

Security Edge Filter Installation Guide



Contributors

Content architect: Rui Maximo

Writers: Fabian Kunz, Rui Maximo

Editor: Kelly Fuller Blue

Published: March 11, 2016

© MB Corporation 2018. All rights reserved.

This document is the intellectual property of MB Corporation. Neither duplication nor distribution is allowed without written permission of MB Corporation. No distribution outside the customer's organization is allowed.

Security Edge Filter, Security Web Filter, Security Federation Filter, Security Authorization Filter, Security Sync Filter and Security Filter Manager are copyrights of MB Corporation.

All trademarked names in this document are the property of their respective owners.

Security-Filters.com/Lync-Solutions.com operates under the legal entity "MB Corporation", and is incorporated in the State of Washington.

MB Corporation, by publishing this document, does not guarantee that any information contained herein is and will remain accurate or that use of the information will ensure correct and faultless operation of the relevant service or equipment. MB Corporation, its agents and employees shall not be held liable to or through any user for any loss or damage whatsoever results from relying on the information contained herein.

Nothing in this document is intended to and does not alter the legal obligations, responsibilities, or relationship between you and MB Corporation as set out in the contract existing between you and MB Corporation. MB Corporation will not be liable for any compliance or technical information provided herein.

This document is provided "as-is." The information and views expressed in this document, including URL and other Internet website references, may change without notice.

Information in the examples in this document is fictitious and is only for illustration. No actual association or connection is in any way intended or should be inferred.

Table of contents

1 Security Edge Filter Enterprise Edition 5

2 Security Concern 5

3 Solution 5

4 Security Edge Filter 7

4.1 Register Security Edge Filter 7

4.2 Create a Service Account 8

4.3 Install Security Edge Filter 10

4.4 Security Edge Filter in Action 13

4.5 Troubleshooting 16

1 Security Edge Filter Enterprise Edition

The Security Edge Filter Enterprise Edition is a security solution to protect Skype for Business Servers and Active Directory Directory Services accounts from external attacks targeting the Edge Server. The Enterprise Edition is designed for customers who have multiple instances of Edge Servers, and who want to centralize the lockout count across all instances of Security Edge Filter and Security Web Filter. The Security Edge Filter is installed on every Edge Server.

2 Security Concern

When customers expose their Skype for Business Server (formerly Lync Server) infrastructure to the Internet by deploying Edge Servers, they expose their Skype for Business Server environment in the internal corporate network and Active Directory Directory Services accounts to external attacks. This puts their users and Skype for Business Servers at risk from Denial of Service (DoS), Distributed Denial of Service (DDoS), and brute-force password attacks as shown in Figure 2 1.

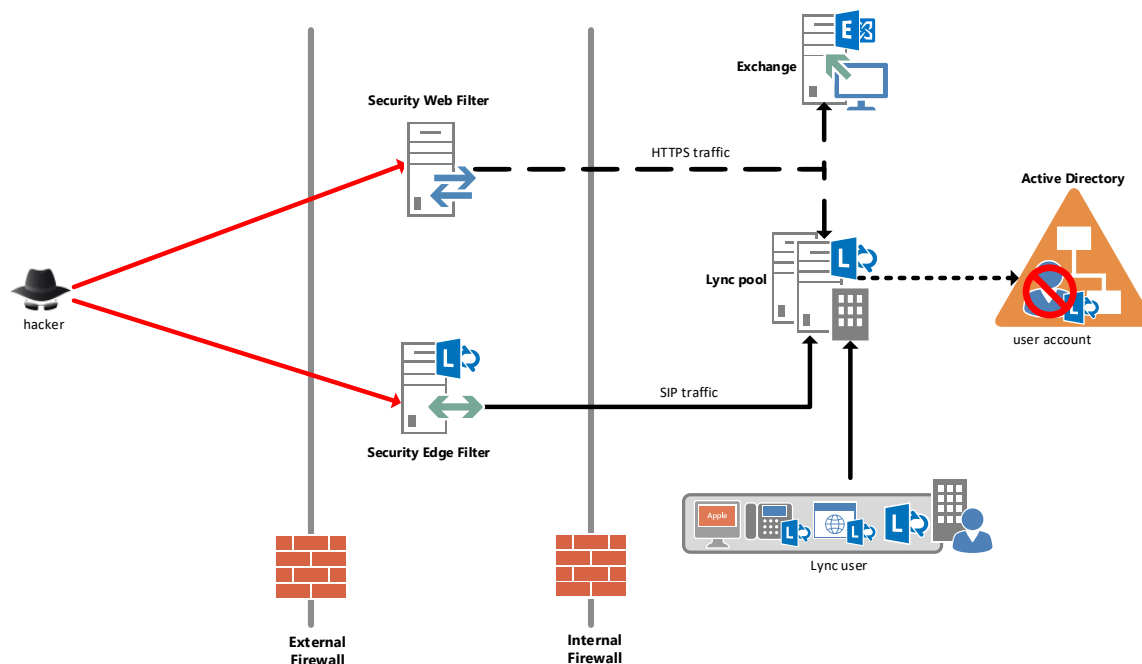


Figure 2.1 Users and Skype for Business Servers that are potentially at risk

3 Solution

The Active Edge Protection solution protects against Active Directory Directory Services account lockout attacks by scanning all incoming unauthenticated traffic. It scans all incoming SIP traffic going through the Edge Server and HTTPS traffic going through the reverse proxy. This solution's architecture consists of the following components:

