SCRIBBLER LOG MANAGER

Version- 1.7

Scribbler
Log Manager

USER GUIDE

WWW.SYSKEYSOFTLABS.COM

Scribbler
Log Manager

Syskey Softlabs

support@syskeysoftlabs.com | sales@syskeysoftlabs.com

Copyright

© 2022 Syskey Softlabs Pvt ltd.

Trademarks

Microsoft, Windows, Windows Server, and Active Directory are either trademarks or registered trademarks of their respective owners in the United States and/or other countries.

Contents

Scribbler Log Manager

Scribbler is the one-stop solution for centralized log management. Scribbler gathers log data from across the network and enables system administrators to easily monitor key metrics and change activities.

Scribbler can collect, analyze, and forward logs in real-time. The web-based analytical dashboard gives insights into the state of a system and its progress.

Key features of Scribbler are:

- **Centralized dashboard -** Track and analyze all the devices on your network with real-time logs to quickly identify faulty devices.
- **Regulatory compliance -** Create and manage audit log retention policies as per your regulatory requirements.
- **Log aggregation for cybersecurity -** Aggregate and search all your system logs to enable forensic analysis of cybersecurity issues and threats.

Other features include user management with LDAP on Active Directory, SNMP health check, log forwarding on RFC5424 protocol, custom log forwarding and storing filters, and database management.

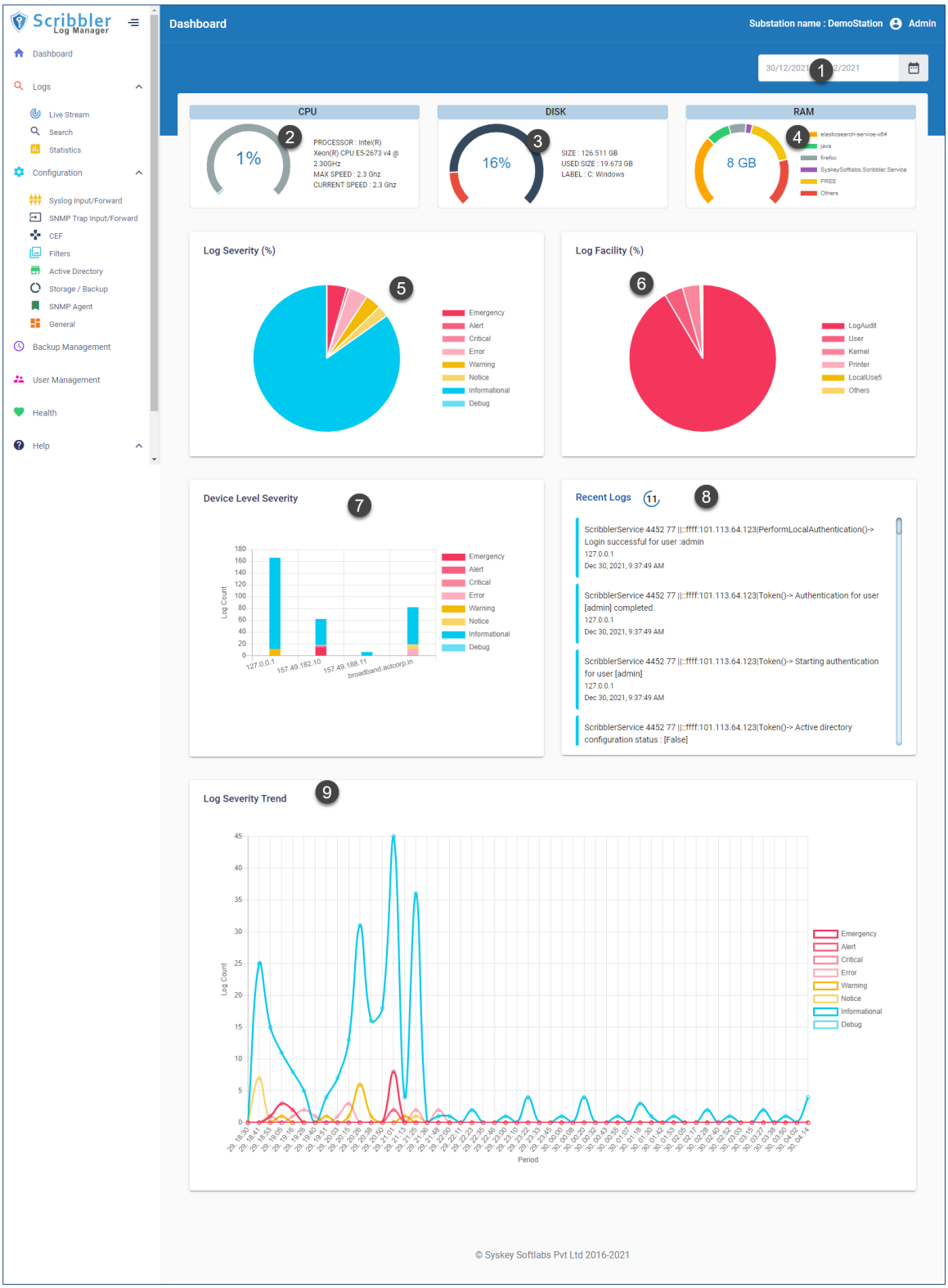
Installing Scribbler

Scribbler supports flexible deployment options. It can either be installed on windows running on a Virtual Machine (VM) or on a bare metal server.

Detailed instructions on how to install Scribbler are provided at the end of the document.

Dashboard overview

Scribbler dashboard is an administrator's cockpit that provides a comprehensive analysis of resource utilization, recent real-time logs, and various charts that represent the log severity and facility levels.



The following table describes the various widgets on the dashboard:

Number	Item	Description
1	Date range	Dashboard data is updated according to the date range selected. The default date is **Today**.
2	CPU	Represents the CPU utilization of the server that is hosting Scribbler.
3	Disk	Represents the disk space utilization of the server that is hosting Scribbler.
4	RAM	Represents the RAM usage details for the top seven applications of the server that is hosting Scribbler.
5	Log Severity (%)	The pie chart displays the percentage distribution of log severity for the selected date range. The list shows the color associated with the severity level. Hover over the chart to view the severity level and percentage value. Click the severity level in the legend to remove or add that level from the chart.
6	Log Facility (%)	The pie chart displays the percentage distribution of logs by the top seven syslog facilities for the selected date range. Hover over the chart to view the severity level and percentage value. Click the facility in the legend to remove or add that level from the chart.
7	Device Level Severity	The bar graph displays the top 10 devices on the x-axis and the log count on the y-axis. The stacked bar colors represent the log severity levels.
8	Recent Logs	The latest 50 logs from the database are displayed. The logs are refreshed every 15 seconds.
9	Log Severity Trend	The bar graph displays the log severity trend in the selected time period.

Configuring Scribbler

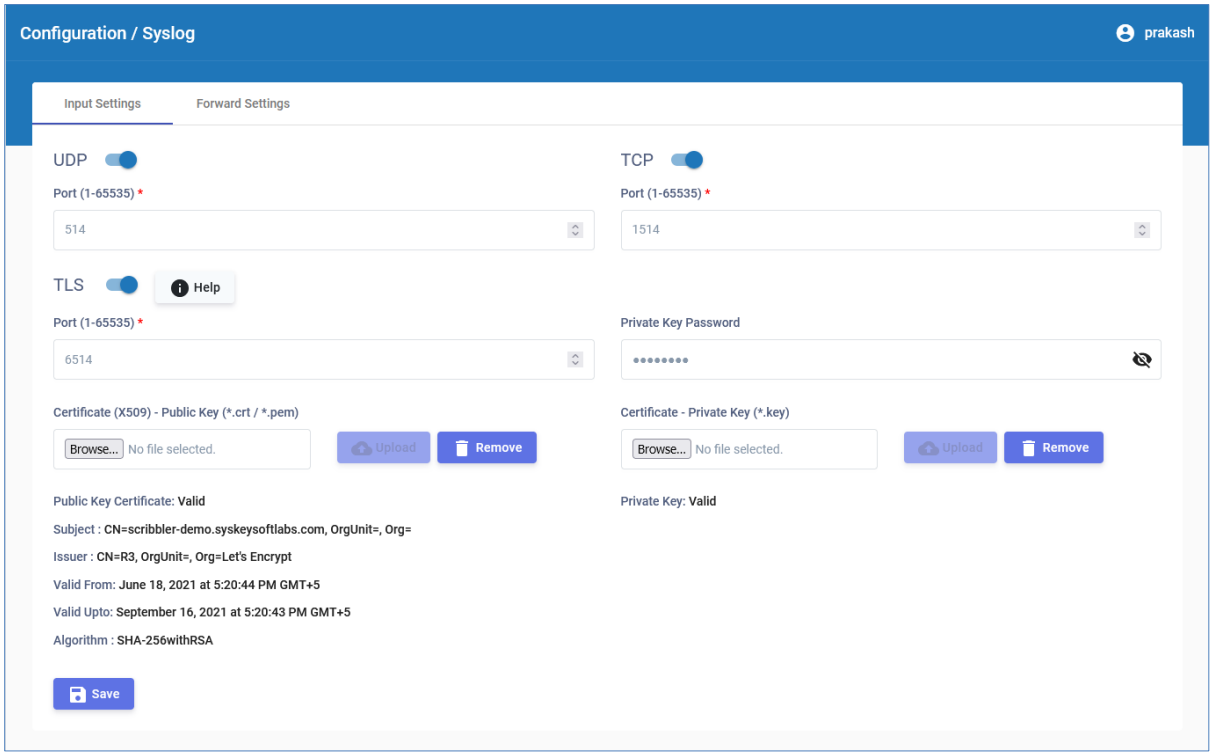
Configuration privileges are available only for administrators.

