COMPLETED BY JARINAT KAREEM

# Splunk Alert Project: Detecting Failed Logins on Windows Server

## 1. Project Overview

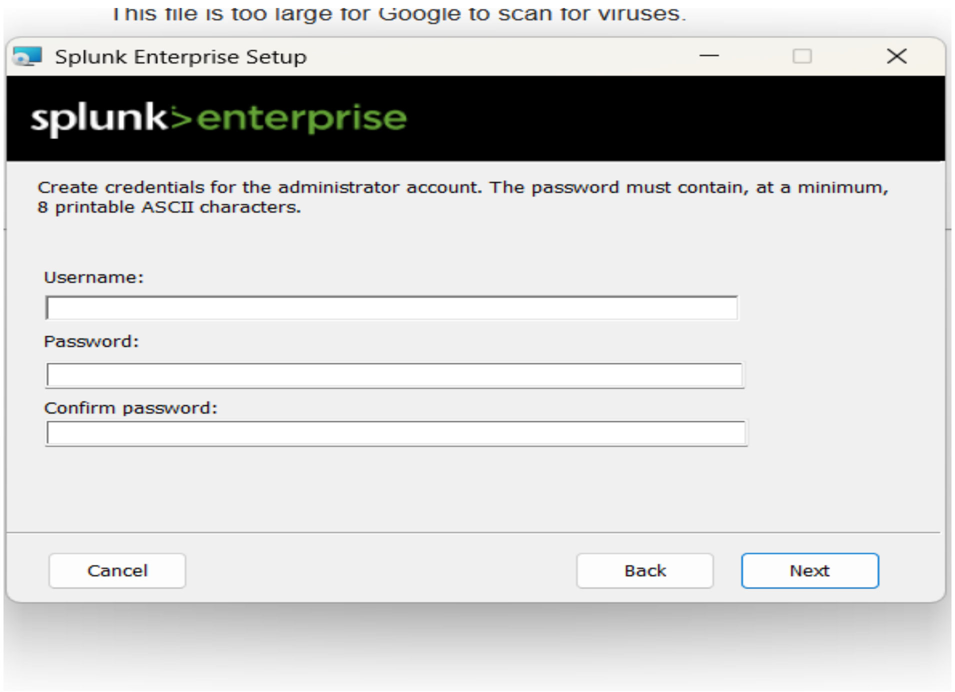
This project demonstrates how to create and trigger a security alert in Splunk Enterprise using data collected from a Windows Server via the Splunk Universal Forwarder. The alert identifies multiple failed login attempts (Event ID 4625), which can be indicative of brute-force attacks or unauthorized access attempts.

## 2. Architecture & Setup

- Splunk Universal Forwarder installed on Windows Server.
- Splunk Enterprise installed on Host PC.
- Forwarder configured to send Windows Security logs to Splunk Enterprise.
- Data indexed under 'main' index with sourcetype 'WinEventLog:Security'.

## 3. Objective

Trigger an alert when more than 5 failed login attempts (EventCode 4625) occur within a 10-minute window.


This file is too large for Google to scan for viruses.

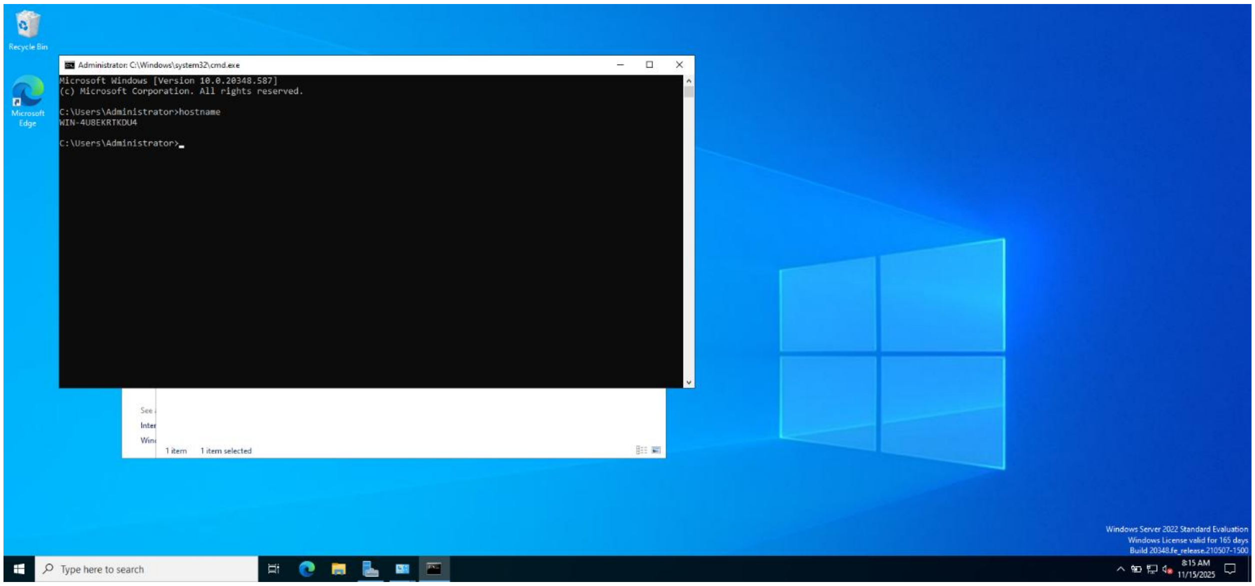
Splunk Enterprise Setup

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:

Password:

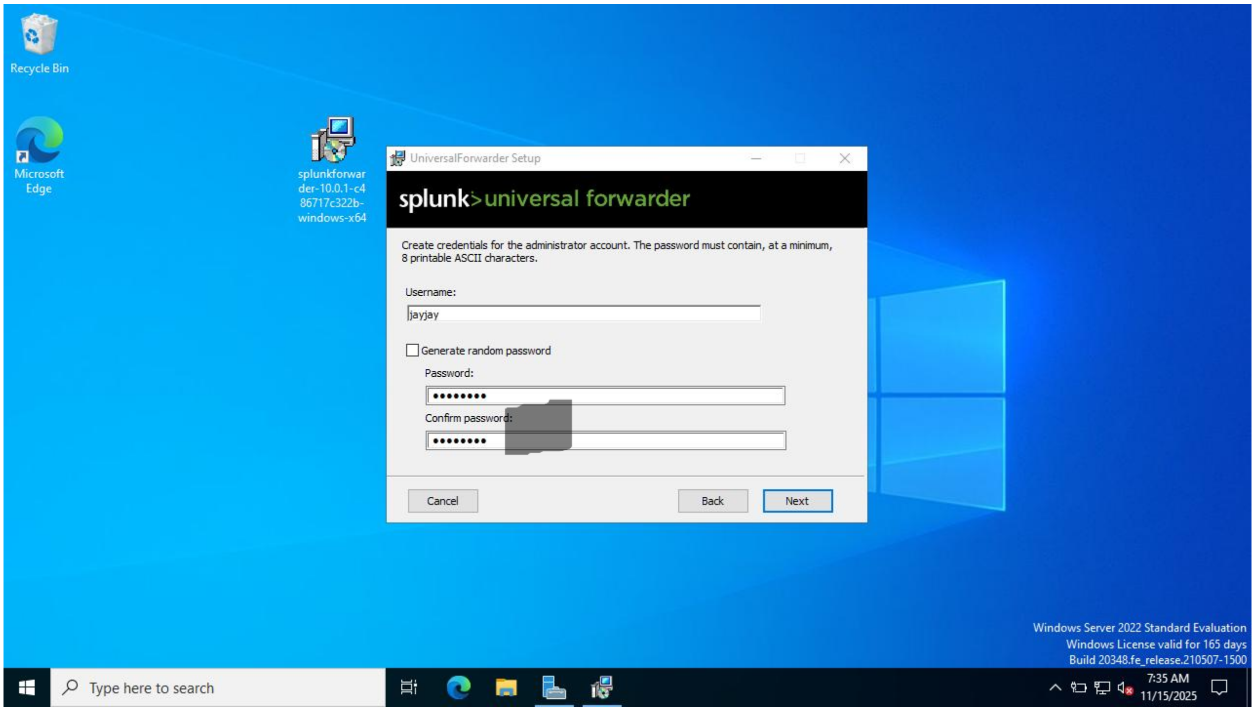
Confirm password:


Administrator: C:\Windows\system32\cmd.exe
Recycle Bin
Microsoft Edge
1 item
1 item selected
Type here to search
Windows Server 2022 Standard Evaluation
Windows License valid for 165 days
Build 20348.fe_release.210507-1500
8:15 AM
11/15/2025

```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>hostname
WIN-4U8EKRTKDU4

C:\Users\Administrator>_
```


Recycle Bin
Microsoft Edge
splunkforwarder-10.0.1-c486717c322b-windows-x64
UniversalForwarder Setup
splunk>universal forwarder
Cancel
Back
Next
Type here to search
Windows Server 2022 Standard Evaluation
Windows License valid for 165 days
Build 20348.fe_release.210507-1500
7:35 AM
11/15/2025

