The screenshot shows the Windows Defender Firewall with Advanced Security console. The left-hand navigation pane is expanded to show 'Ausgehende Regeln' (Outgoing Rules), which is highlighted with a red arrow. The main area displays a list of outgoing rules with columns for Name, Gruppe, Profil, Aktiviert, and Aktion. The right-hand pane shows the 'Aktionen' (Actions) menu, where 'Neue Regel...' (New Rule...) is highlighted with a red arrow.

Name	Gruppe	Profil	Aktiviert	Aktion
✓ "Wiedergabe auf Gerät"-Funktionalität (q...	"Wiedergabe auf Gerät"-Fun...	Privat,...	Ja	Zulasser
✓ "Wiedergabe auf Gerät"-Funktionalität (q...	"Wiedergabe auf Gerät"-Fun...	Privat,...	Ja	Zulasser
✓ "Wiedergabe auf Gerät"-Streamingserver (...)	"Wiedergabe auf Gerät"-Fun...	Privat	Ja	Zulasser
✓ "Wiedergabe auf Gerät"-Streamingserver (...)	"Wiedergabe auf Gerät"-Fun...	Öffen...	Ja	Zulasser
✓ "Wiedergabe auf Gerät"-Streamingserver (...)	"Wiedergabe auf Gerät"-Fun...	Domä...	Ja	Zulasser
✓ @{Microsoft.Windows.CloudExperienceHo...	@{Microsoft.Windows.Cloud...	Alle	Ja	Zulasser
✓ @{Microsoft.Windows.ContentDeliveryMa...	@{Microsoft.Windows.Conte...	Alle	Ja	Zulasser
✓ @{Microsoft.Windows.ShellExperienceHos...	@{Microsoft.Windows.Shelle...	Alle	Ja	Zulasser
✓ @FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	Alle	Ja	Zulasser
✓ 3D-Viewer	3D-Viewer	Alle	Ja	Zulasser
✓ AllJovn-Router (TCP aussehend)	AllJovn-Router	Domä...	Ja	Zulasser

Zunächst wird eine neue ausgehende Regel erstellt:

1. „Ausgehende Regel“ auswählen
2. „Neue Regel ...“ öffnen

6

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:**
"Wiedergabe auf Gerät"-Funktionalität
Regel, die die Verbindungen für einen Windows-Vorgang steuert.
- Benutzerdefiniert**
Benutzerdefinierte Regel

< Zurück

Weiter >

„Port“ auswählen, dann auf
„Weiter“ gehen.

7

Assistent für neue ausgehende 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 Remoteports oder für bestimmte Remoteports?

Alle Remoteports
 Bestimmte Remoteports:

Beispiel: 80, 443, 5000-5010

< Zurück **Weiter >**

„TCP“ auswählen, bei „Bestimmte Remoteports“ den Port „8765“ eingeben und dann auf „Weiter“ gehen.

8

Aktion

Wählen 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 sind mit den Einstellungen in den IPsec-Eigenschaften und -regeln im Knoten "Verbindungssicherheitsregel" gesichert.

Anpassen...

Verbindung blockieren

< Zurück Weiter >

„Verbindung zulassen“ auswählen und dann auf „Weiter“ gehen.

9

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.

< Zurück

Weiter >

Haken bei „Domäne“, „Privat“ und „Öffentlich“ setzen und dann auf „Weiter“ gehen.

10

Name

Geben Sie den Namen und die Beschreibung dieser Regel an.

Schritte:

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

Name:
ASV

Beschreibung (optional):
Port 8765 für Kommunikation zwischen ASV-Server und -Clients|

< Zurück Fertig stellen

Der Regel einen aussagekräftigen Namen und eine Beschreibung geben und dann auf „Fertig stellen“ gehen.

11



Dann wird noch eine neue eingehende Regel erstellt:

1. „Eingehende Regeln“ auswählen
2. „Neue Regel ...“ öffnen

12

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:**
"Wiedergabe auf Gerät"-Funktionalität
Regel, die die Verbindungen für einen Windows-Vorgang steuert.
- Benutzerdefiniert**
Benutzerdefinierte Regel

< Zurück

Weiter >

„Port“ auswählen, dann auf
„Weiter“ gehen.

13

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:

Beispiel: 80, 443, 5000-5010

< Zurück

Weiter >

„TCP“ auswählen, bei „Bestimmte lokale Ports“ den Port „8765“ eingeben und dann auf „Weiter“ gehen.

14

Aktion

Wählen 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 mit den Einstellungen in den IPsec-Eigenschaften und -regeln im Knoten "Verbindungssicherheitsregel" gesichert.

[Anpassen...](#) **Verbindung blockieren**

< Zurück

Weiter >

„Verbindung zulassen“ auswählen und dann auf „Weiter“ gehen.

15

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.

< Zurück Weiter >

Haken bei „Domäne“, „Privat“ und „Öffentlich“ setzen und dann auf „Weiter“ gehen.

16

Name

Geben Sie den Namen und die Beschreibung dieser Regel an.

Schritte:

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

Name:
ASV

Beschreibung (optional):
Port 8765 für Kommunikation zwischen ASV-Server und -Clients|

< Zurück Fertig stellen

Der Regel einen aussagekräftigen Namen und eine Beschreibung geben und dann auf „Fertig stellen“ gehen.

Wenn der Zugriff dann immer noch nicht funktioniert, den Rechner neu starten.