How to configure input options

Configure the input options to enable Scribbler to listen on the port and for the protocol used by the network devices.

Procedure

1. In the navigation pane, go to **Configuration > Syslog Input/Forward**.



2. In the **Input Settings** tab, select the protocols used by the network devices. The options are:
   - **UDP** - Specify the port number for UDP syslog messages.
   - **TCP** - Specify the port number for TCP syslog messages.
   - **TLS** - Specify the port number for TLS syslog messages.
3. If TLS is chosen, upload the private key and public key certificates along with the private key password. The accepted certificate formats for public key are .crt and .pem, and for private key is .key.

   TLS is enabled only if all the details such as private key, public key and private key password are correct. Else, though it shows as enabled on the interface, TLS will not be enabled internally.

   After the upload is complete, certificate details are displayed.

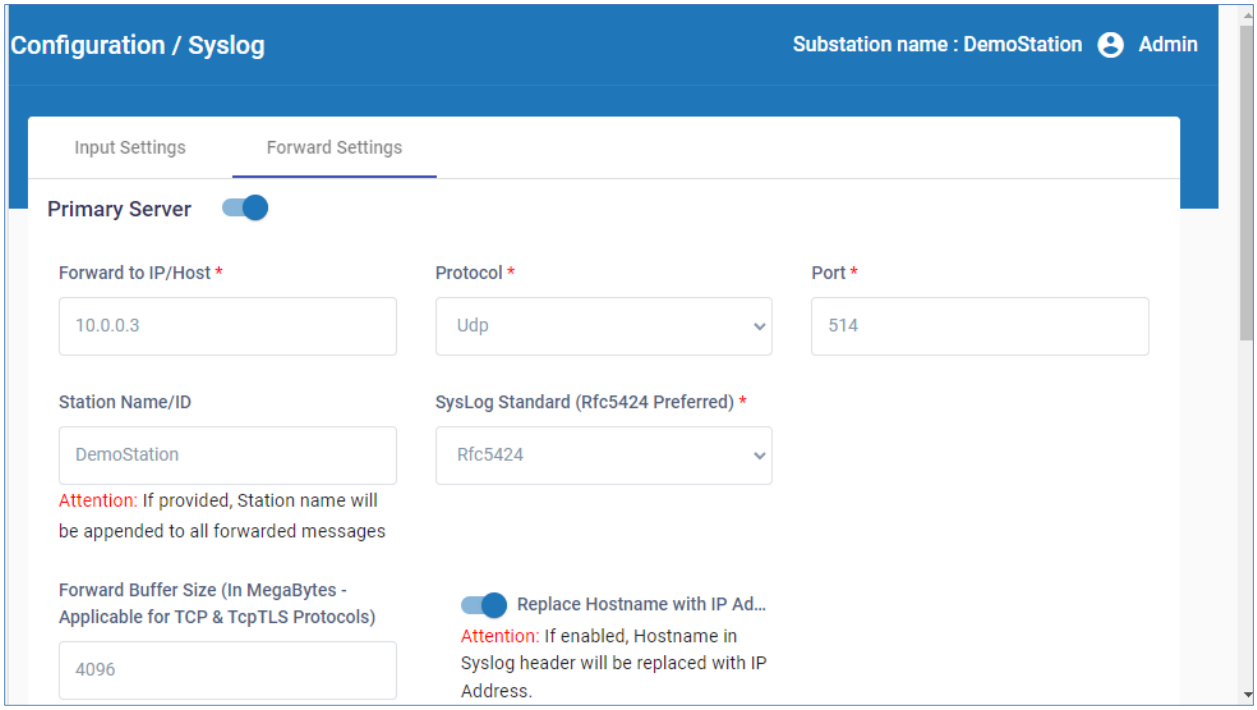
4. Click 

How to forward logs to a remote server

You can configure Scribbler to forward system logs to a remote server.

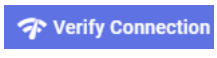
Procedure

1. In the navigation pane, go to **Configuration > Syslog Input/Forward**.



2. In the **Forward Settings** tab, specify the IP address, network protocol, port number, station ID, and syslog standard of the primary remote server.
3. If the protocol is TCP, select the method for TCP framing. The available options are **Octet Counting** and **Non Transparent Framing**.
4. If the protocol is either TCP or TCPTLS, enter the **Forward Buffer Size** in MB. The minimum value is 64 MB and the maximum value is 32K MB.

   Note: The buffer holds the failed messages when the forward server is unreachable. After the buffer reaches the size specified here, the buffer resets to empty. This does not affect the logs in the local database.

5. Enable **Replace Hostname with IP Address** to replace the hostname in Syslog header with the IP address.
6. Click 

to verify the TLS connection parameters are correctly configured..
7. Click 

.

You can refer to the Log Forwarding section for more details about the various configuration parameters available for this option.

You can calculate the correct buffer size depending on the daily expected logs file size and the maximum down time expected. For example, if the daily expected logs are 1GB and the maximum expected down time for the forward server is 2 days, the correct buffer size can be calculated as:

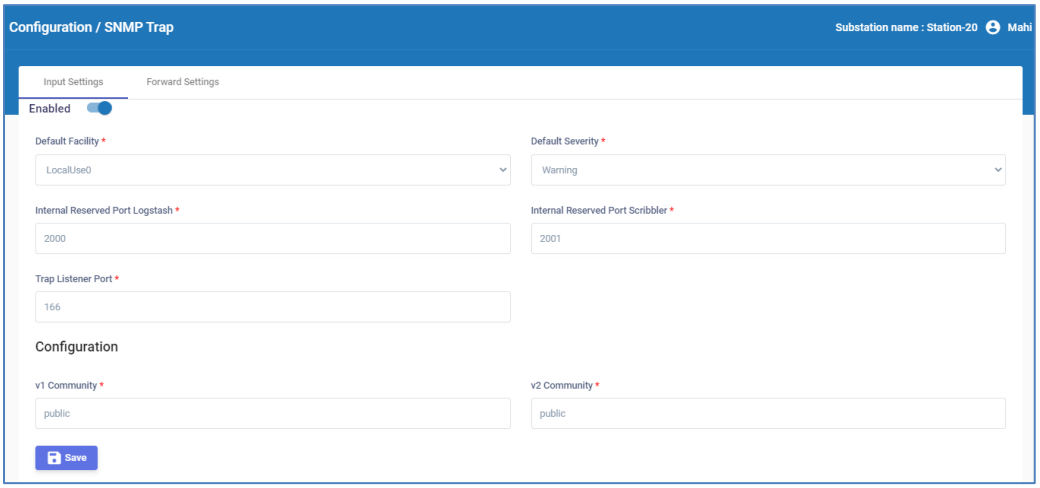
1 GB * (2 + 1 [extra day]) = 3GB => 3000 MB

How to configure SNMP trap input settings

You can configure Scribbler to receive SNMP traps from network devices and then forward the information to Logstash.

Procedure

1. In the navigation pane, go to **Configuration > SNMP Trap**.



2. In the **Input Settings** tab, enable Scribbler to receive SNMP traps.
3. Set the default facility and default severity levels for the traps.
4. Specify the port reserved on Logstash to receive the traps.
5. Specify the port reserved on Scribbler to receive the traps.
6. Specify the port that must be monitored for SNMP traps.
7. Specify the community string that must be included for SNMPv1 and SNMPv2 protocols. The default value is “public”.
8. Click 

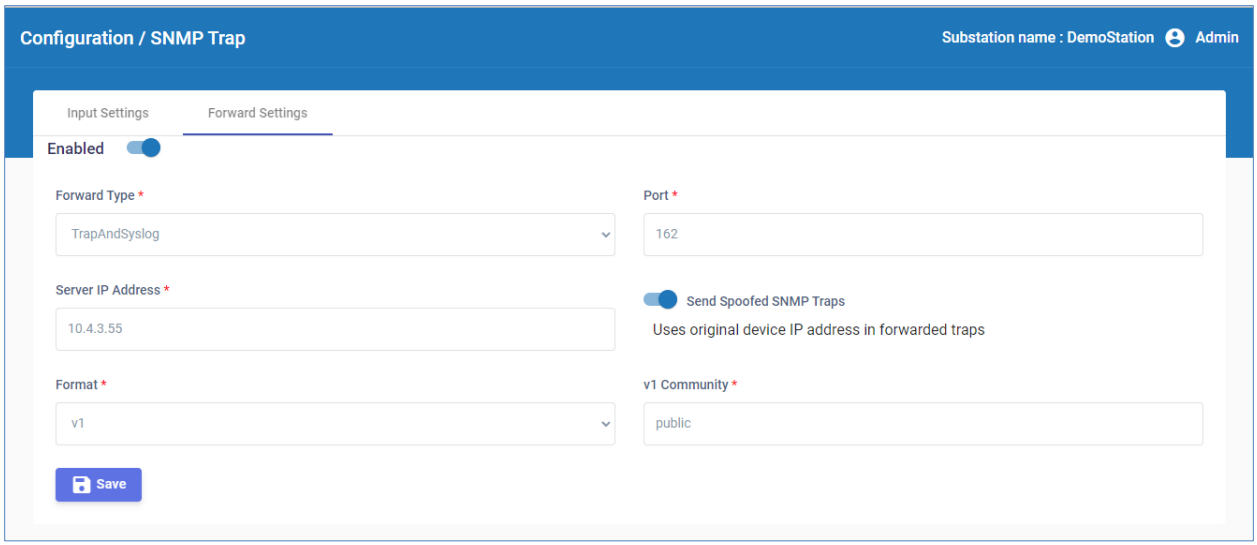
.

How to configure SNMP traps forward settings

You must configure Scribbler to forward the SNMP traps to a remote server.