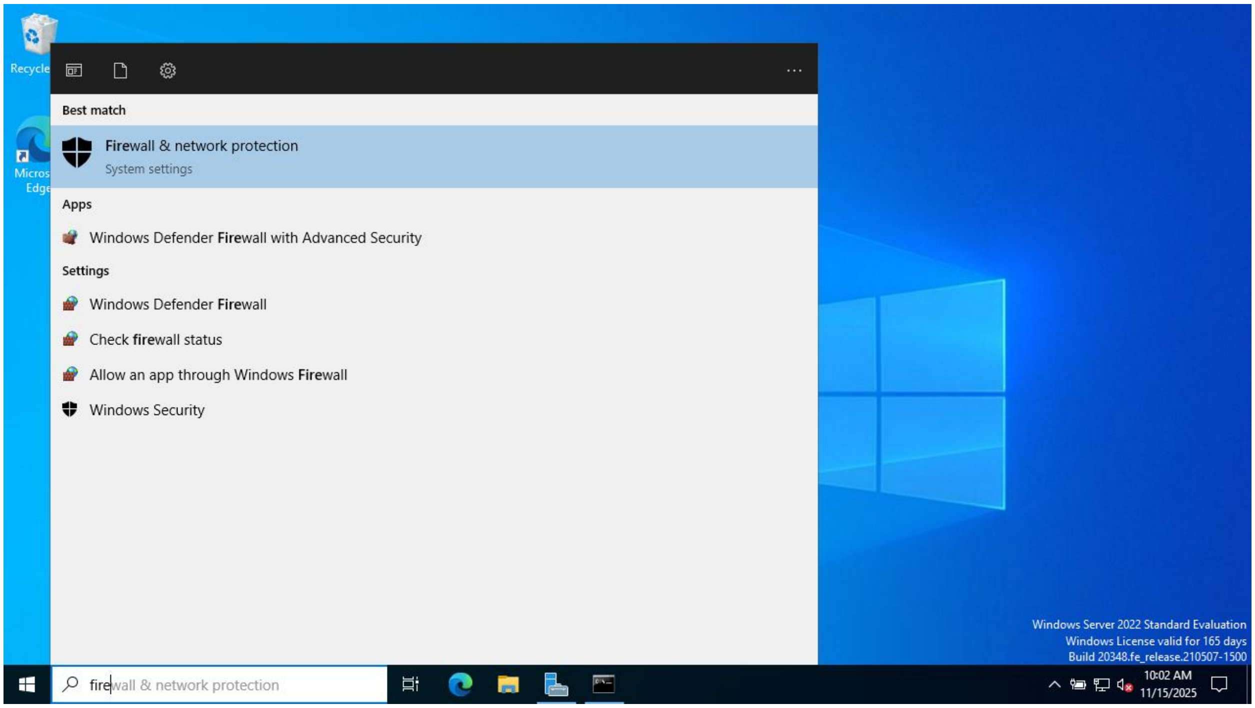
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username: jayjay

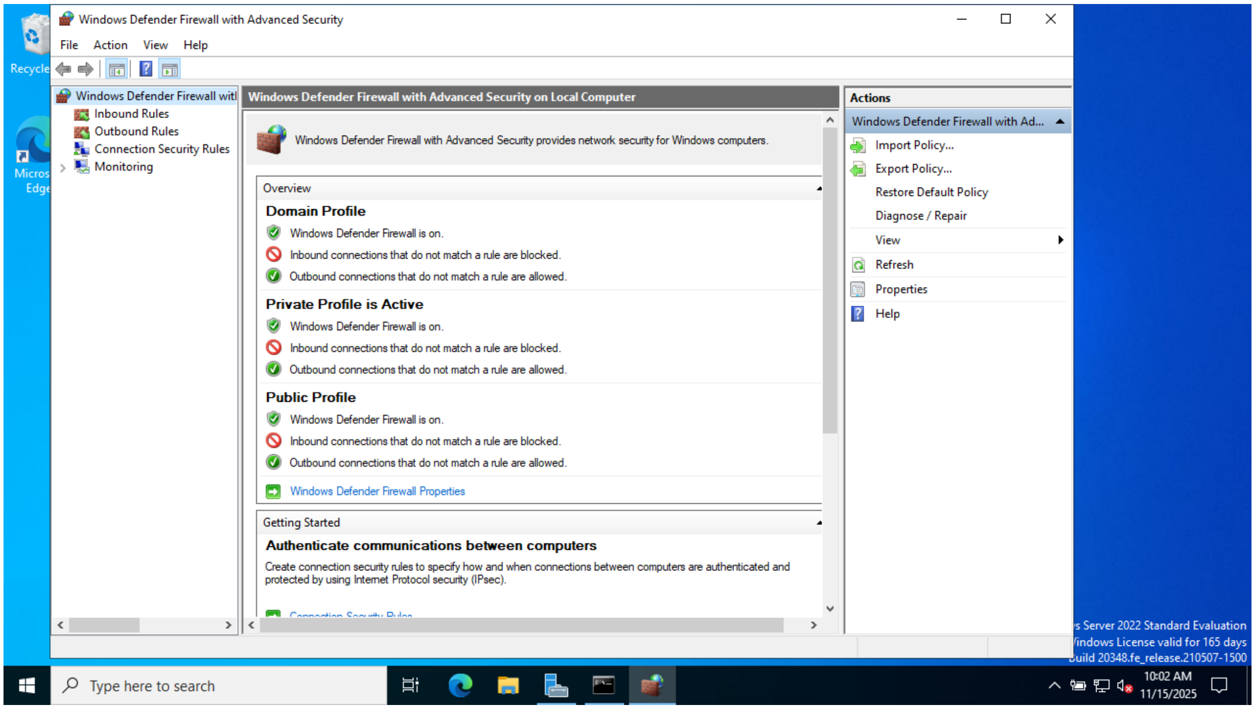
□ Generate random password

Password: ••••••••

Confirm password: ••••••••


Recycle
Microsoft Edge
Best match
Firewall & network protection
System settings
Apps
Windows Defender Firewall with Advanced Security
Settings
Windows Defender Firewall
Check firewall status
Allow an app through Windows Firewall
Windows Security
Windows Server 2022 Standard Evaluation
Windows License valid for 165 days
Build 20348.fe_release.210507-1500
10:02 AM
11/15/2025

firewall & network protection


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Overview
Actions
Windows Defender Firewall with Ad...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
Getting Started
Connection Security Rules
Windows Server 2022 Standard Evaluation
Windows License valid for 165 days
Build 20348.fe_release.210507-1500
Type here to search
10:02 AM
11/15/2025