- Security Edge Filter

- Security Web Filter
- Security Filter Manager

Here's how it all works:

- The Security Edge Filter is designed to track denied authentication attempts and block further login attempts before the Active Directory Directory Services lockout limit is reached.
- The lockout gives you one more tier of account security, safely locking the account out of the extranet.
- Security Filters prevent password-guessing on the extranet by blocking authentication attempts for that account after the number of failed authentication attempts reaches a threshold.
- Even when an Active Directory user account is locked out at the network perimeter by the Security Filters, the employee can still log in to their Active Directory account from within the corporate network or through a VPN. The DoS risk is substantially mitigated, without much inconvenience.
- Security Filters can require external users to log in to Skype for Business Server from a corporate domain-joined computer.
- When the Security Filters are configured to block Windows NT LAN Manager (NTLM) authentication and enforce the whitelist, remote users must sign in to Skype for Business Server from a domain-joined computer without preventing Skype for Business Mobile clients from signing in.

The Security Edge Filter tracks the number of failed login attempts from remote users. When the number of failed login attempts exceeds the administrator's specified threshold, the Security Edge Filter blocks all further login attempts until the lockout period expires or the administrator unlocks the account. The Security Filter Manager centralizes the number of failed login attempts, configuration settings, and logging information across all instances of the Security Edge Filters and Security Web Filters, and provides an administrative web interface that visualizes metrics captured by the Security Filters.

Figure 3.1 illustrates the architecture of the Active Edge Protection solution.

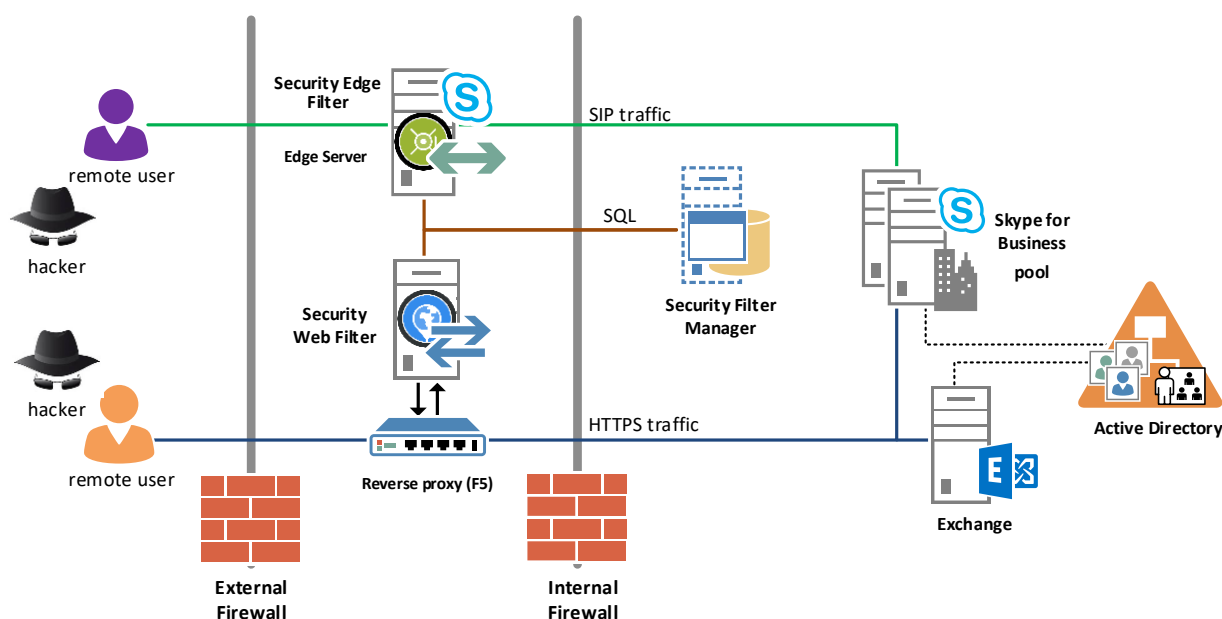


Figure 3.1 Active Edge Protection architecture

4 Security Edge Filter

After the Security Filter Manager is installed and configured, you can continue installing the Security Edge Filter on all your Edge Servers in your site. You must install an instance of the Security Filter Manager per site (that is, per data center). The Security Edge Filter protects the SIP traffic to your Skype for Business Servers.

4.1 Register Security Edge Filter

Before you can install the Security Edge Filter, you must first register the application with your Edge Server or with your Edge pool. You only need to complete this registration once. Run the following Skype for Business PowerShell cmdlets with Skype for Business Server administrative permissions.

1. From a Front End Server, specify the fully qualified domain name (FQDN) of the internal edge of the Edge pool in the parameter, <internal Edge FQDN>, where the Security Edge Filter will be installed.