Procedure

1. In the navigation pane, go to **Configuration > SNMP Trap**.



2. In the **Forward Settings** tab, enable Scribbler to forward SNMP traps.
3. Select the **Forward Type** as **Trap**, **Syslog**, or **Trap and Syslog**.
4. Specify the port number and the IP address of the remote server.
5. To forward the SNMP traps with original source address in the IP header, enable **Send Spoofed SNMP Traps**.
6. Select the format of the forwarded messages as either v1 or v2c.
7. Specify the community string that must be included with the SNMP traps.
8. Click 

.

How to configure Active Directory Authentication

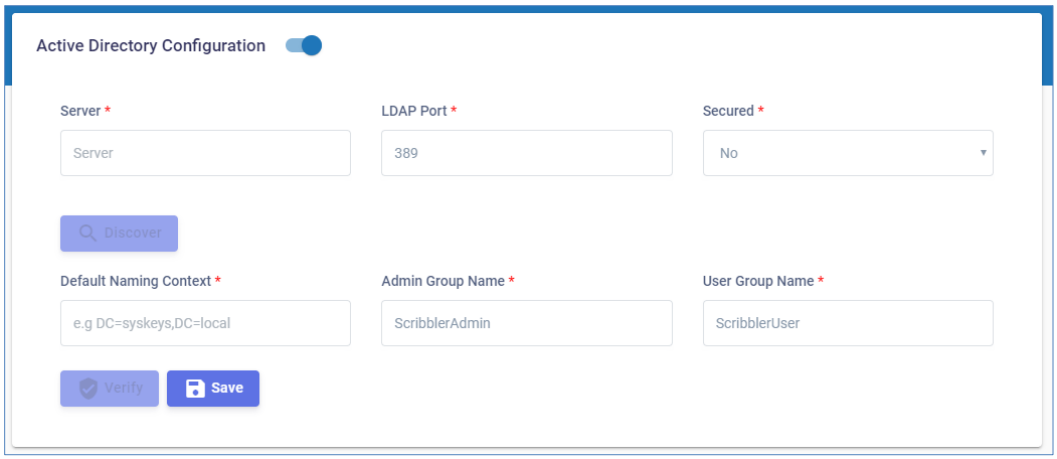
The solution supports integration with Microsoft Active Directory through LDAP. The authentication is **"**pass-through**"**, which indicates that the credentials are not stored.

Upon successful login with the AD, Scribbler will check whether the user is part of ScribblerAdmin or ScribblerUser groups (configurable) and provide access based on their role.

If the login fails due to any reason (wrong password, insufficient permission, server down), the credentials are validated against local accounts and the user will be allowed to login upon successful verification.

Procedure

1. In the navigation pane, go to **Configuration > Active Directory**.



2. Enable the active directory option.
3. Provide the Active Directory server IP address or FQDN (Fully Qualified Domain Name).
4. Provide the port number for the LDAP connection on the AD Server.
    a. Typically, 389 for non-TLS connections
    b. Typically, 636 for TLS connections. TLS works only on proper certificate infrastructure.
5. Click Discover. The system will try to find the LDAP naming context.
6. Once obtained, the naming context will be automatically shown on the “Default Naming Context”
7. Provide a group name for Admin and User roles in “Admin Group Name” and “User Group Name”
8. Login to the Active Directory server and create the groups with the name you entered in Step 6. Add assign the users to the group.
9. Click the verify button and try to validate the configuration. An error message is displayed in case incorrect inputs are provided. Please troubleshoot the issue based on the message or contact support.
10. Once verified, click 

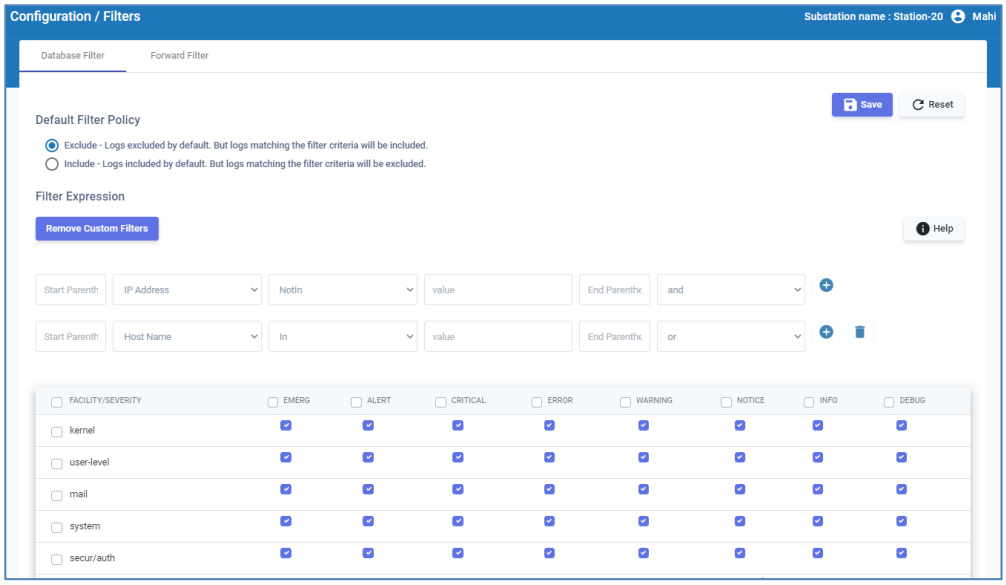
Active Directory is enabled from the next login.

How to set database filters

Database filters decide which logs are stored in the database. The application reads all the logs and stores a copy to the database based on the configured filters. You can set filters for facilities for each severity level.

Procedure

1. In the navigation pane, go to **Configuration > Filters**.



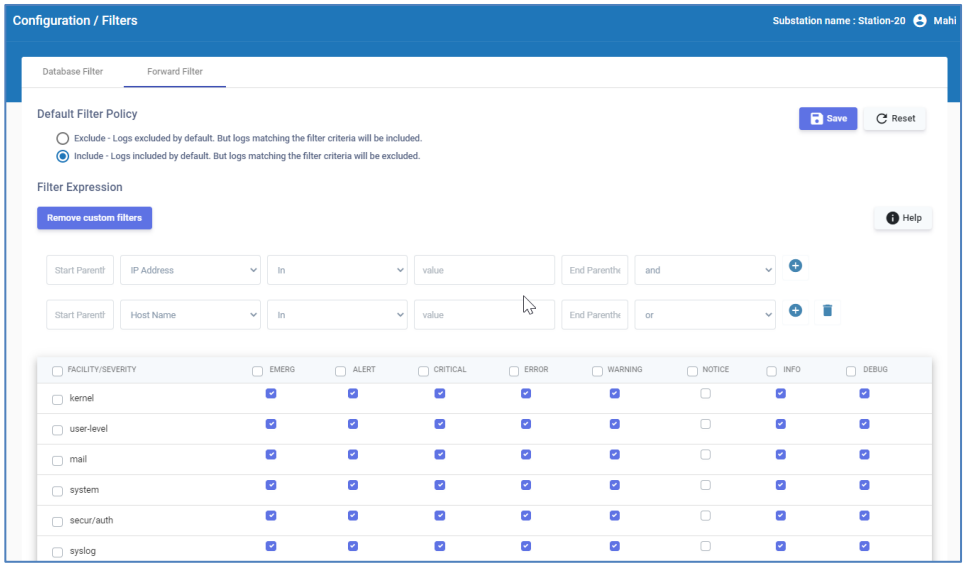
2. Set the Default filter policy:
   - Choose the **Include** option to keep only the selected logs.
   - Choose the **Exclude** option to remove the selected logs.
3. Click Add Custom Filters to add custom filter expressions to narrow or expand the focus of your search in the priority matrix.
   Click Help for more information about the custom filters and search expression examples.
4. For each facility, select the severity levels of log messages that must be stored.
5. Click Save

How to set forward filters

You must forward log data to a remote backup database to conserve database storage space. The application reads all the logs and stores a copy to the database based on the configured filters. You can set filters for facilities for each severity level.

Procedure

1. In the navigation pane, go to **Configuration > Filters**.



2. In the **Forward Filter** page, set the Default filter policy:
   - Choose the **Include** option to keep only the selected logs.
   - Choose the **Exclude** option to remove the selected logs.
3. Click **Add Custom Filters** to add custom filter expressions to narrow or expand the focus of your search in the priority matrix.

   Click Help for detailed examples about using the custom filters and search expression.

4. Select the severity levels of log messages that must be forwarded for each facility.
5. Click **Save**.

How to configure storage

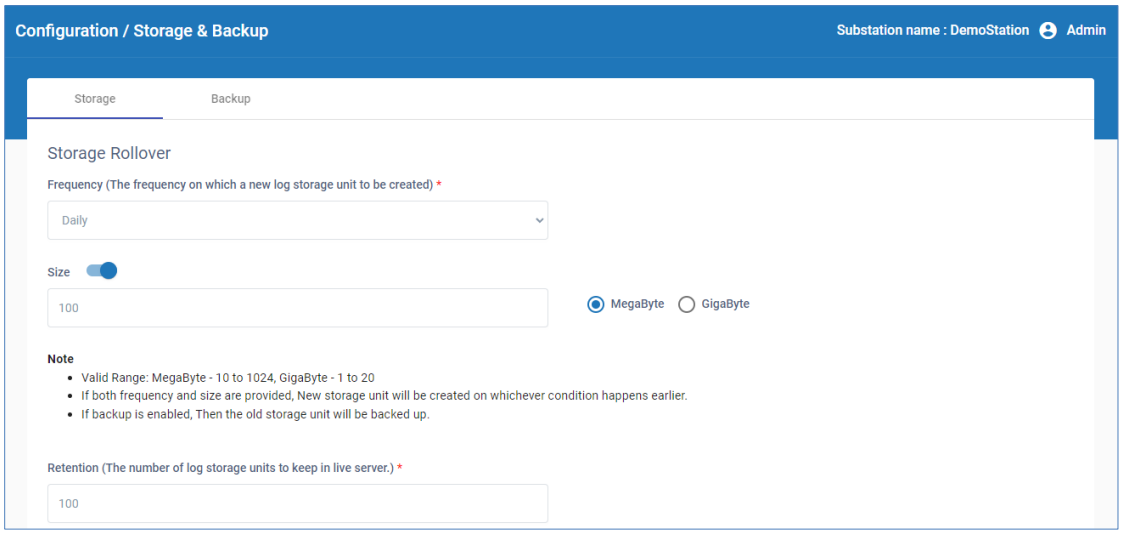
You can configure the storage settings to set the frequency for creating a new log storage unit, the number of storage units that must be retained in the live database, and the size of the storage unit.