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

**Domain Profile**

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

**Private Profile is Active**

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

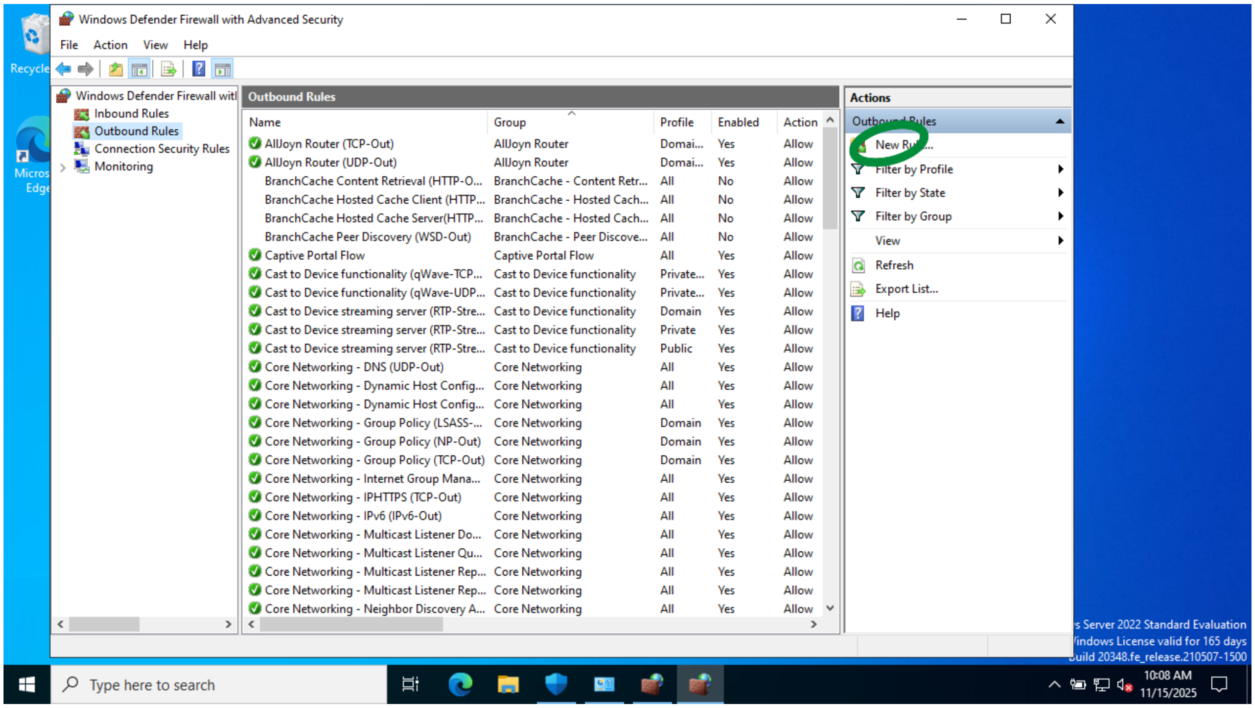
**Public Profile**

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

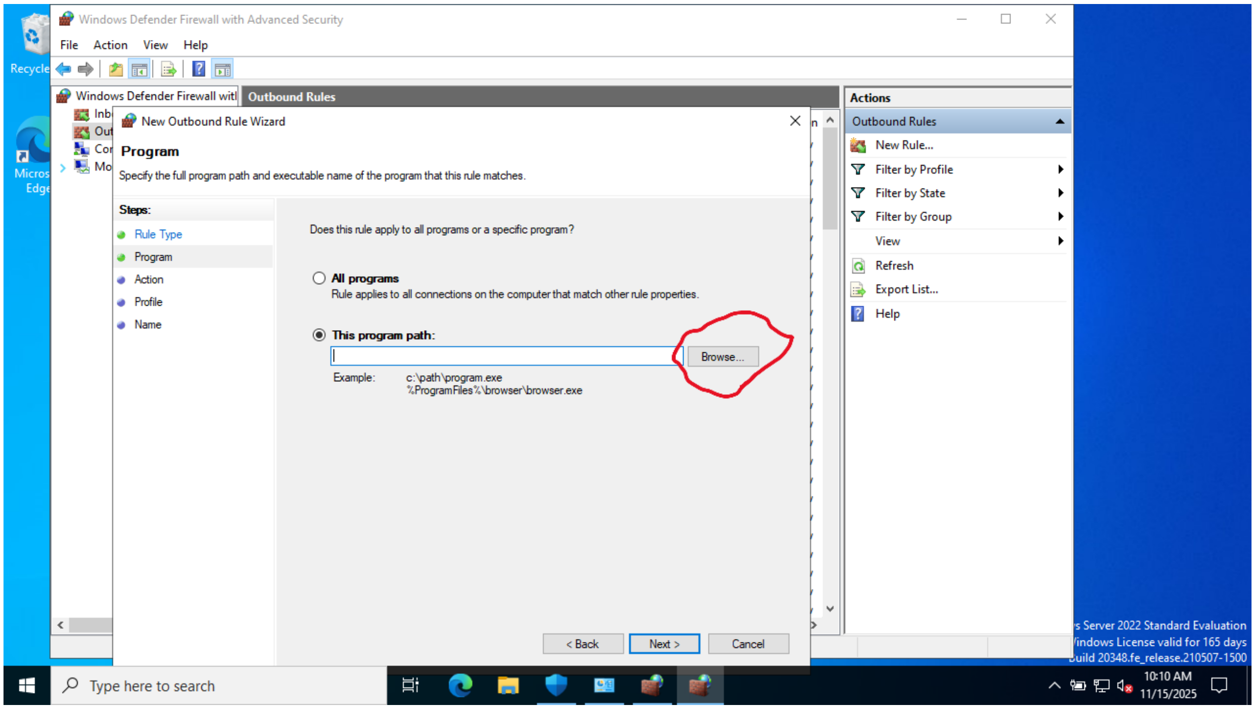
**Authenticate communications between computers**

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).



Outbound Rules

| Name | Group | Profile | Enabled | Action |
|---|---|---|---|---|
| AllJoyn Router (TCP-Out) | AllJoyn Router | Domai... | Yes | Allow |
| AllJoyn Router (UDP-Out) | AllJoyn Router | Domai... | Yes | Allow |
| BranchCache Content Retrieval (HTTP-O... | BranchCache - Content Retr... | All | No | Allow |
| BranchCache Hosted Cache Client (HTTP... | BranchCache - Hosted Cach... | All | No | Allow |
| BranchCache Hosted Cache Server(HTTP... | BranchCache - Hosted Cach... | All | No | Allow |
| BranchCache Peer Discovery (WSD-Out) | BranchCache - Peer Discove... | All | No | Allow |
| Captive Portal Flow | Captive Portal Flow | All | Yes | Allow |
| Cast to Device functionality (qWave-TCP... | Cast to Device functionality | Private... | Yes | Allow |
| Cast to Device functionality (qWave-UDP... | Cast to Device functionality | Private... | Yes | Allow |
| Cast to Device streaming server (RTP-Stre... | Cast to Device functionality | Domain | Yes | Allow |
| Cast to Device streaming server (RTP-Stre... | Cast to Device functionality | Private | Yes | Allow |
| Cast to Device streaming server (RTP-Stre... | Cast to Device functionality | Public | Yes | Allow |
| Core Networking - DNS (UDP-Out) | Core Networking | All | Yes | Allow |
| Core Networking - Dynamic Host Config... | Core Networking | All | Yes | Allow |
| Core Networking - Dynamic Host Config... | Core Networking | All | Yes | Allow |
| Core Networking - Group Policy (LSASS-... | Core Networking | Domain | Yes | Allow |
| Core Networking - Group Policy (NP-Out) | Core Networking | Domain | Yes | Allow |
| Core Networking - Group Policy (TCP-Out) | Core Networking | Domain | Yes | Allow |
| Core Networking - Internet Group Mana... | Core Networking | All | Yes | Allow |
| Core Networking - IPHTTPS (TCP-Out) | Core Networking | All | Yes | Allow |
| Core Networking - IPv6 (IPv6-Out) | Core Networking | All | Yes | Allow |
| Core Networking - Multicast Listener Do... | Core Networking | All | Yes | Allow |
| Core Networking - Multicast Listener Qu... | Core Networking | All | Yes | Allow |
| Core Networking - Multicast Listener Rep... | Core Networking | All | Yes | Allow |
| Core Networking - Multicast Listener Rep... | Core Networking | All | Yes | Allow |
| Core Networking - Neighbor Discovery A... | Core Networking | All | Yes | Allow |



New Outbound Rule Wizard

**Program**

Specify the full program path and executable name of the program that this rule matches.

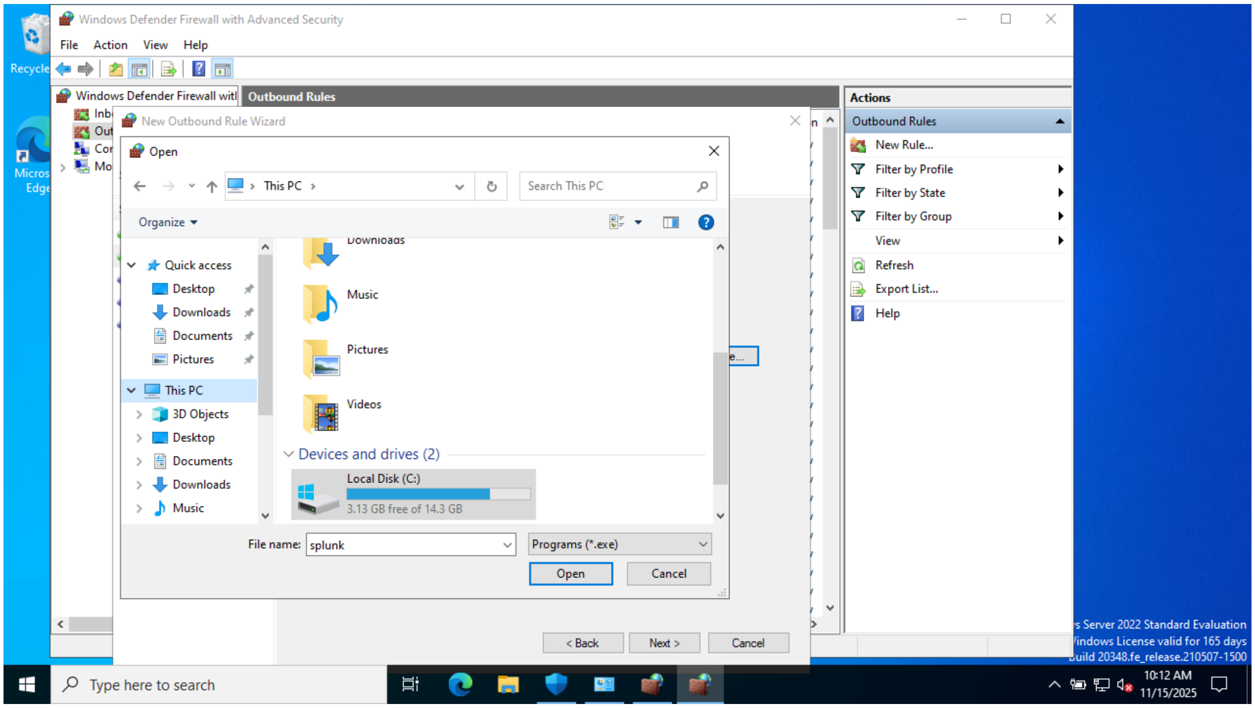
Steps:
- Rule Type
- Program
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

○ **All programs**
Rule applies to all connections on the computer that match other rule properties.