Important: Keep the -uri parameter value set to "http://www.lync-solutions.com/security_filter" (include the quotation marks).

```
new-CsServerApplication -identity "EdgeServer:<internal Edge FQDN>/security_filter" -uri "http://www.lync-solutions.com /security_filter" -critical $false
```

1. Run the following cmdlet to initiate the replication of Central Management Store configuration to the Edge Server.

```
invoke-CsManagementStoreReplication
```

2. From a Front End Server, specify the FQDN of the internal edge of the Edge pool in the parameter <internal Edge FQDN>.

```
Set-CsServerApplication -Identity "service:<internal Edge FQDN>/security_filter"  
-Enabled $true
```

4.2 Create a Service Account

A service account is required to run the Security Edge Filter service. Create a local user account on the Edge Server, and then make this account a member of the **RTC Server Applications** local group (see Figure 4.1).

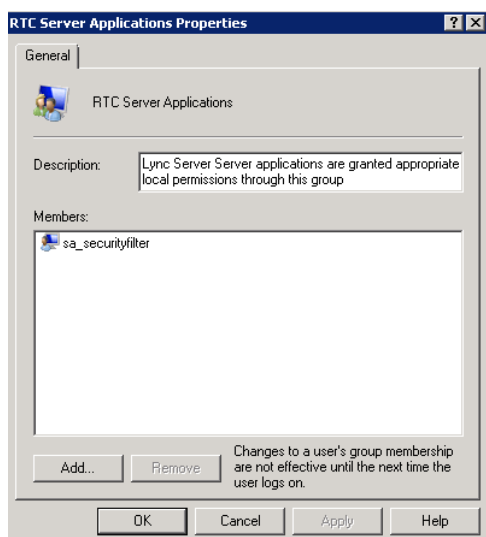


Figure 4.1 Security Edge Filter service account

If you restrict user access to this server, make sure this account has permissions to “Log on as a Service”. This setting can be found under the Local Security Policy (Figure 4.2).

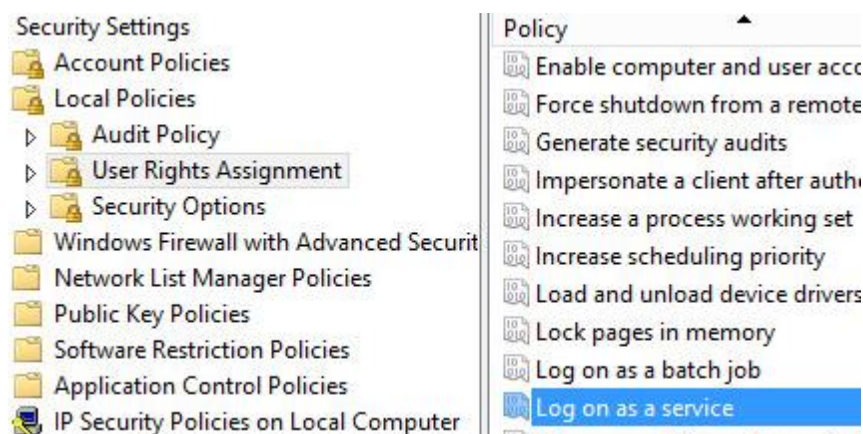


Figure 4.2 Service account permissions

To locate the Local Security Policy, open Server Manager, click on Tools and select Local Security Policy from the dropdown menu (Figure 4.3).