It is important to configure the correct values for storage and retention. If they are incorrectly configured, log collection might be impacted. For example, if the expected log size per day is 1GB, and the retention period is 6 months, then the maximum storage unit size must be 180GB.

The more the size of the storage unit, the more time it takes to create backups and restore. It is recommended that you plan at least an additional 6x (storage unit size) space on the data drive. For example, 10 GB size rollover must have 60GB additional space.

Procedure

1. In the navigation pane, go to **Configuration > Storage / Backup.**



2. In the **Storage** tab, set the frequency for creating new storage units for storing log files. The options are: every ten minutes, daily, weekly, and monthly.
3. Enable the option to set the **Size** of the storage unit and enter the maximum size of the storage unit in either MB or GB. The valid range for storage units are either 10-1024MB or 1-20GB.

   Note: If both, frequency and size are specified, new storage units are created based on the condition that occurs first. If backup is enabled, the old storage unit is backed up.

4. Enter the maximum number of storage units that can be stored on the live database. The minimum number of units is 1 and the maximum is 250.

   Note: Storage units older than the retention configuration are automatically deleted. If backup is enabled, storage units older than the retention configuration are backed up before deletion.

5. Click Save.

How to configure backup

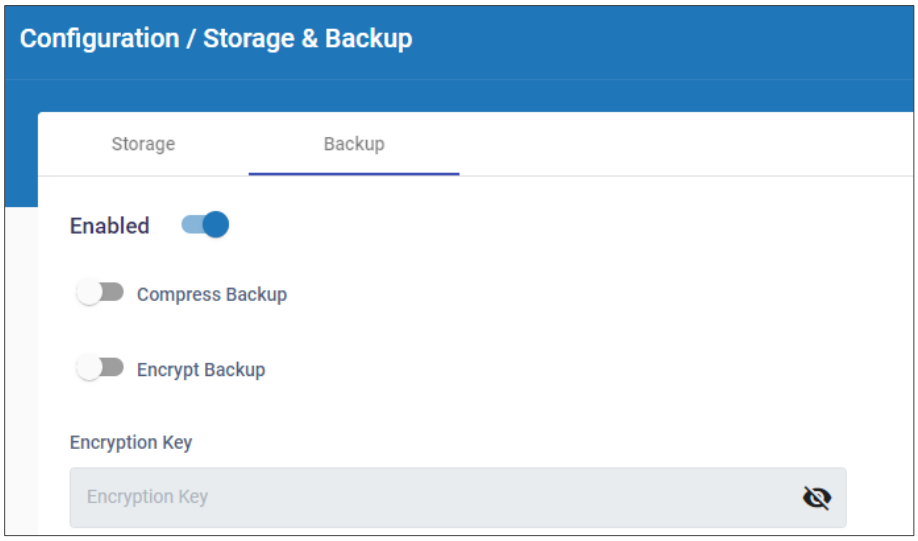
You can configure the backup storage location. You can also compress and encrypt the backup files to secure them.

Note: Encryption and Compression are high CPU intensive operations. These configurations must be enabled only if necessary.

It is strongly recommended that you keep a separate copy and history of encryption keys and ID combinations. The backup files will be unreadable in case of disk failures.

Procedure

1. In the navigation pane, go to **Configuration > Storage / Backup.**



2. In the Backup tab, enable **Compress Backup** to compress all the data in the backup.
3. Enable **Encrypt Backup** to encode all the data in the backup.
4. If encryption is enabled, you must enter an **Encryption Key** to access the encrypted backup.

   Note: Any encryption change will be applied from the next backup onwards. The existing backups will not be affected by the change. The system can detect the encryption state and process the backup files accordingly.

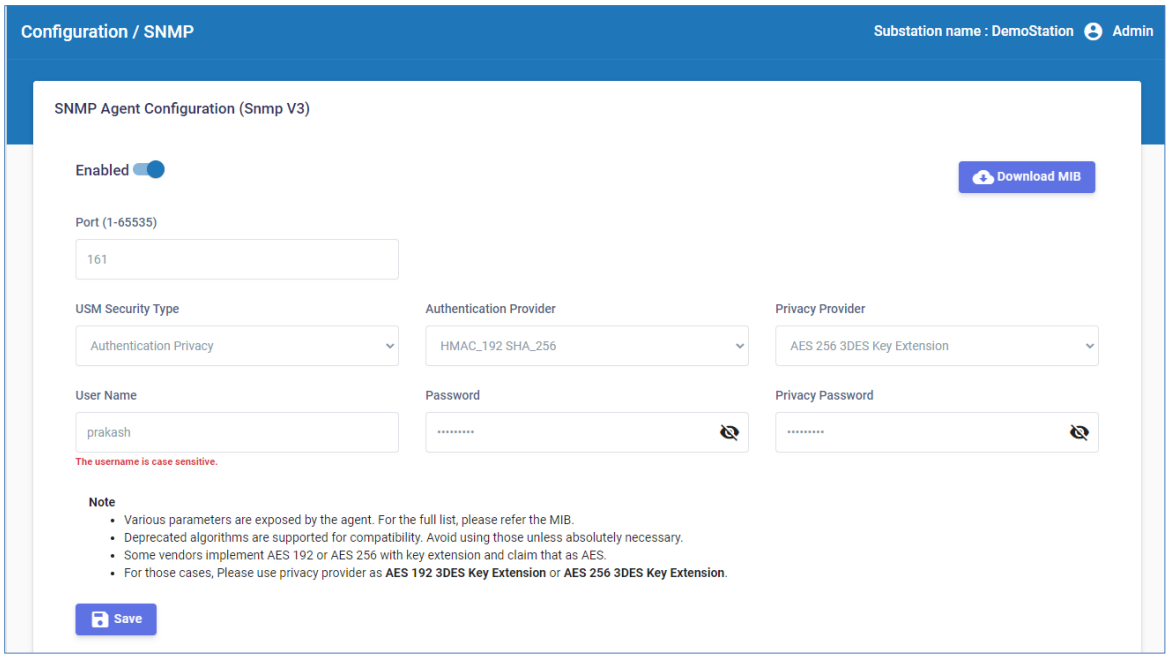
5. Choose to store the backup files in the **Local Drive** or **SMB (Windows Network Share)**.
6. If local drive is selected, specify the local drive path to store the backup. If SMB is selected, specify the user credentials and the server path to store the backup.
7. Click Save.

How to configure SNMP

Scribbler supports SNMPv3 for reporting purposes.

Procedure

1. In the navigation pane, go to **Configuration > SNMP Agent**.



2. Enable SNMP Agent.
3. Enter the agent **Port** number.
4. Select the **USM Security Type**. The options are: No Authentication No Privacy, Authentication No Privacy, and Authentication Privacy.
5. If the security type includes authentication, select the **Authentication Provider** and enter the user credentials.
6. If the security type includes privacy, select the **Privacy Provider** and enter the privacy password.
7. Click  .
8. To view the full list of parameters exposed by the agent, download the MIB file. Click  .

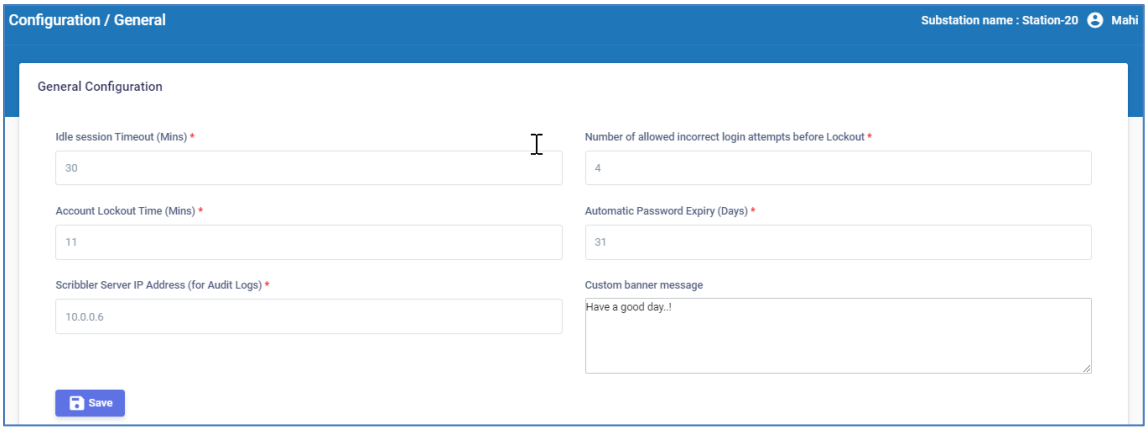
Note: Deprecated algorithms such as MD5, SHA, and DES are supported for compatibility. It is recommended that the deprecated algorithms are not used unless absolutely necessary. If you are using AES 192 or AES 256 with key extension, use privacy provider as AES 192 3DES Key Extension or AES 256 3DES Key Extension respectively.

How to configure general settings

The General Configuration page provides options to configure security settings for account logins, session timeout, and password expiry. You can also configure audit logging IP address and banners.