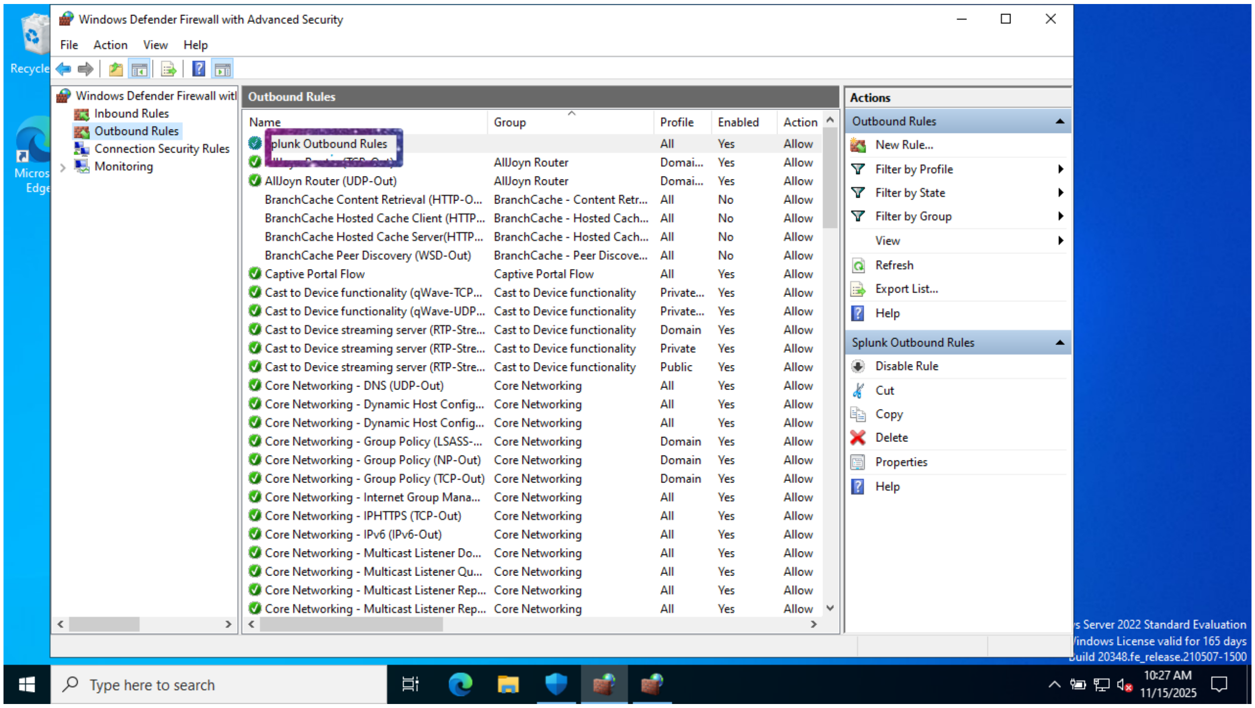
● **This program path:**
[ ] Browse...

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe



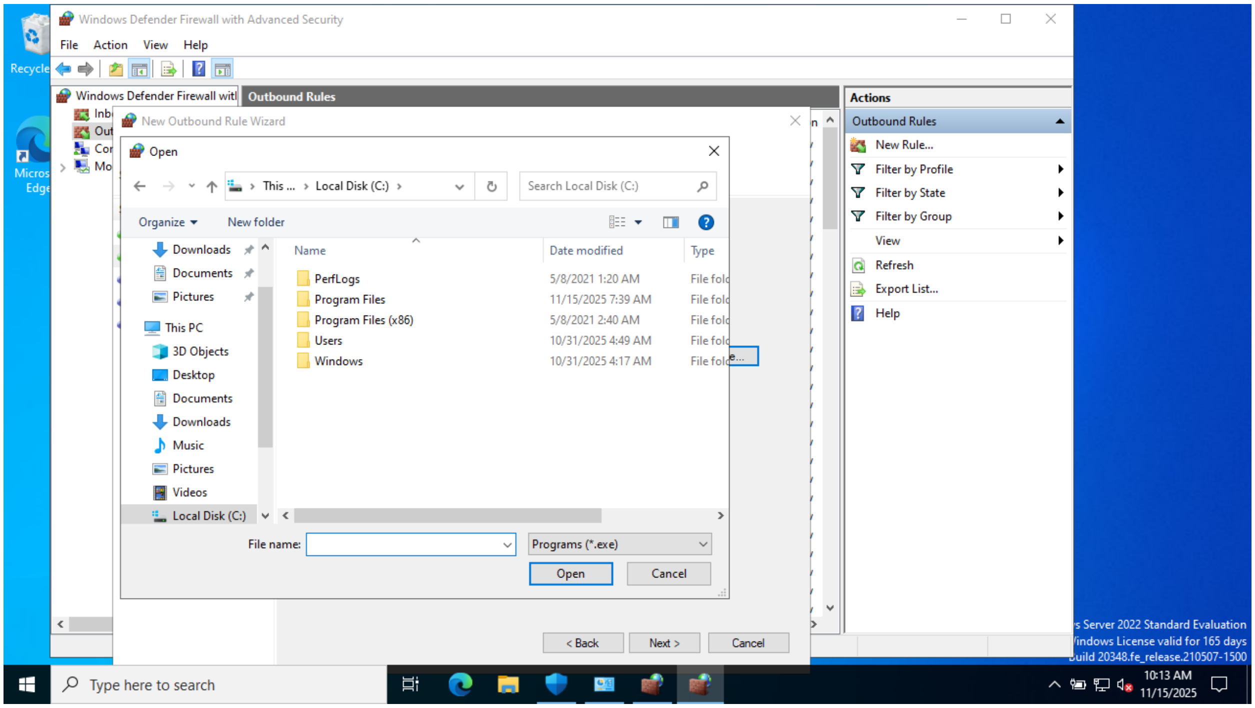
File name: splunk

Programs (*.exe)



Outbound Rules

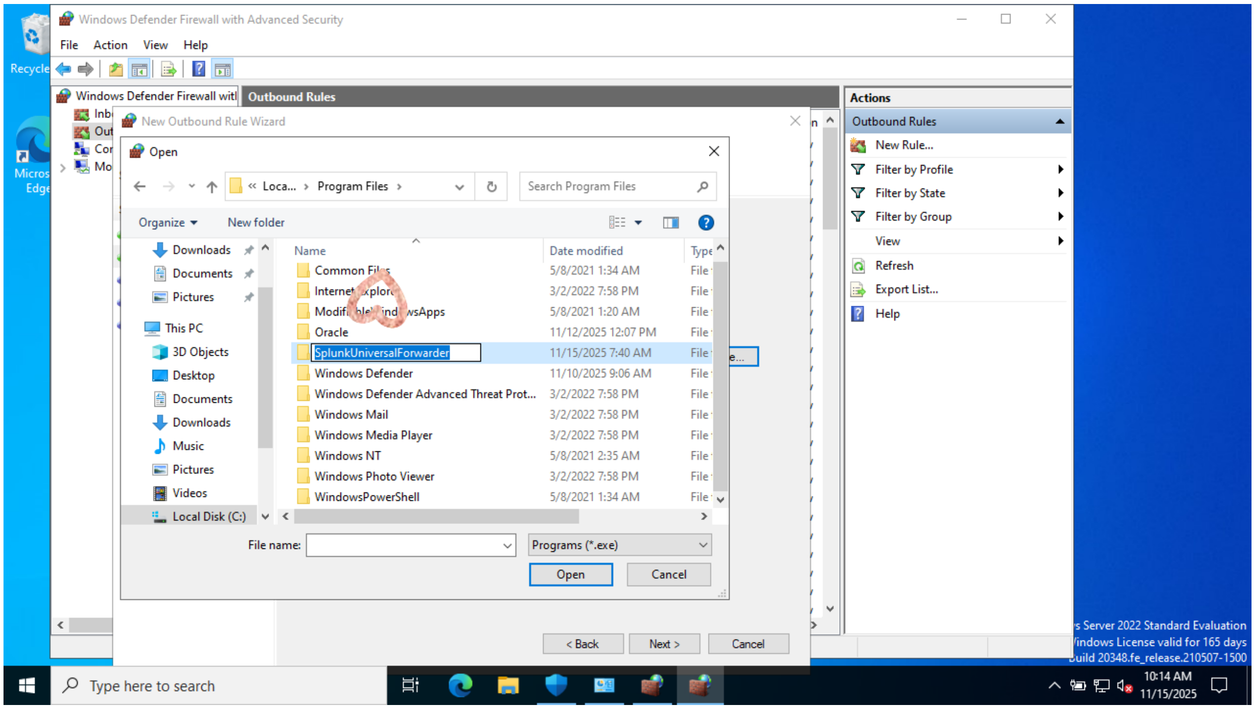
| Name | Group | Profile | Enabled | Action |
|---|---|---|---|---|
| ✓ plunk Outbound Rules | | All | Yes | Allow |
| ✓ AllJoyn Router (TCP-Out) | AllJoyn Router | Domai... | Yes | Allow |
| ✓ AllJoyn Router (UDP-Out) | AllJoyn Router | Domai... | Yes | Allow |
| BranchCache Content Retrieval (HTTP-O... | BranchCache - Content Retr... | All | No | Allow |
| BranchCache Hosted Cache Client (HTTP... | BranchCache - Hosted Cach... | All | No | Allow |
| BranchCache Hosted Cache Server(HTTP... | BranchCache - Hosted Cach... | All | No | Allow |
| BranchCache Peer Discovery (WSD-Out) | BranchCache - Peer Discove... | All | No | Allow |
| ✓ Captive Portal Flow | Captive Portal Flow | All | Yes | Allow |
| ✓ Cast to Device functionality (qWave-TCP... | Cast to Device functionality | Private... | Yes | Allow |
| ✓ Cast to Device functionality (qWave-UDP... | Cast to Device functionality | Private... | Yes | Allow |
| ✓ Cast to Device streaming server (RTP-Stre... | Cast to Device functionality | Domain | Yes | Allow |
| ✓ Cast to Device streaming server (RTP-Stre... | Cast to Device functionality | Private | Yes | Allow |
| ✓ Cast to Device streaming server (RTP-Stre... | Cast to Device functionality | Public | Yes | Allow |
| ✓ Core Networking - DNS (UDP-Out) | Core Networking | All | Yes | Allow |
| ✓ Core Networking - Dynamic Host Config... | Core Networking | All | Yes | Allow |
| ✓ Core Networking - Dynamic Host Config... | Core Networking | All | Yes | Allow |
| ✓ Core Networking - Group Policy (LSASS-... | Core Networking | Domain | Yes | Allow |
| ✓ Core Networking - Group Policy (NP-Out) | Core Networking | Domain | Yes | Allow |
| ✓ Core Networking - Group Policy (TCP-Out) | Core Networking | Domain | Yes | Allow |
| ✓ Core Networking - Internet Group Mana... | Core Networking | All | Yes | Allow |
| ✓ Core Networking - IPHTTPS (TCP-Out) | Core Networking | All | Yes | Allow |
| ✓ Core Networking - IPv6 (IPv6-Out) | Core Networking | All | Yes | Allow |
| ✓ Core Networking - Multicast Listener Do... | Core Networking | All | Yes | Allow |
| ✓ Core Networking - Multicast Listener Qu... | Core Networking | All | Yes | Allow |
| ✓ Core Networking - Multicast Listener Rep... | Core Networking | All | Yes | Allow |
| ✓ Core Networking - Multicast Listener Rep... | Core Networking | All | Yes | Allow |