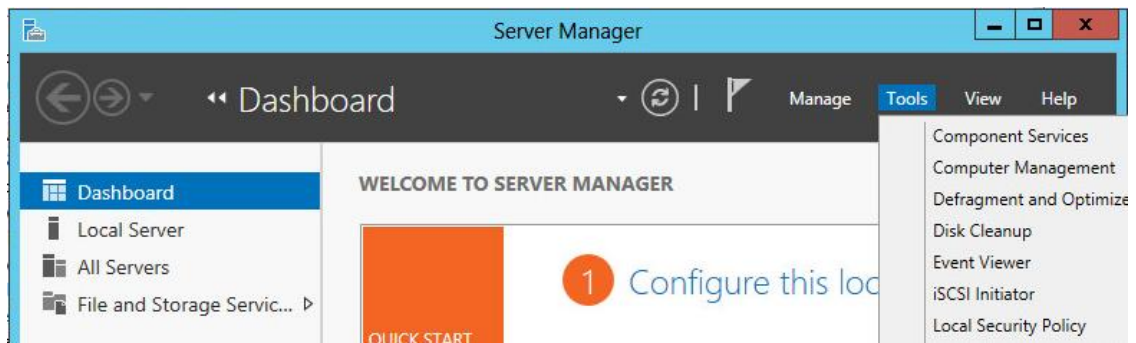


Figure 4.3 Local Security Policy

4.3 Install Security Edge Filter

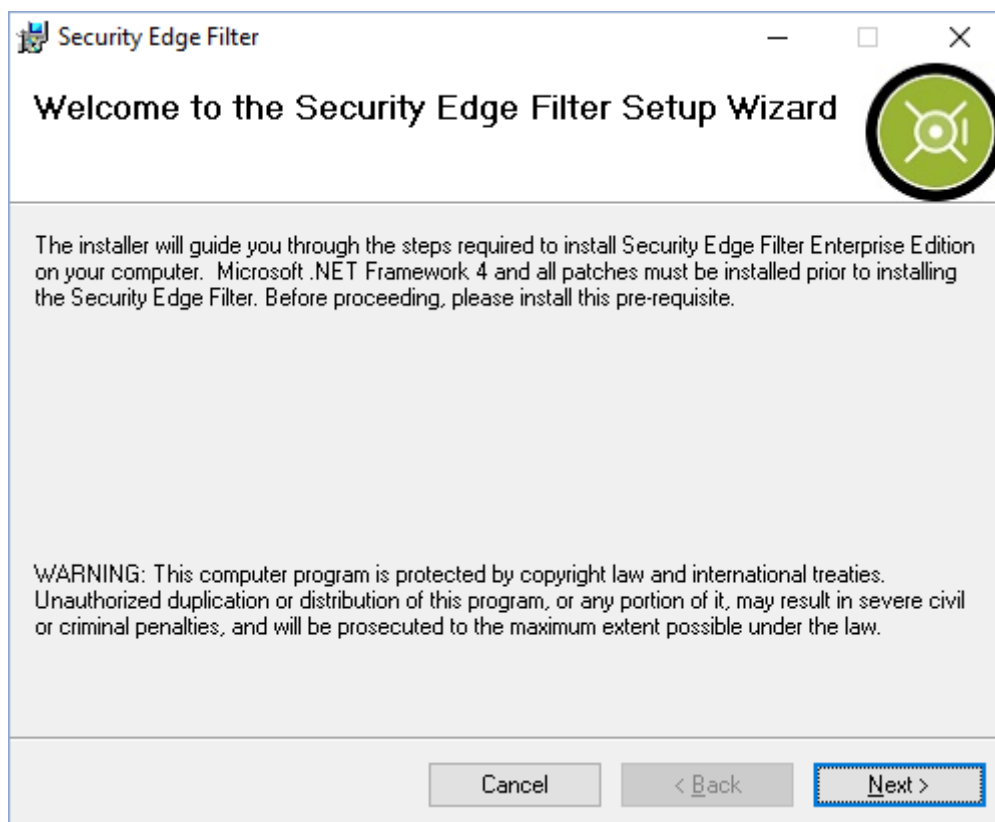
Use the following steps on every Edge Server in the Edge pool. The Security Edge Filter contains the following files:

- SecurityEdgeFilterSetup_enterprise.msi
- Setup.exe

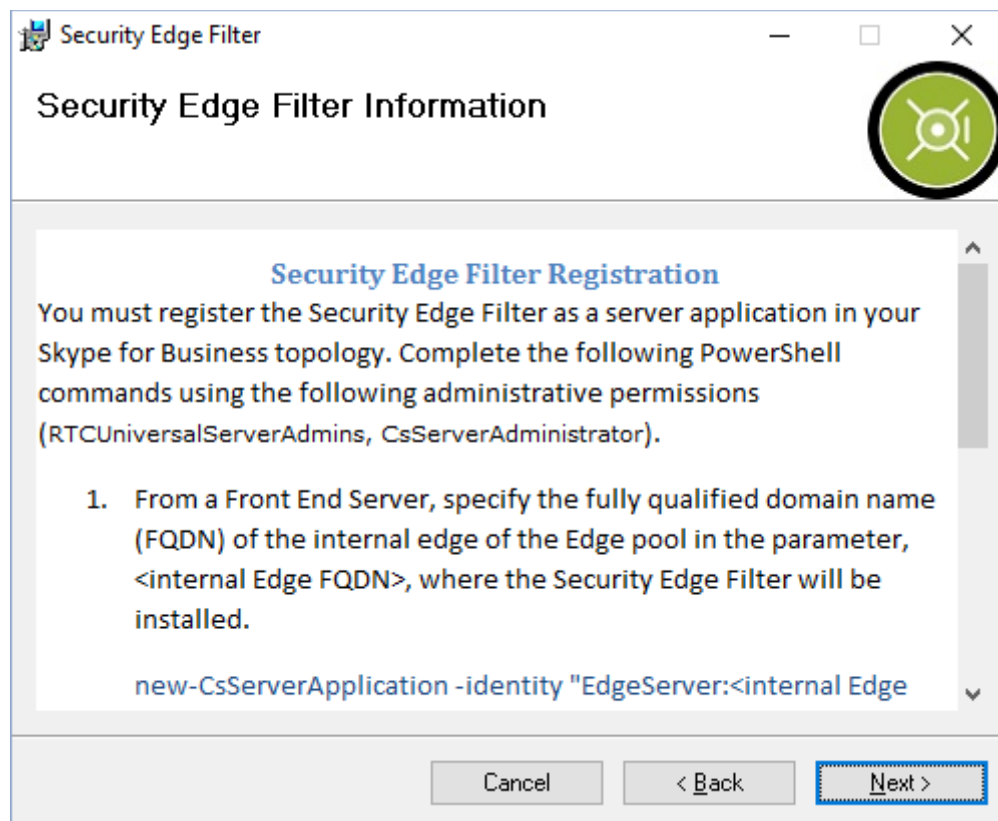
The Security Edge Filter requires that .NET Framework 4 and all its updates be installed. Download all these files from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=17851) (<http://www.microsoft.com/en-us/download/details.aspx?id=17851>).