Procedure

1. In the navigation pane, go to **Configuration > General**.



Enter the values for the fields on the page. The following table describes the fields.

Field	Description
Idle session Timeout (Mins)	The web session timeout in minutes.
Number of allowed incorrect login attempts before Lockout	The maximum number of login attempts allowed before the user account is locked out.
Account Lockout Time (Mins)	Time in minutes for which the user will be locked out of their account.
Automatic Password Expiry (Days)	The number of days after which the user password automatically expires.
Scribbler Server IP Address (for Audit Logs)	The IP address of the Scribbler server to collect audit logs.
Custom banner message	Text that will be displayed as banner message prior to the login page.

2. After you enter the configuration values, click 

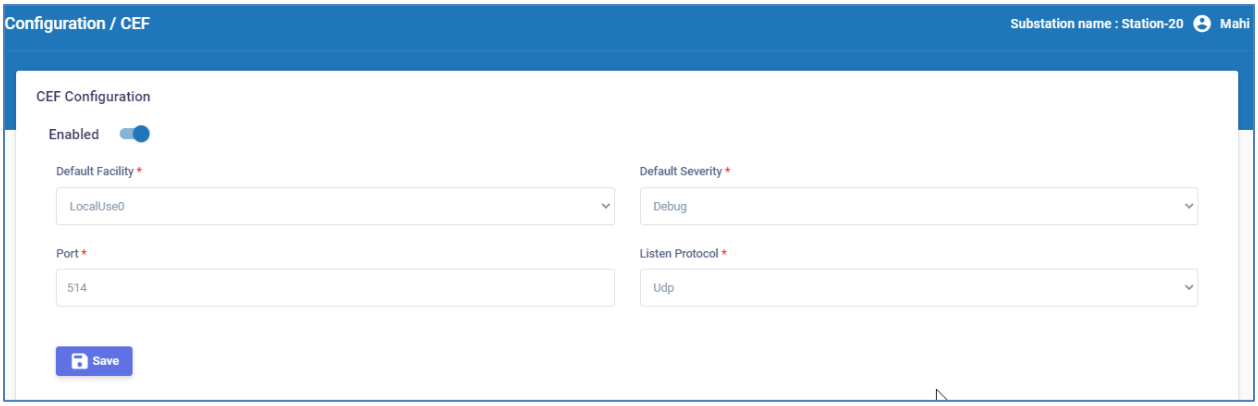
.

How to configure CEF logs

You can configure Scribbler to collect syslogs in Common Event Format (CEF) format.

Procedure

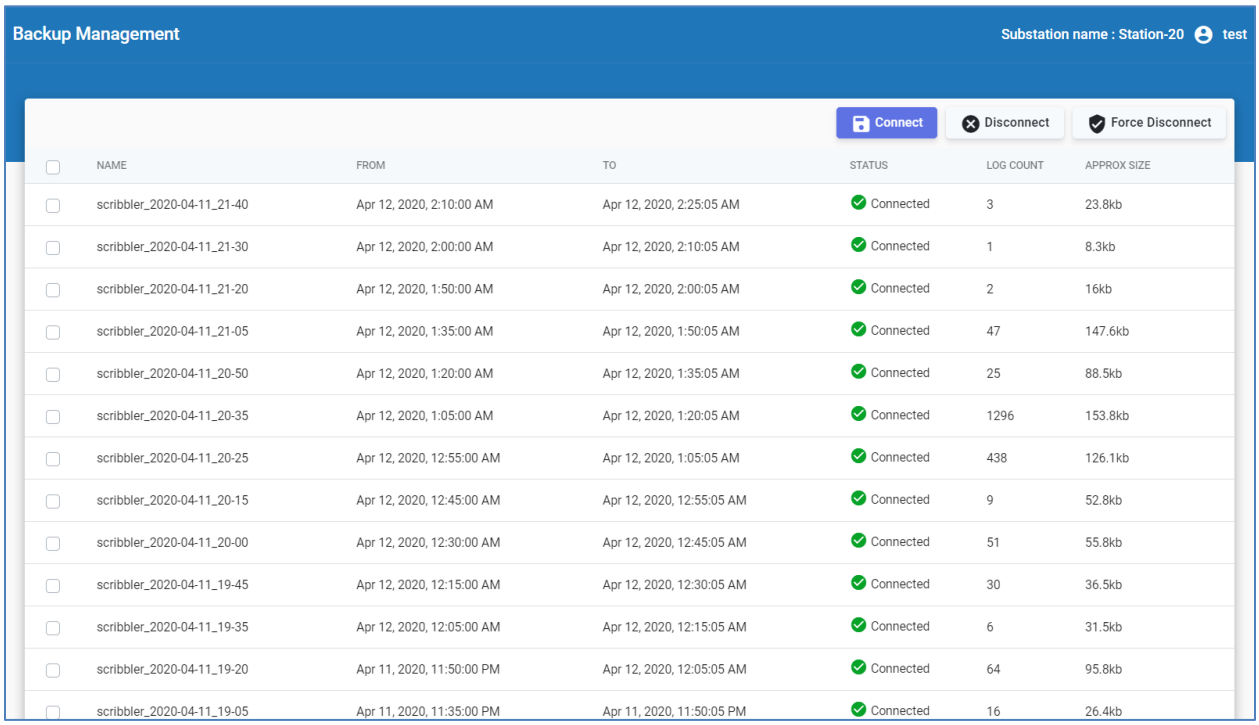
1. In the navigation pane, go to **Configuration > CEF**.



2. Enable Scribbler to collect CEF logs.
3. Select the **Default Facility** that will collect the logs.
4. Select the Default Severity level of the logs.
5. Specify the port that will receive the logs.
6. Select either UDP or TCP as the listening protocol.
7. If you select TCP, enter the message delimiter that should be used to identify separate syslog messages.
8. After you enter the values, click Save.

Managing database backup

By default, log data is backed up to the backup folder at the end of every month. The Backup Management page displays the list of backup folders, the backup period, the connection status, log count and the approximate size of the backup files.



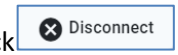
NAME	FROM	TO	STATUS	LOG COUNT	APPROX SIZE
scribbler_2020-04-11_21-40	Apr 12, 2020, 2:10:00 AM	Apr 12, 2020, 2:25:05 AM	Connected	3	23.8kb
scribbler_2020-04-11_21-30	Apr 12, 2020, 2:00:00 AM	Apr 12, 2020, 2:10:05 AM	Connected	1	8.3kb
scribbler_2020-04-11_21-20	Apr 12, 2020, 1:50:00 AM	Apr 12, 2020, 2:00:05 AM	Connected	2	16kb
scribbler_2020-04-11_21-05	Apr 12, 2020, 1:35:00 AM	Apr 12, 2020, 1:50:05 AM	Connected	47	147.6kb
scribbler_2020-04-11_20-50	Apr 12, 2020, 1:20:00 AM	Apr 12, 2020, 1:35:05 AM	Connected	25	88.5kb
scribbler_2020-04-11_20-35	Apr 12, 2020, 1:05:00 AM	Apr 12, 2020, 1:20:05 AM	Connected	1296	153.8kb
scribbler_2020-04-11_20-25	Apr 12, 2020, 12:55:00 AM	Apr 12, 2020, 1:05:05 AM	Connected	438	126.1kb
scribbler_2020-04-11_20-15	Apr 12, 2020, 12:45:00 AM	Apr 12, 2020, 12:55:05 AM	Connected	9	52.8kb
scribbler_2020-04-11_20-00	Apr 12, 2020, 12:30:00 AM	Apr 12, 2020, 12:45:05 AM	Connected	51	55.8kb
scribbler_2020-04-11_19-45	Apr 12, 2020, 12:15:00 AM	Apr 12, 2020, 12:30:05 AM	Connected	30	36.5kb
scribbler_2020-04-11_19-35	Apr 12, 2020, 12:05:00 AM	Apr 12, 2020, 12:15:05 AM	Connected	6	31.5kb
scribbler_2020-04-11_19-20	Apr 11, 2020, 11:50:00 PM	Apr 12, 2020, 12:05:05 AM	Connected	64	95.8kb
scribbler_2020-04-11_19-05	Apr 11, 2020, 11:35:00 PM	Apr 11, 2020, 11:50:05 PM	Connected	16	26.4kb

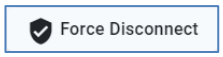
How to restore data from backup database

You can restore logs from the backup database.