| Name | Date modified | Type |
|---|---|---|
| PerfLogs | 5/8/2021 1:20 AM | File fold |
| Program Files | 11/15/2025 7:39 AM | File fold |
| Program Files (x86) | 5/8/2021 2:40 AM | File fold |
| Users | 10/31/2025 4:49 AM | File fold |
| Windows | 10/31/2025 4:17 AM | File fold |

File name:

Programs (*.exe)

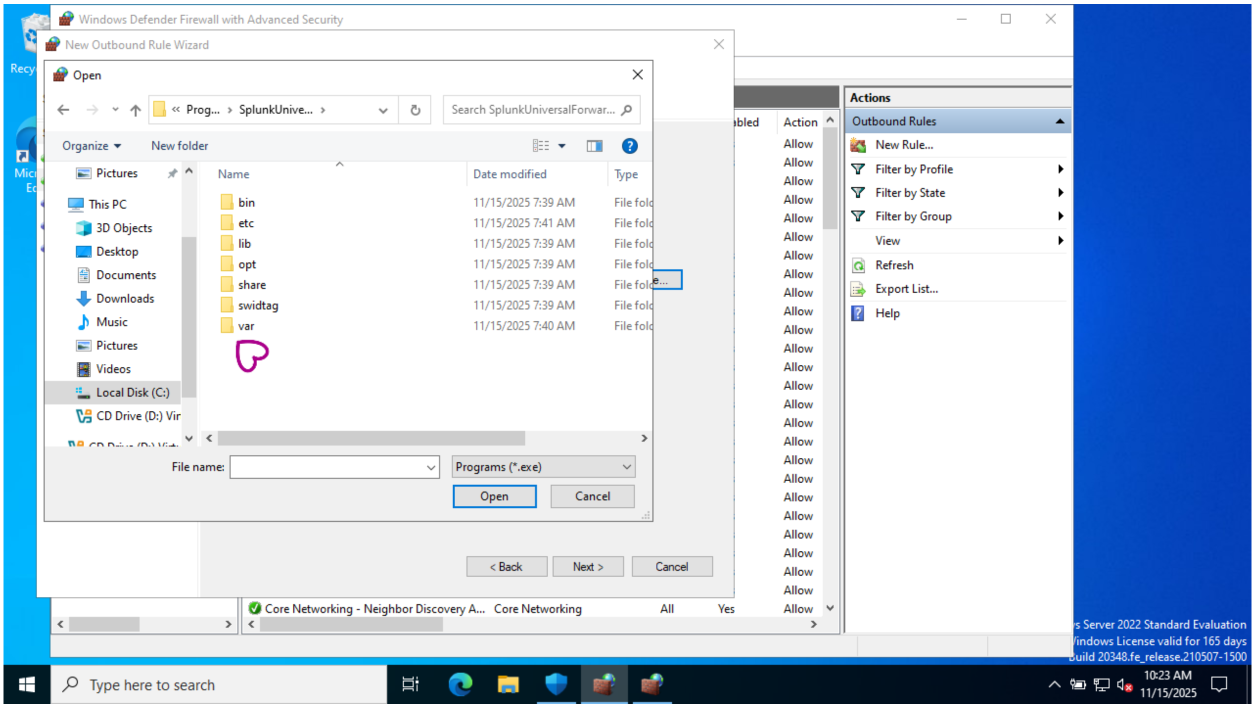


| Name | Date modified | Type |
|---|---|---|
| Common Files | 5/8/2021 1:34 AM | File |
| Internet Explorer | 3/2/2022 7:58 PM | File |
| ModifiableWindowsApps | 5/8/2021 1:20 AM | File |
| Oracle | 11/12/2025 12:07 PM | File |
| SplunkUniversalForwarder | 11/15/2025 7:40 AM | File |
| Windows Defender | 11/10/2025 9:06 AM | File |
| Windows Defender Advanced Threat Prot... | 3/2/2022 7:58 PM | File |
| Windows Mail | 3/2/2022 7:58 PM | File |
| Windows Media Player | 3/2/2022 7:58 PM | File |
| Windows NT | 5/8/2021 2:35 AM | File |
| Windows Photo Viewer | 3/2/2022 7:58 PM | File |
| WindowsPowerShell | 5/8/2021 1:34 AM | File |

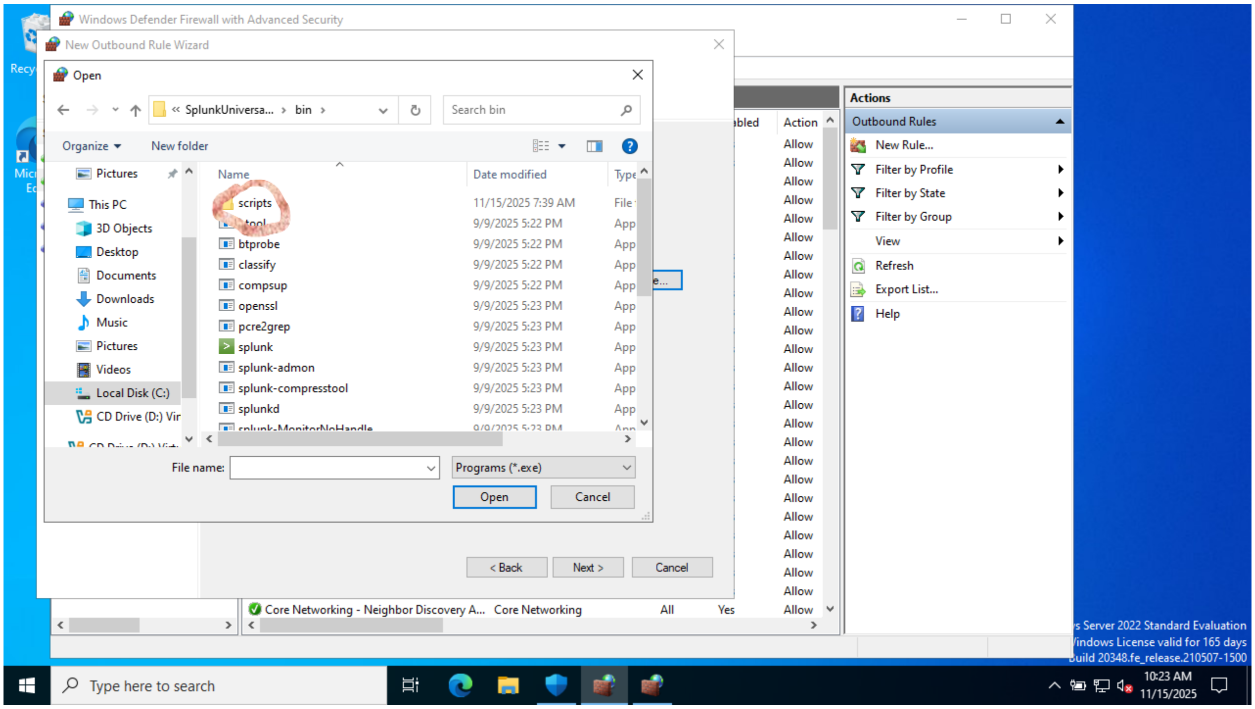
File name:

Programs (*.exe)

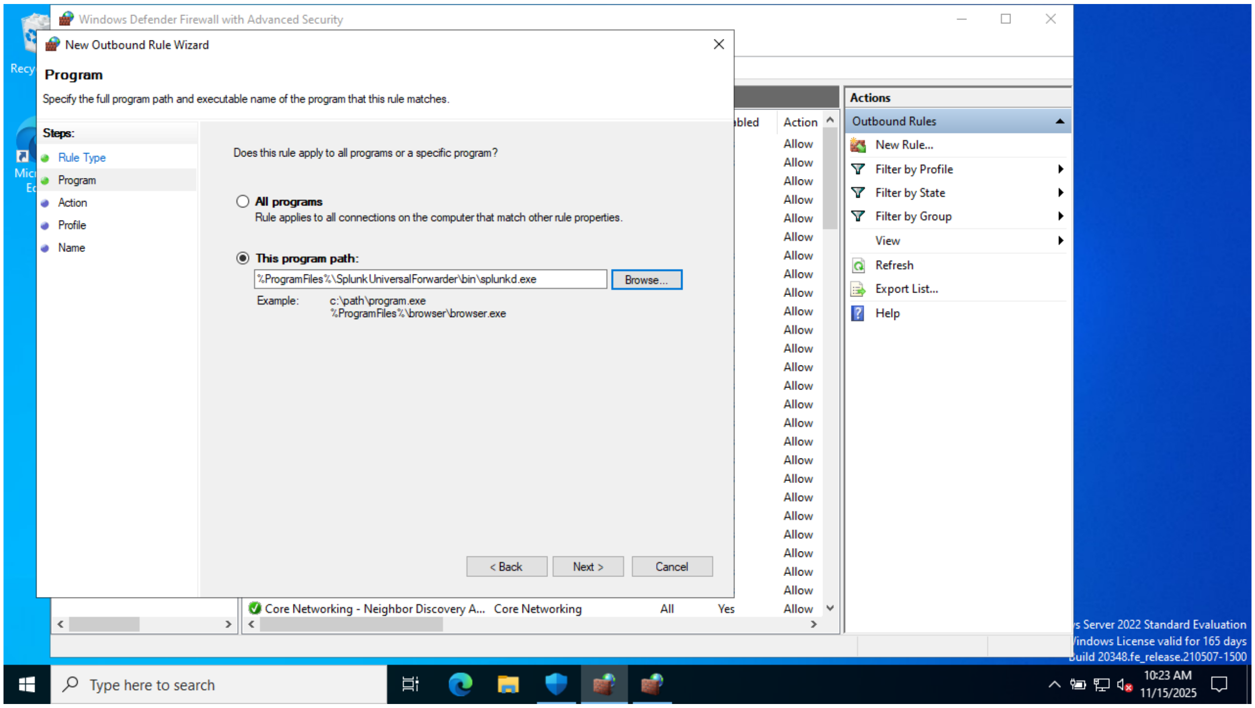
-



| Name | Date modified | Type |
|---|---|---|
| bin | 11/15/2025 7:39 AM | File fold |
| etc | 11/15/2025 7:41 AM | File fold |
| lib | 11/15/2025 7:39 AM | File fold |
| opt | 11/15/2025 7:39 AM | File fold |
| share | 11/15/2025 7:39 AM | File fold |
| swidtag | 11/15/2025 7:39 AM | File fold |
| var | 11/15/2025 7:40 AM | File fold |



| Name | Date modified | Type |
|---|---|---|
| scripts | 11/15/2025 7:39 AM | File |
| tool | 9/9/2025 5:22 PM | App |
| btprobe | 9/9/2025 5:22 PM | App |
| classify | 9/9/2025 5:22 PM | App |
| compsup | 9/9/2025 5:22 PM | App |
| openssl | 9/9/2025 5:23 PM | App |
| pcre2grep | 9/9/2025 5:23 PM | App |
| splunk | 9/9/2025 5:23 PM | App |
| splunk-admon | 9/9/2025 5:23 PM | App |
| splunk-compresstool | 9/9/2025 5:23 PM | App |
| splunkd | 9/9/2025 5:23 PM | App |
| splunk-MonitorNoHandle | 9/9/2025 5:23 PM | App |



Windows Defender Firewall with Advanced Security

New Outbound Rule Wizard

**Program**

Specify the full program path and executable name of the program that this rule matches.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

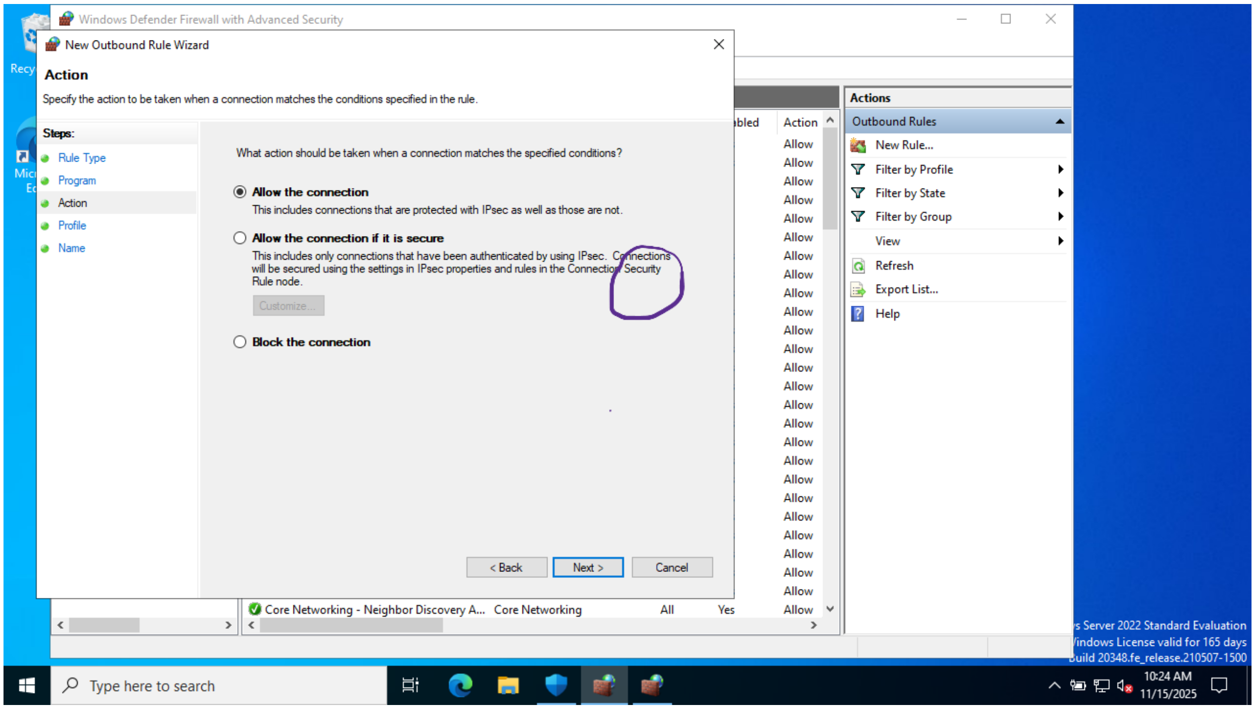
○ **All programs**
Rule applies to all connections on the computer that match other rule properties.

● **This program path:**
%ProgramFiles%\SplunkUniversalForwarder\bin\splunkd.exe [Browse...]