Here's how to set up the Security Edge Filter on your Edge Server.

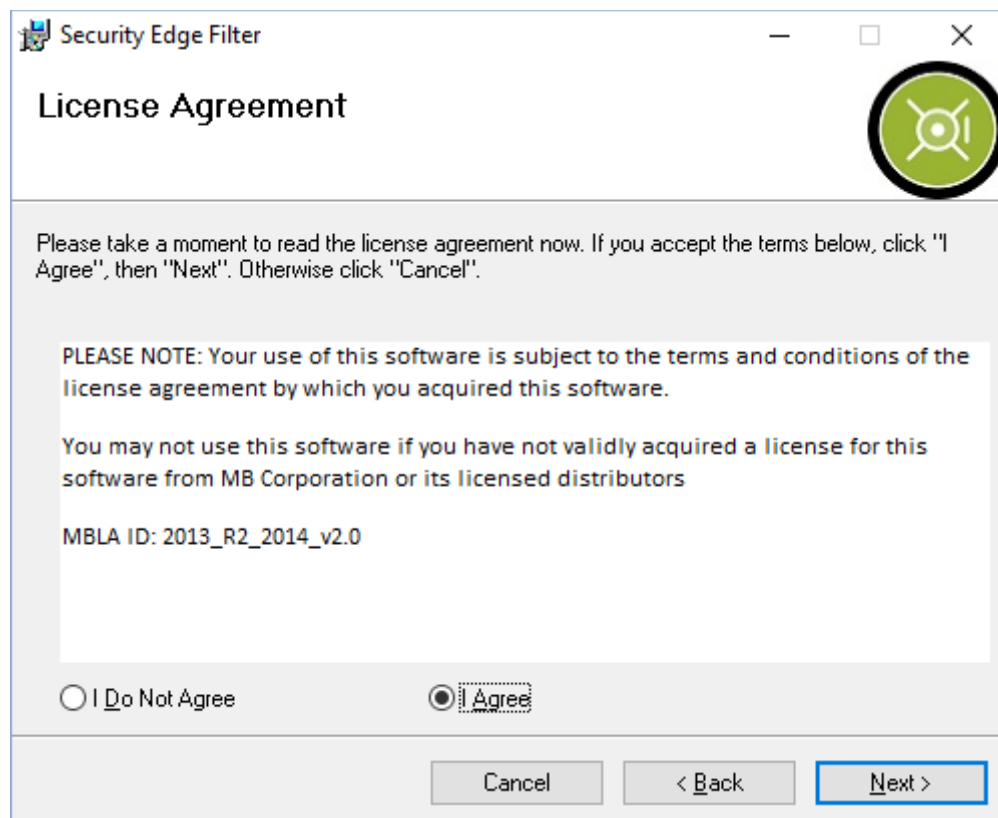
1. Download the Security Edge Filter from [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?id=17851) (<http://www.microsoft.com/en-us/download/details.aspx?id=17851>).
2. Run setup.exe with **local administrator** privileges. The Security Edge Filter Setup Wizard opens.



3. Click **Next**.
4. Run the PowerShell cmdlets to register the Security Edge Filter with your Edge Server as shown in the [Register Security Edge Filter](#) section of this document.