Procedure

1. In the navigation pane, go to **Backup Management**.
2. In the Backup Management page, select the backup folder you want to restore. Click 

to restore the logs from the backup.
3. To delete the restored logs, select the backup folder and click 

. Logs from the real-time database are deleted.
4. Click 

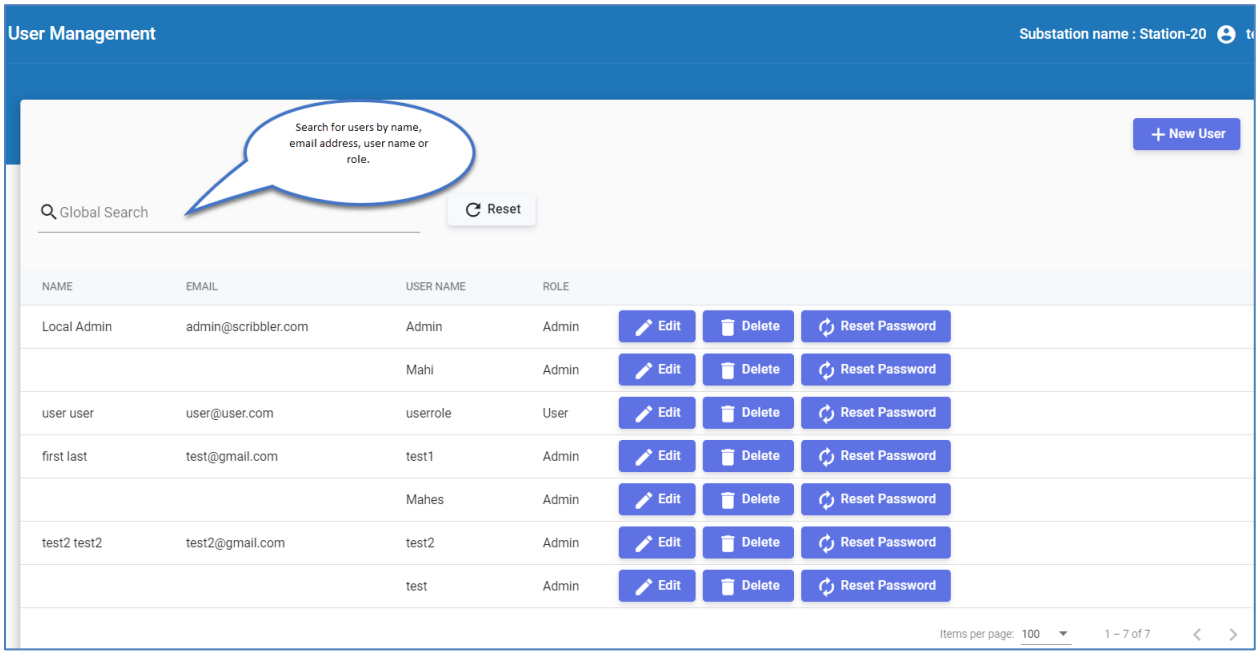
to forcibly disconnect the backup database. The data from the real-time database will be deleted immediately.

Managing user accounts

User management allows you to add and manage users for the application. The User Management option is available only for administrators.

In this page, you can search through the user accounts registered in your application. You can search for users by name, email address, user name or role. From this page you can:

- Create a new user
- Edit details of an existing user
- Delete a user
- Reset password of a user account

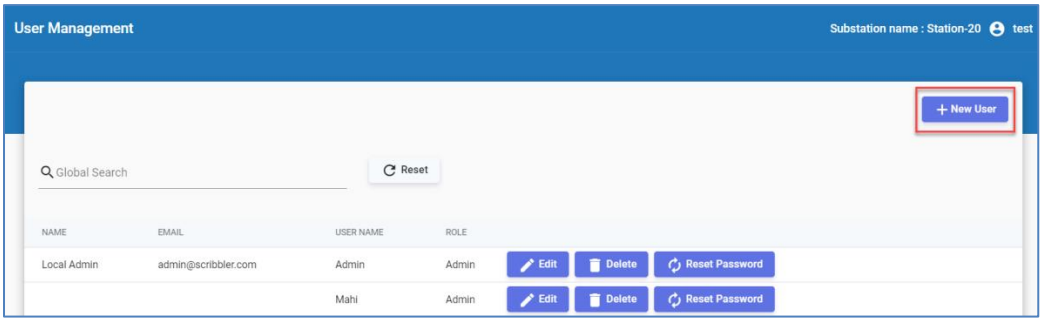


How to create new user

You can create a new user account and assign a user role to the account.

Procedure

1. In the navigation pane, go to **User Management**.
2. To add a new user, click +**New User** button at the top right corner of the page.



3. Enter the information required to create a new user such as user name, first name and last name of the user, and email address.

4. Set a password for the user profile.
5. Assign a role to the user account. Select **Admin** or **User** from the list.
6. Click 

to create the user account.

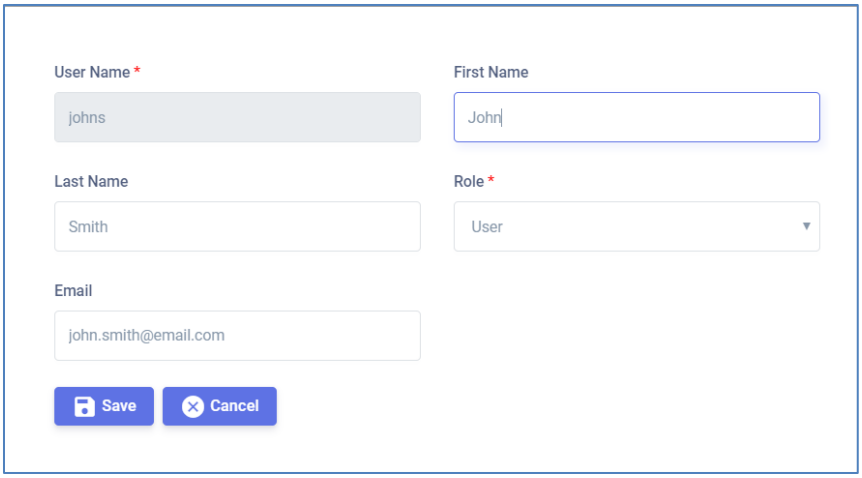
How to edit user account details

You can edit and update the user account details except the user name.

Procedure

1. In the navigation pane, go to **User Management.**
2. Search for the user whose account details you want to edit and click 

.



3. Modify the required details and save the changes.

How to delete user account

You can delete a user account that is no longer in use.

Procedure

1. In the navigation pane, go to **User Management.**
2. Search for the user account you want to delete and click 

.
3. Click **OK** in the confirmation message to delete the account.

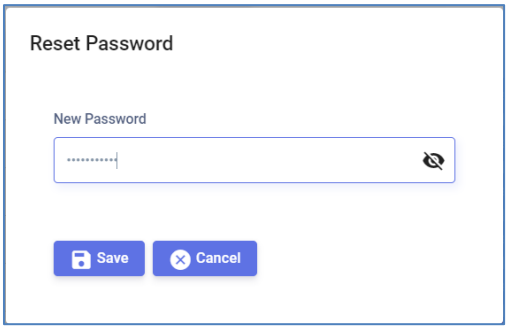
How to reset account password

Administrators can reset the password of any other user account.

Procedure

1. In the navigation pane, go to **User Management.**
2. Search for the user account whose password must be reset and click 

.



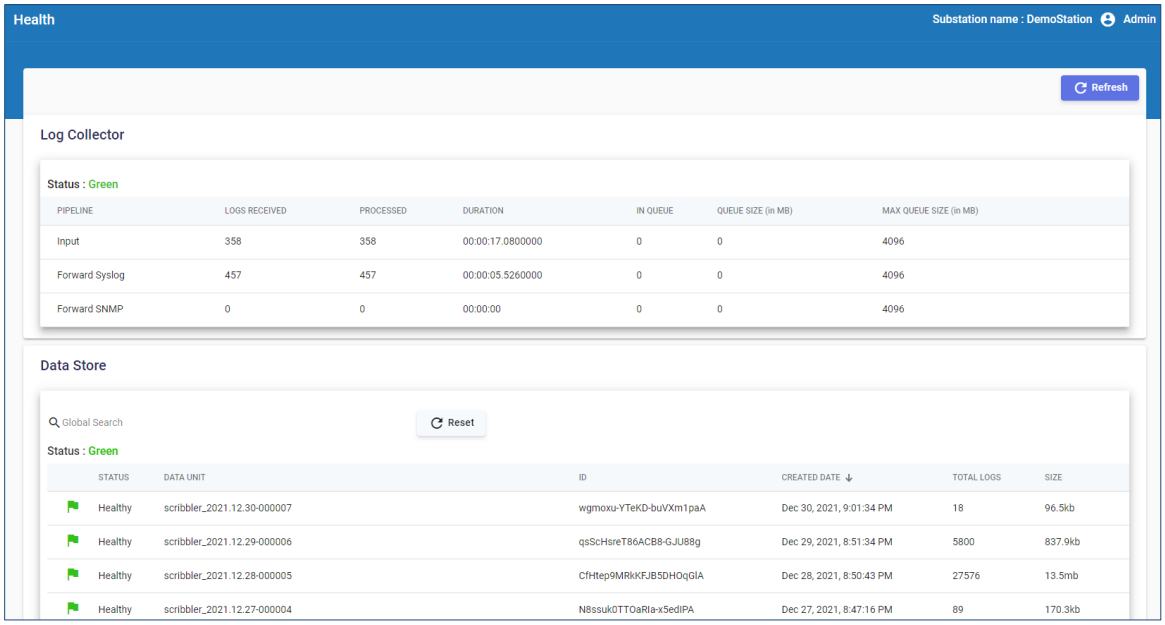
3. Enter the new password and save the changes.