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

< Back | Next > | Cancel

Core Networking - Neighbor Discovery A... | Core Networking | All | Yes | Allow



Windows Defender Firewall with Advanced Security

New Outbound Rule Wizard

**Action**

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

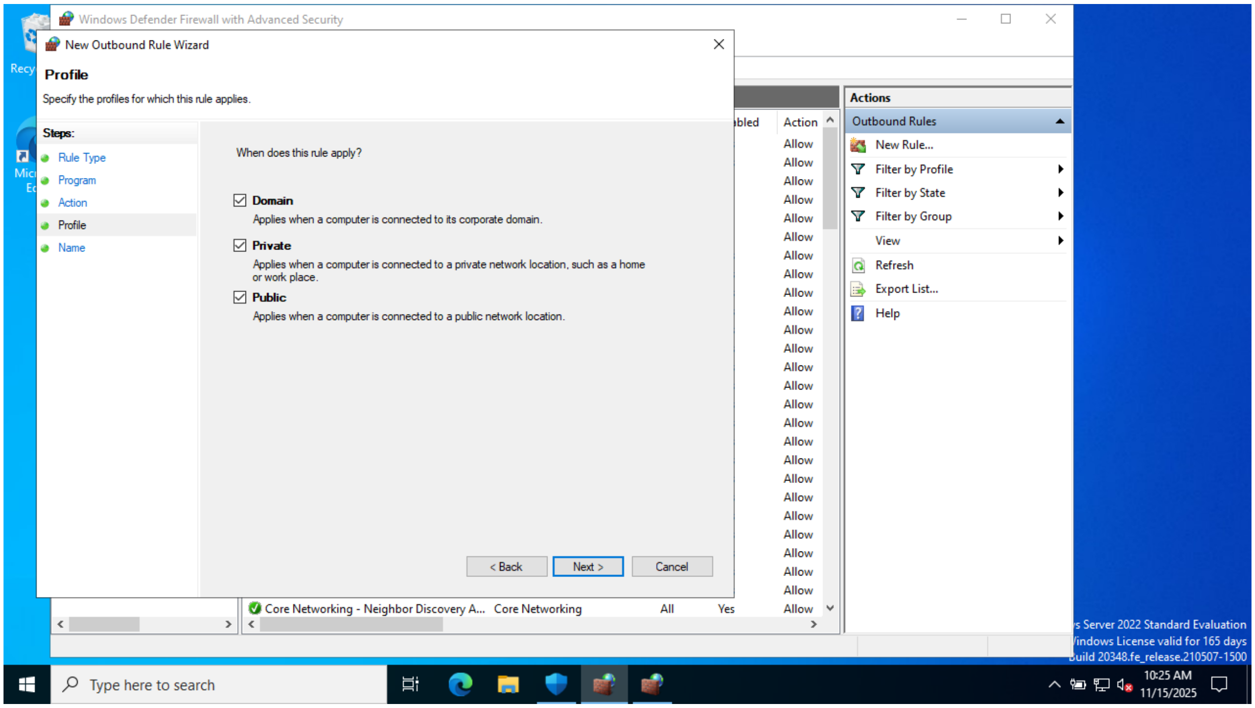
● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...]

○ **Block the connection**

< Back | Next > | Cancel

Core Networking - Neighbor Discovery A... | Core Networking | All | Yes | Allow



New Outbound Rule Wizard

**Profile**

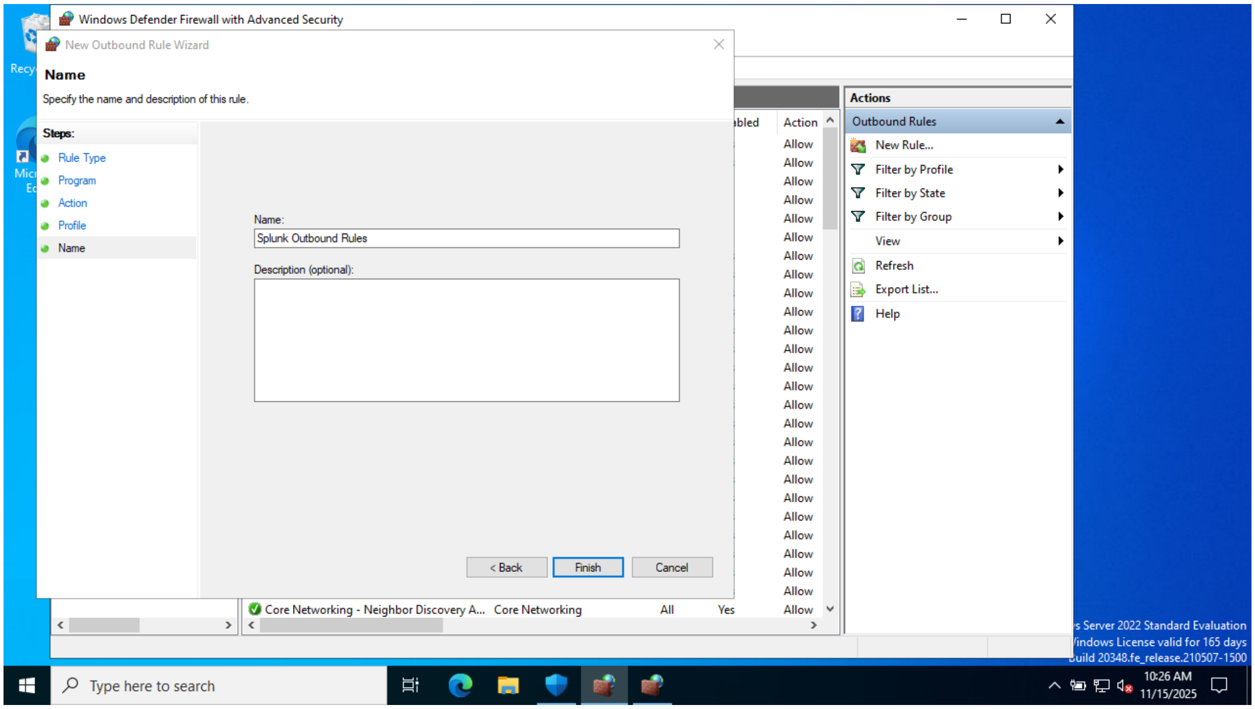
Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.



New Outbound Rule Wizard

**Name**

Specify the name and description of this rule.

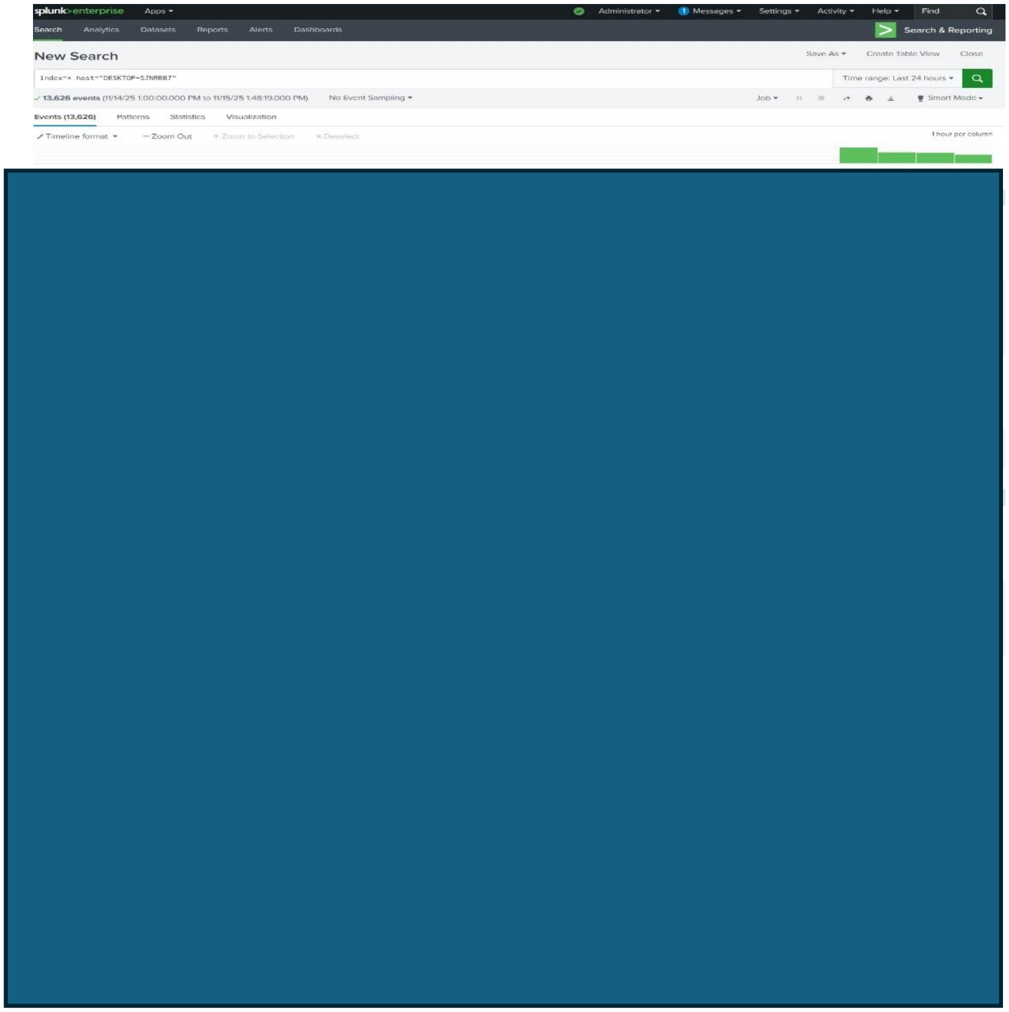
Name:
Splunk Outbound Rules

Description (optional):

## 4. Splunk Search Query

The following SPL query was used to detect failed login attempts:

```
index=main sourcetype=WinEventLog:Security EventCode=4625
| stats count by Account_Name, host
| where count > 5
```