5. Click **Next**.
6. On the **License Agreement** page, click **I Agree**, and then click **Next**.

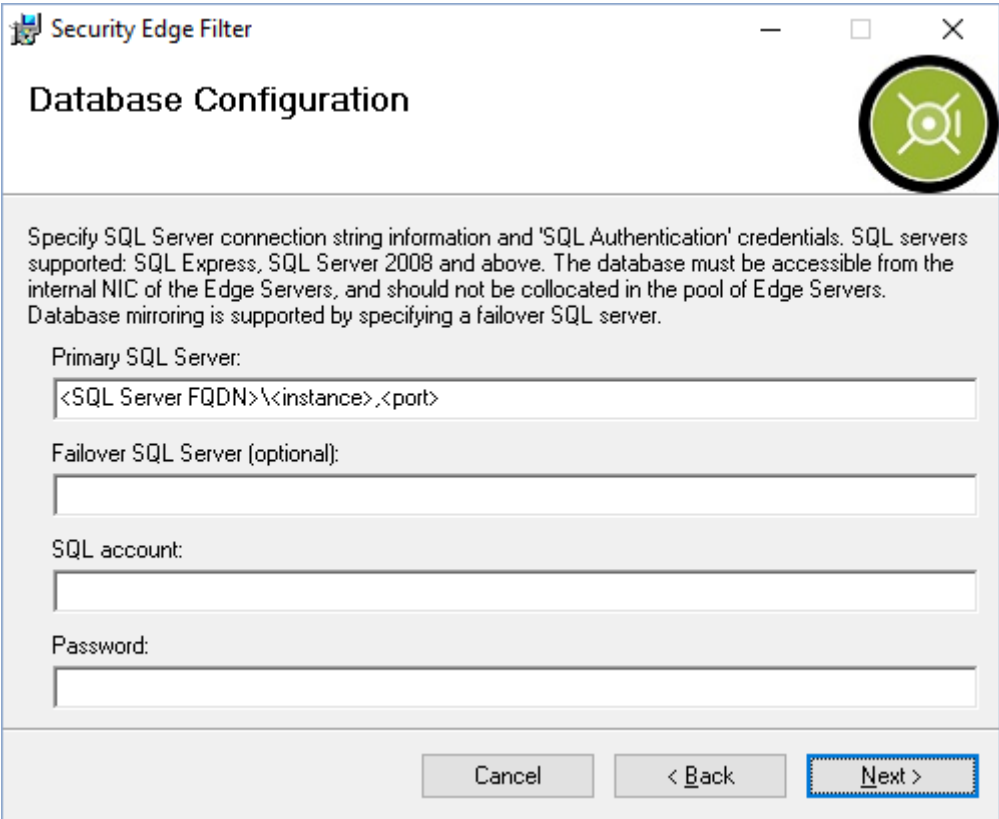


7. Specify the **Primary SQL Server** information and the SQL Authentication credentials to connect to the SecurityFilterManager database in the **Database Configuration** page.

Choose from the following, and then click **Next**.

- a. The default instance name for SQL Express Edition is SQLEXPRESS.
- b. The default instance name for both SQL Server Standard Edition and SQL Server Enterprise Edition is MSSQLSERVER.

Optionally, you can specify a **Failover SQL Server**. The database(s) must be accessible from the internal network interface of the Edge Server.



The screenshot shows a window titled "Security Edge Filter" with a sub-header "Database Configuration". On the right side of the header is a green circular icon with a white Android-like robot head. Below the header, there is a block of text: "Specify SQL Server connection string information and 'SQL Authentication' credentials. SQL servers supported: SQL Express, SQL Server 2008 and above. The database must be accessible from the internal NIC of the Edge Servers, and should not be collocated in the pool of Edge Servers. Database mirroring is supported by specifying a failover SQL server." Below this text are four input fields: "Primary SQL Server:" with a placeholder "<SQL Server FQDN>\<instance>,<port>", "Failover SQL Server (optional):", "SQL account:", and "Password:". At the bottom right are three buttons: "Cancel", "< Back", and "Next >". The "Next >" button is highlighted with a blue dashed border.

8. Click **Next**.
9. The **Confirm Installation** page appears; click **Next** to complete the installation.
10. Open the Services Management Console, and then locate the Security Edge Filter service.
11. Modify the logon settings of the Security Edge Filter service, and then specify the previously created service account.



12. Restart the service.

4.4 Security Edge Filter in Action

The Security Edge Filter logs information about login attempts in the Application Windows Logs.

The following screenshots show possible event log entries.

The first bad login attempt shows a Warning in the Event Viewer as shown in Figure 4.4.

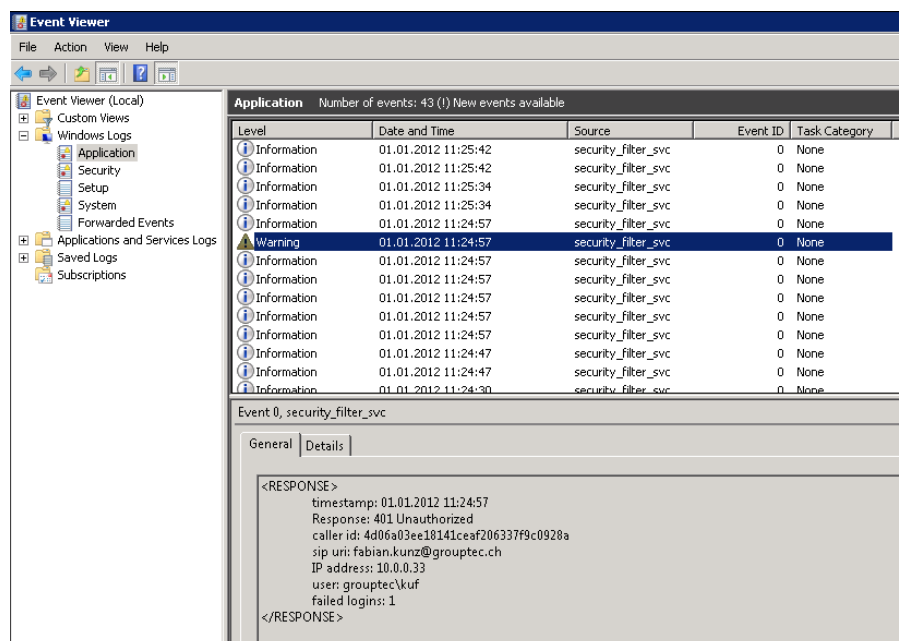


Figure 4.4 Warning in Event Viewer showing first bad login attempt

Maximum bad login attempts are reached, and then lockout is enforced as shown in Figure 4.5.