Monitoring the health of stored log files

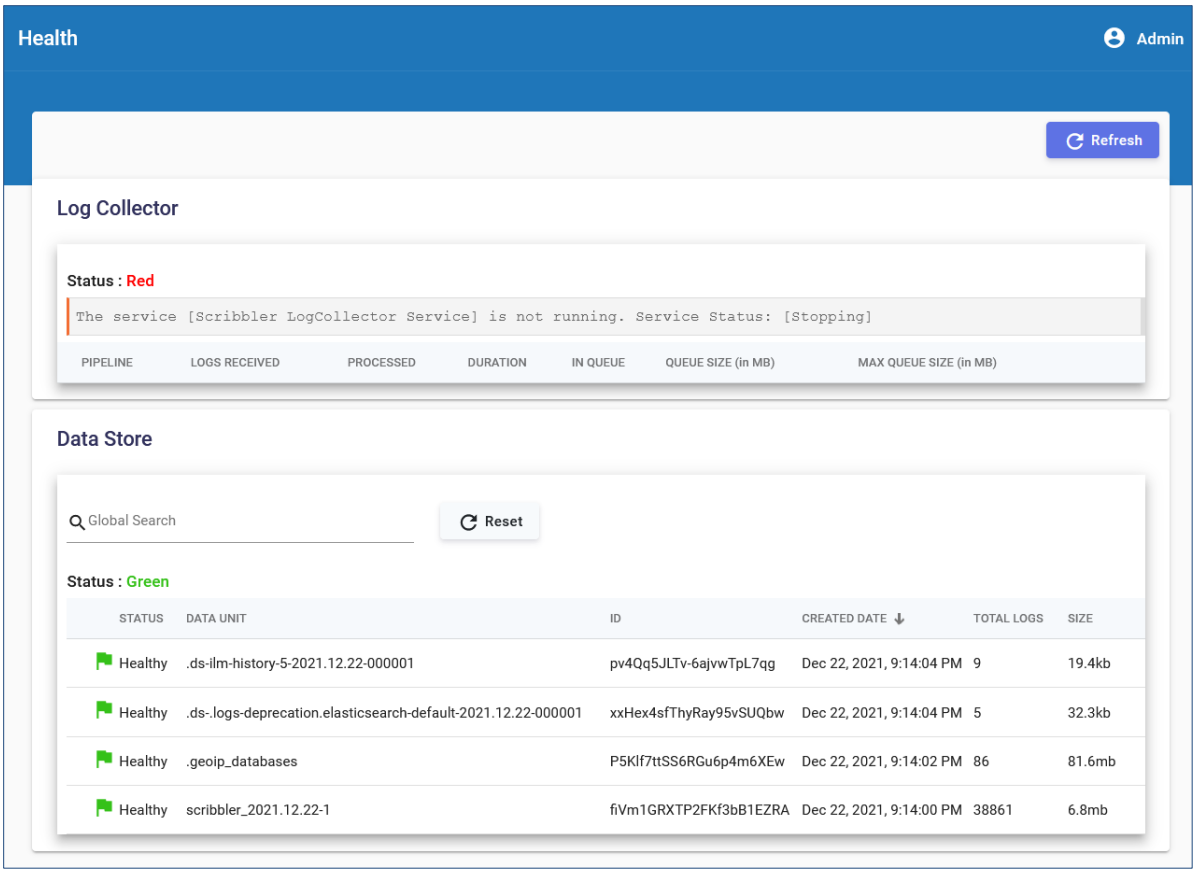
You can monitor the health of the log storage units that are created for backup purposes.

Procedure

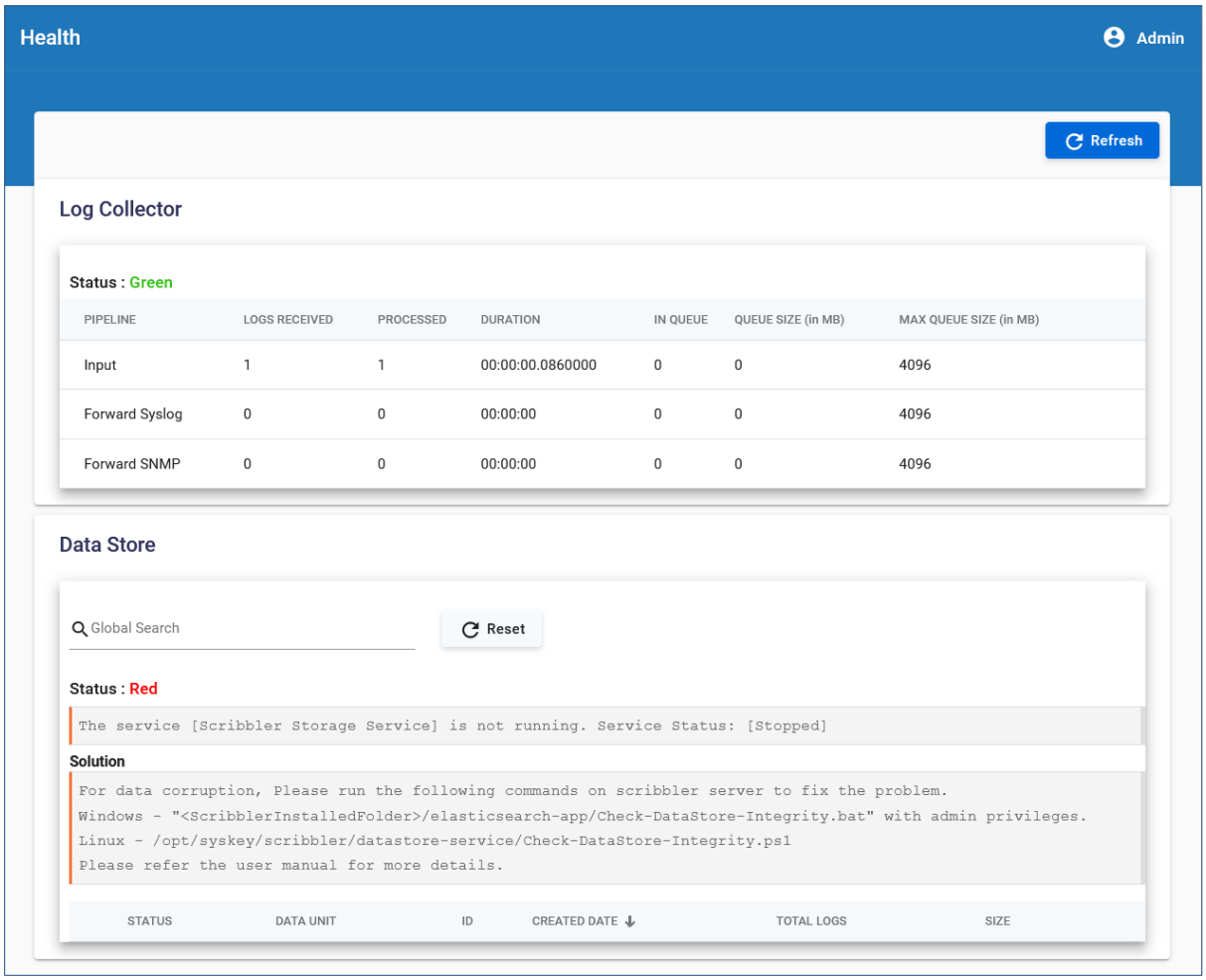
1. In the navigation pane, go to **Health**.
2. You can view the status of the current log collector storage unit, which shows the pipeline, logs received and processed and other details.
3. You can search for a particular backup storage unit with either the data unit or ID values.



If the status is green, the storage unit is working as expected and is not corrupted. If the status is Red, it might indicate that the storage unit is corrupted. The issue with the health of the storage unit is also displayed along with a possible solution.


Health
Admin
Refresh
Log Collector
Status : Red
The service [Scribbler LogCollector Service] is not running. Service Status: [Stopping]
PIPELINE
LOGS RECEIVED
PROCESSED
DURATION
IN QUEUE
QUEUE SIZE (in MB)
MAX QUEUE SIZE (in MB)
Data Store
Global Search
Reset
Status : Green
STATUS
DATA UNIT
ID
CREATED DATE
TOTAL LOGS
SIZE
Healthy .ds-ilm-history-5-2021.12.22-000001 pv4Qq5JLTv-6ajvwTpL7qg Dec 22, 2021, 9:14:04 PM 9 19.4kb
Healthy .ds-.logs-deprecation.elasticsearch-default-2021.12.22-000001 xxHex4sfThyRay95vSUQbw Dec 22, 2021, 9:14:04 PM 5 32.3kb
Healthy .geoip_databases P5Klf7ttSS6RGu6p4m6XEw Dec 22, 2021, 9:14:02 PM 86 81.6mb
Healthy scribbler_2021.12.22-1 fiVm1GRXTP2FKf3bB1EZRA Dec 22, 2021, 9:14:00 PM 38861 6.8mb

The status of the backup storage units is also displayed as either red or green depending on its health.



How to install Scribbler

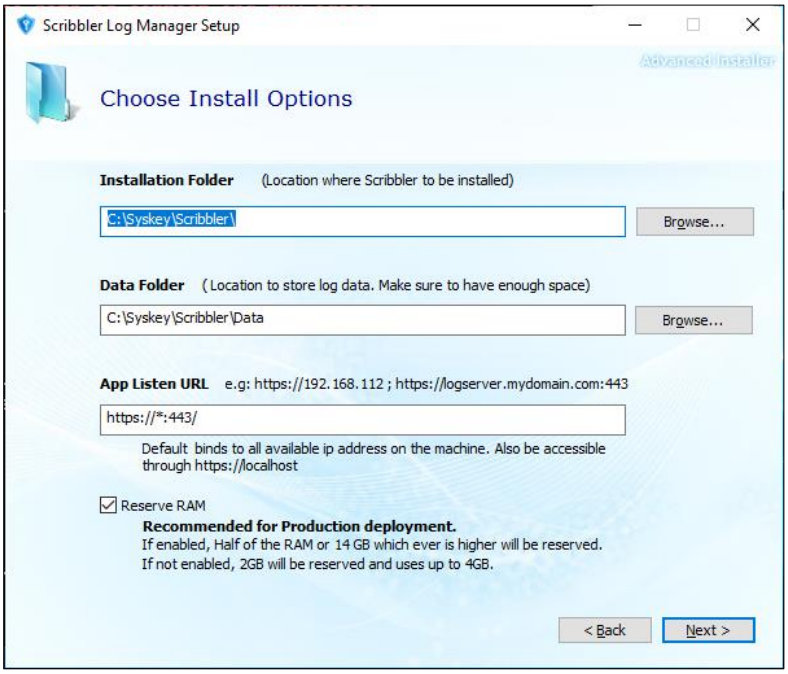
The Scribbler solution is distributed as an installable MSI package.