New Search

```
index=* host="DESKTOP-5JNRBB7"
```

Time range: Last 24 hours

✓ 13,626 events (11/14/25 1:00:00.000 PM to 11/15/25 1:48:19.000 PM)  No Event Sampling

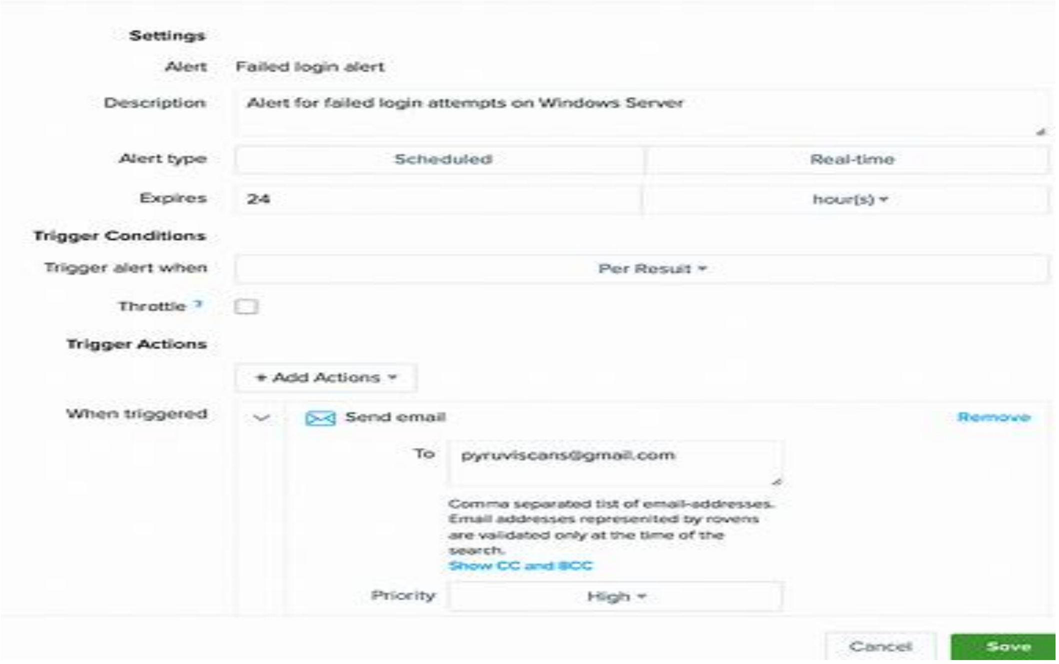
Events (13,626)

[redacted]

## 5. Alert Configuration

- Title: Failed Logins Alert
- Type: Scheduled Alert (Every 10 minutes)
- Time Range: Last 10 minutes

- Trigger Condition: Number of results > 0
- Trigger Actions: Send Email (Configured via SMTP in Splunk Settings)



Settings

Alert: Failed login alert

Description: Alert for failed login attempts on Windows Server

Alert type: Scheduled | Real-time

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Per Result

Throttle: □

Trigger Actions

When triggered: Send email

To: pyruviscans@gmail.com

Comma separated tist of email-addresses. Email addresses represenited by rovens are validated only at the time of the search.

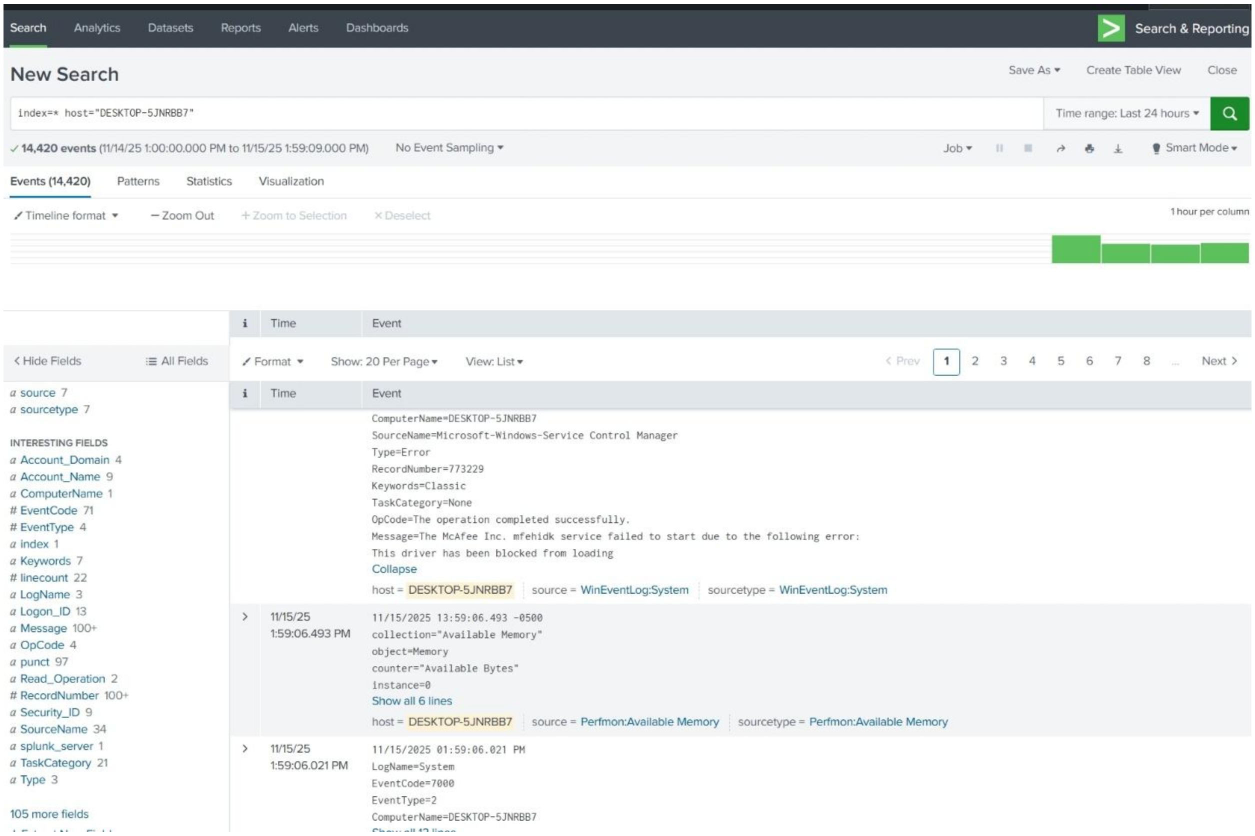
Priority: High

### 6. Simulating the Alert

To simulate real-world conditions, failed login attempts were manually triggered on the Windows Server using the `runas` command with incorrect credentials. This ensured multiple Event ID 4625 logs were generated and forwarded to Splunk for processing.

### 7. Validation & Output

The alert was successfully triggered after 6 failed login attempts. It appeared in the 'Triggered Alerts' section of Splunk and an email notification was received, confirming successful detection and response.



```
index=* host="DESKTOP-5JNRBB7"
```

✓ 14,420 events (11/14/25 1:00:00.000 PM to 11/15/25 1:59:09.000 PM)

| | |
|---|---|
| a source | 7 |
| a sourcetype | 7 |
| INTERESTING FIELDS | |
| a Account_Domain | 4 |
| a Account_Name | 9 |
| a ComputerName | 1 |
| # EventCode | 71 |
| # EventType | 4 |
| a index | 1 |
| a Keywords | 7 |
| # linecount | 22 |
| a LogName | 3 |
| a Logon_ID | 13 |
| a Message | 100+ |
| a OpCode | 4 |
| a punct | 97 |
| a Read_Operation | 2 |
| # RecordNumber | 100+ |
| a Security_ID | 9 |
| a SourceName | 34 |
| a splunk_server | 1 |
| a TaskCategory | 21 |
| a Type | 3 |

105 more fields

| i | Time | Event |
|---|---|---|
| | | ComputerName=DESKTOP-5JNRBB7<br>SourceName=Microsoft-Windows-Service Control Manager<br>Type=Error<br>RecordNumber=773229<br>Keywords=Classic<br>TaskCategory=None<br>OpCode=The operation completed successfully.<br>Message=The McAfee Inc. mfehidk service failed to start due to the following error:<br>This driver has been blocked from loading<br>Collapse<br>host = DESKTOP-5JNRBB7 source = WinEventLog:System sourcetype = WinEventLog:System |
| > | 11/15/25<br>1:59:06.493 PM | 11/15/2025 13:59:06.493 -0500<br>collection="Available Memory"<br>object=Memory<br>counter="Available Bytes"<br>instance=0<br>Show all 6 lines<br>host = DESKTOP-5JNRBB7 source = Perfmon:Available Memory sourcetype = Perfmon:Available Memory |
| > | 11/15/25<br>1:59:06.021 PM | 11/15/2025 01:59:06.021 PM<br>LogName=System<br>EventCode=7000<br>EventType=2<br>ComputerName=DESKTOP-5JNRBB7 |

## 8. Conclusion

This project demonstrates the practical use of Splunk for real-time log monitoring and alerting.