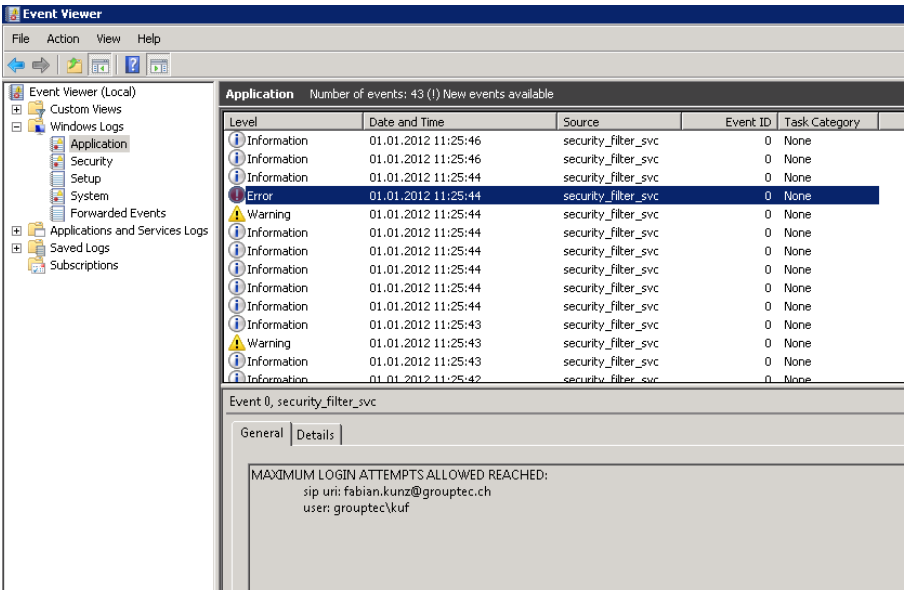


Figure 4.5 Lockout enforced after maximum bad login attempts shown in Event Viewer

Lockout is still enforced for an already blocked user as shown in Figure 4.6.

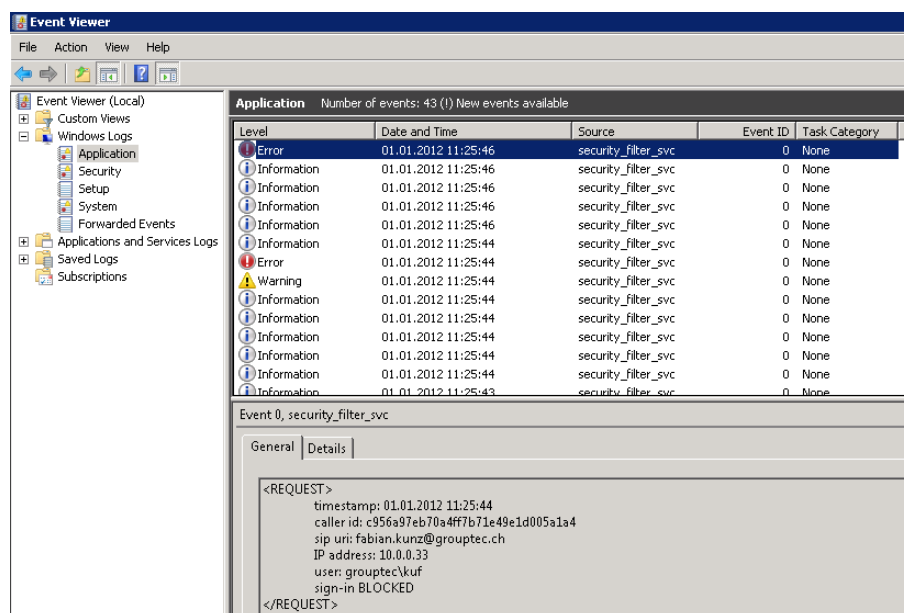


Figure 4.6 Event viewer showing already blocked user

By default the Security Edge Filter only logs failed logins. To view successful logins as well, configure the Security Edge Filter for verbose logging. This requires modifying the configuration file. Locate the config file %programFiles%\MB\Security Edge Filter\security_filter_svc.exe.config

Open the config file using Notepad or your preferred text editor. Modify the value, "normal", to "verbose" for the key, "logLevel".

```
<add key="logLevel" value="verbose" />
```

NTLM v2 login attempt is rejected as shown in Figure 4.7.

Security Edge Filter is configured only for TLS-DSK authentication and blocks Windows Challenge/Response (NTLM) v2 authentication.