Procedure

1. Ensure the target environment meets the system requirements
    a. OS: Windows 2016 or higher
    b. CPU: Min 6 Core with at 2Ghz or higher
    c. RAM: 8 GB or higher
    d. Disk: 100 GB or higher (as required). RAID 1 is recommended but not required.
2. Run the installation package and follow the on-screen instructions to install pre-requisites
3. Read and accept the license agreement
4. Provide Installation parameters as shown below
    a. Install Folder – The location to install the software.
    b. Data Folder – The location to store the data files (log database, application logs,…). Make sure to have enough space on the drive.

c. App Listen URL – The address to bind the scribbler web application. The application will be accessible only through this address after installation.
   i. Ensure the port is provided is not used by any other application.
   ii. 0.0.0.0 is a special address where the solution will be accessible from all available IP address in the system (**preferred**)
   iii. Only https protocol is supported. The solution will be installed with a self-signed certificate which can be changed after installation.

d. Select the **Reserve RAM** option if you are installing the application for production use. Do not select this option if you are installing the application for development and test purposes.



5. Click **Next** and continue the installation.

How to upgrade Scribbler

Follow these steps to upgrade to latest version of Scribbler.

Procedure

1. Shutdown the following Scribbler services manually.
   - Scribbler Backend Service
   - Scribbler LogCollector Service
   - Scribbler Storage Service

   Wait for about a minute for all the services to stop completely.

2. It is recommended to take a backup of the DATA folder.

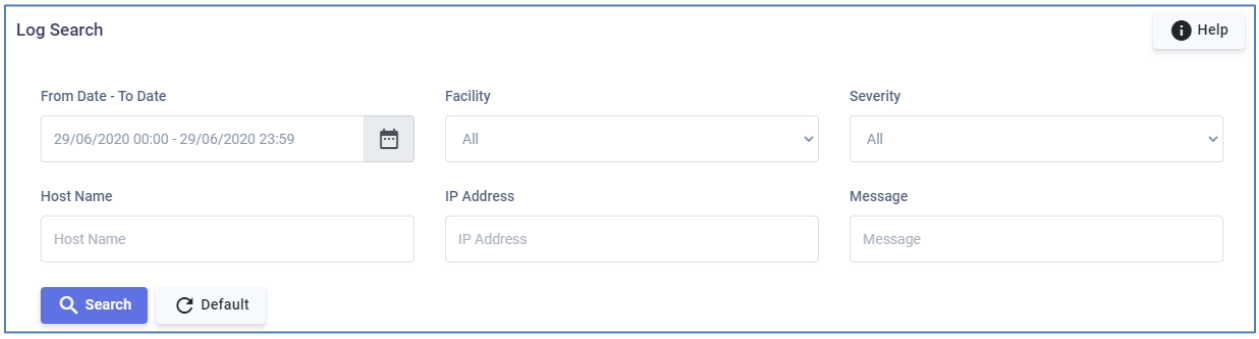
3. Run the latest installer. The installer automatically detects and uninstalls the earlier version of Scribbler.
4. Ensure that the Data Folder is correctly pointing to the older data folder path.

Log Forward

Different combinations of log forward are supported but use the following table as reference for the configuration.

Sl.No	Configuration	Comments
1	Protocol: TCP / TCP TLS Format: RFC 5424	Supported and recommended.
2	Protocol : UDP Format: RFC 3164 / RFC 5424	Supported but NOT Recommended due to the unreliable nature of the UDP protocol.
3	Protocol: TCP / TCP TLS Format: RFC 3164	NOT Recommended. RFC 5424 is superior and structured format compared to RFC 3164.

Log Search Recommendation



Sl.No	Field	Description
1	From & To Date	Option to select a date range.
2	Facility & Priority	Option to select from predefined list of Facility & Severity
3	Host	The host name. The search is always a “Starts With”. For example, a search term of “abc” will look for all hostnames starts with abc.
4	IP Address	The search term for the IP Address

Sl.No	Field	Description
		The search is always a “Starts With”. i.e. A search term of “170” will look for all IP Addresses starts with 170.
5	Message	The search term for the message **Operators** • + signifies AND operation • | signifies OR operation • - negates a single token • " wraps a number of tokens to signify a phrase for searching • * at the end of a term signifies a prefix query By default, the words in the search term are combined as OR. And the search will look for exact words. **Examples**. (Try without the surrounding single quotes) 1. 'login admin user' transforms to 'login OR admin OR user' . Search for logs which 2. 'login +admin +user' transforms to 'login AND admin AND user' 3. 'login -admin' transforms to 'login OR (NOT admin)' Search for logs which contain 'login' or not contain 'admin'. 4. 'login +-admin' transforms to 'login AND (NOT admin)' Search for logs which contain 'login' but not 'admin' 5. '"john-doe"' search for logs which matches exact or in sequence. Special chars are usually ignored. i.e. the above will match the following logs 'billi john doe' 'misc john-doe data3' 'security misc john-doe data3' But not, 'security audit by john d doe' 6. '(login +admin) | (user)' transforms to '(login AND admin) OR user' 7. 'Sys' -> Search for logs which contains exact word 'Sys' 8. 'Sys*' -> Search for logs which contains any word starts with 'Sys' Note '*' can only be used at the end. i.e. '*Sys' will NOT work.

Sl.No	Field	Description
6	Help	Click **Help** for more information about the search operators that can be used to narrow the scope of your search along with examples.

Log Collection – DNS Name Resolving

The scribbler solution supports resolving of IP addresses extracted from the log message into hostnames.

Requirements:

1. DNS server capable of reverse DNS Lookup. The default DNS server on windows environments may not be configured with reverse DNS. If not, configure it for reverse DNS lookup.
2. Correct DNS IP Address on the host machine TCP/IP properties to be present.

Once an environment fulfills the above requirements, scribbler will automatically convert the IP address into a hostname.

License Activation Process guide

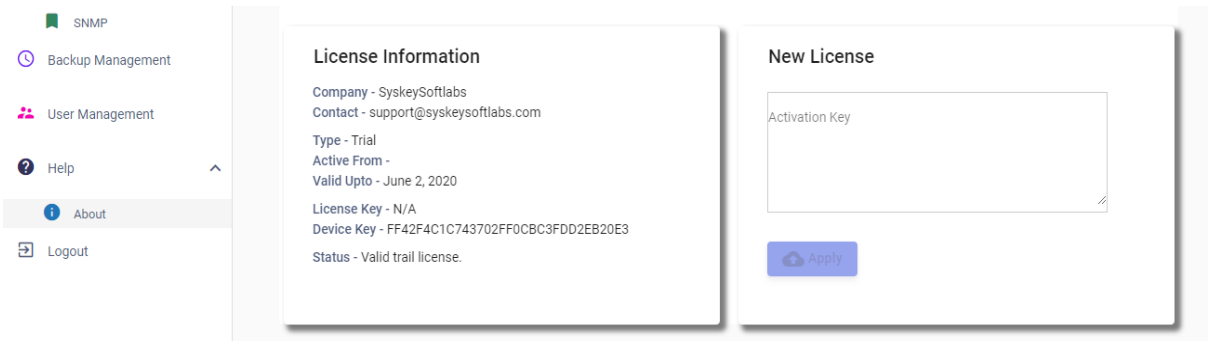
The scribbler license activation is based on a unique device key generated per installation.

Terms Associated:

- License key - Issued to the customer at the time of fulfilling a purchase order.
- Device key - Generated and available in the scribbler application after the installation on a machine in customer environment.
- Activation key - Issued to the customer by Syskey Softlabs on request by submitting the license key and device key.

Procedure

1. After the license key is issued, the customer can install the application in their environment.
2. Once installed, login to the Scribbler application and visit the “About” page.



3. Copy the device key along with the previously issued license key and send it to the support@syskeysoftlabs.com mailbox requesting activation key.

4. Once the activation key is issued by Syskey Softlabs, copy and paste it to the “New License” field and click **Apply.**
5. The license will be activated.

Configuring Exclusions from File Protection

The following Scribbler folders must be excluded from file monitoring software such as McAfee Application Control or ePO.

- <Scribbler Installed Folder>\logstash-app\temp
- <Scribbler Data folder>

Example: Configurations for McAfee Solidifier

1. Enter update mode using the command:

   ```
   sadmin begin-update
   ```

2. **Add folder exclusion for <Scribbler Installed Folder>\logstash-app\temp** using the command:

   ```
   sadmin trusted -u C:\Syskey\Scribbler\logstash-app\temp
   ```

   With the assumption that `C:\Syskey\Scribbler` is the installed folder.

3. **Add folder exclusion for data folder** using the command:

   ```
   sadmin skiplist add -i "\Syskey\Scribbler\Data"
   ```

   As the data folder path is customizable during the installation, it can be different based on the environment. Ensure that you provide the correct data folder path.

   `\syskey\scribbler\data` should match with the data folder. Drive letter is not required.

4. Exit update mode using the command:

   ```
   sadmin end-update
   ```

Example: Configurations for McAfee Application Control – ePolicy Orchestrator

Add trusted folder exclusion for logstash temp folder

Refer McAfee Application Control 8.2.0 - Windows Product Guide.

Add folder exclusion for data folder

1. On the McAfee ePO console, perform one of these actions.

   a. Create an Application Control policy or rule group.
   b. Create an Application Control policy (to apply bypass rules to one endpoint).

2. Select the Exclusions tab.

3. Click Add to open the Add exclusion rules dialog box.

4. Expand nodes for the options where you want to add bypass rules.

   - Memory protection
   - Installation detection
   - Advanced options

5. (Optional) Select Advanced options where you want to add bypass rules, then provide the required information.

   - Ignore path for file operations — Specify a relative path in the Relative Path field to ignore the relative path for file operations using the `skiplist -i` command.
   - Since the data folder path is customizable during the installation, it will be different per environment. Correct data folder path should be provided. `\syskey\scribbler\data` should match with the data folder. Drive letter is not required.

For more information, see McAfee Application Control 8.2.0 - Windows Product Guide.