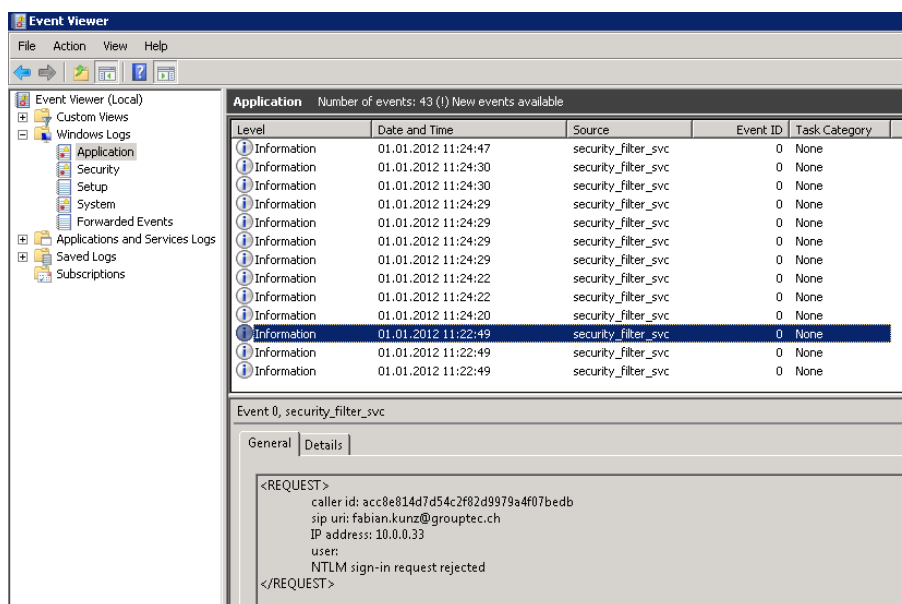


Figure 4.7 NTLM v2 login attempt is rejected

The database connection has been lost. Verify that the TCP/IP connectivity to the SQL database is working properly as shown in Figure 4.8. If the database is running, investigate potential firewall issues between the Edge Server and the Security Filter Manager running the SQL Server.

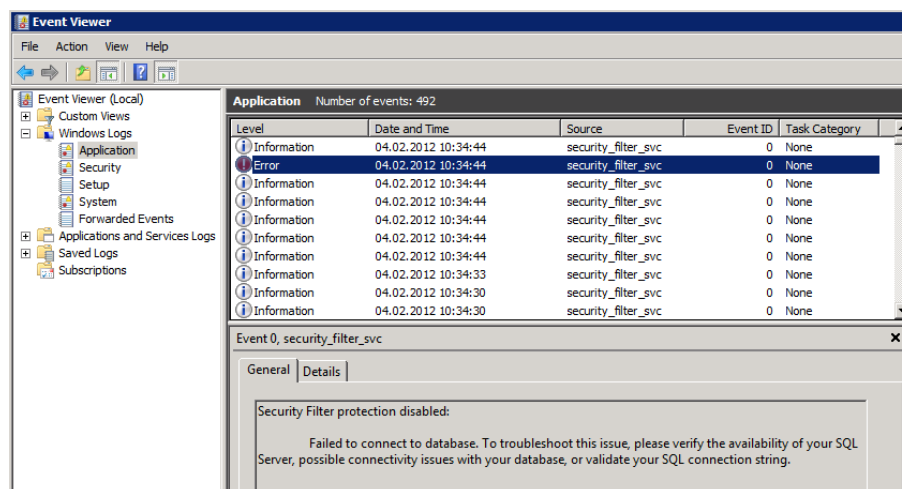


Figure 4.8 Database connection has been lost

4.5 Troubleshooting

Before opening a case, please reproduce your issue with verbose logging enabled. This will provide additional information not available in the Application Event Viewer.

Use the DebugView tool to capture this verbose logging. You can download this free tool from [Windows Sysinternals](http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx) (<http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx>).

1. Start Dbgview.exe using administrative privileges, and check the **Capture Global Win32** option as shown in Figure 6.14.

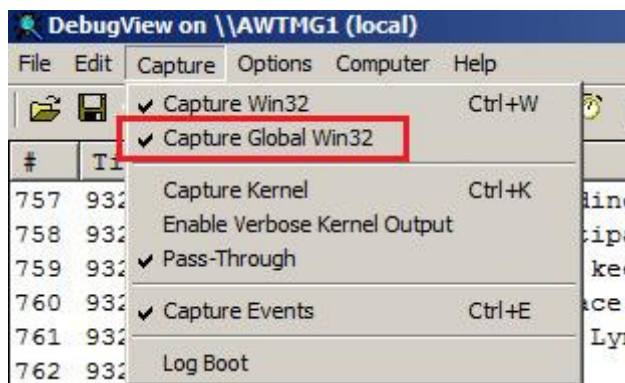


Figure 6.14 Options to select for DbgView

2. As soon as you have reproduced the issue, save the output to a text file as shown in Figure 6.15.

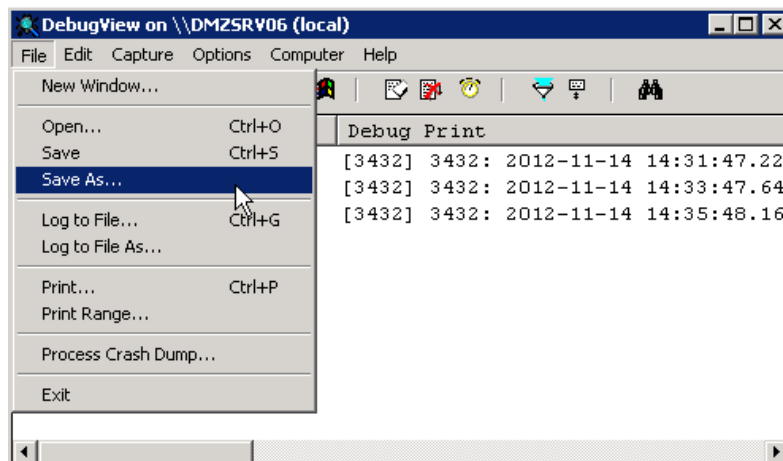


Figure 6.15 Debug output