SurePassID Security Information Event Management (SIEM) Sync Guide

SurePassID Authentication Server 2024

SurePassID, Corp.

360 Central Avenue

First Central Tower

Suite 800

St. Petersburg, FL 33701

USA

+1 (888) 200-8144

www.surepassid.com

Table of Contents

Table of Figures

No table of figures entries found.

What is the SIEM Sync Application?

The SurePassID SIEM Sync App reads SurePassID logs and can directly send their event data to your SIEM for ingestion or to other log locations where your SIEM can ingest them from there such as such as Windows Event Logs, Syslog, Elastic Search, formatted text files (csv, json, etc.).

Installing the SIEM Sync Application

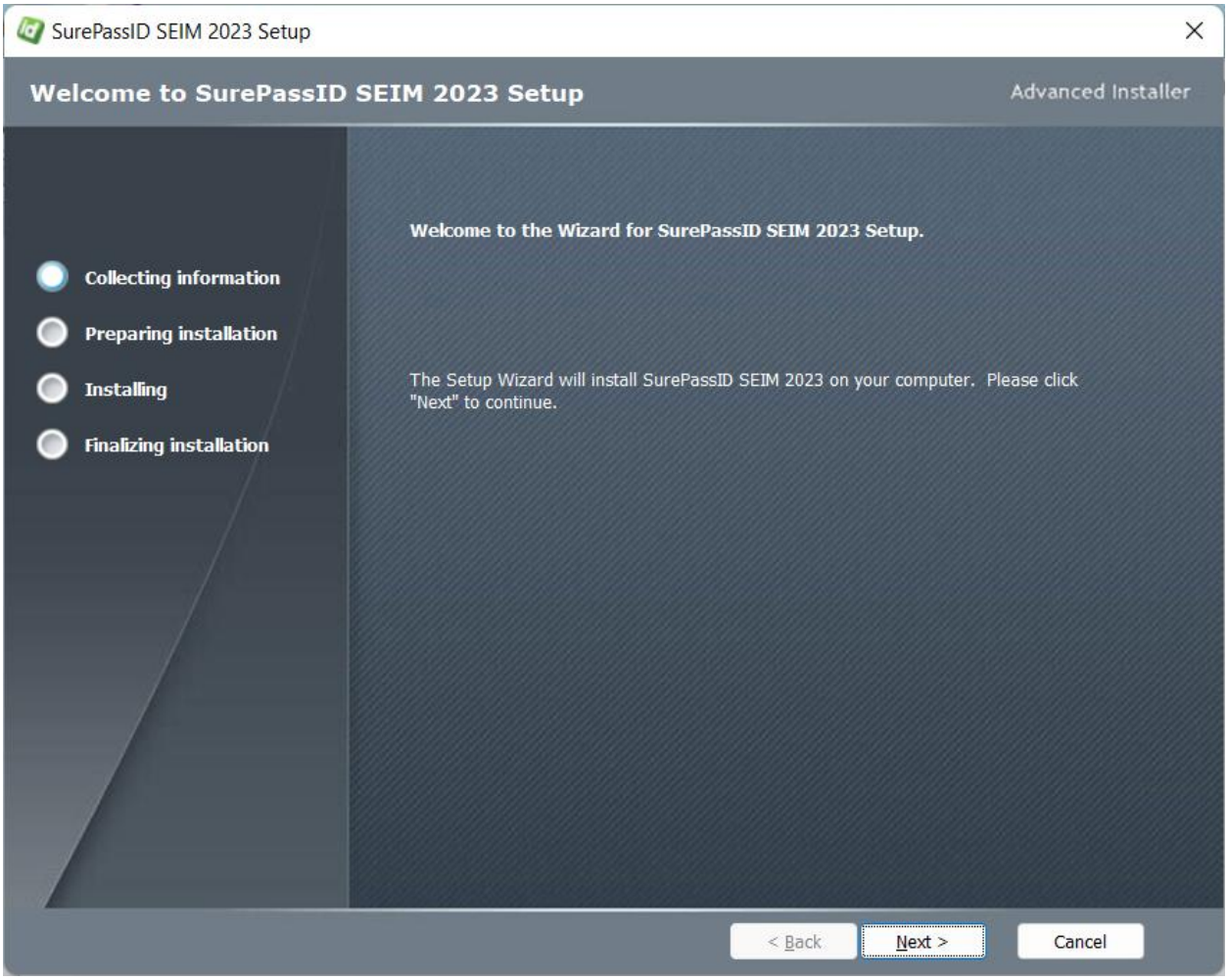
To install the SIEM application (formerly Event Log Sync) you must first download and unzip the installer from here:

https://downloads.surepassid.com/SIEM/SIEM.zip

After downloading the file unzip, unzip the file and run the installer file **SurePassID_SIEM2023.exe**

The installer and application is digitally signed by SurePassID. You must verify that as part of the installation.

Then you will see the following installation screen.

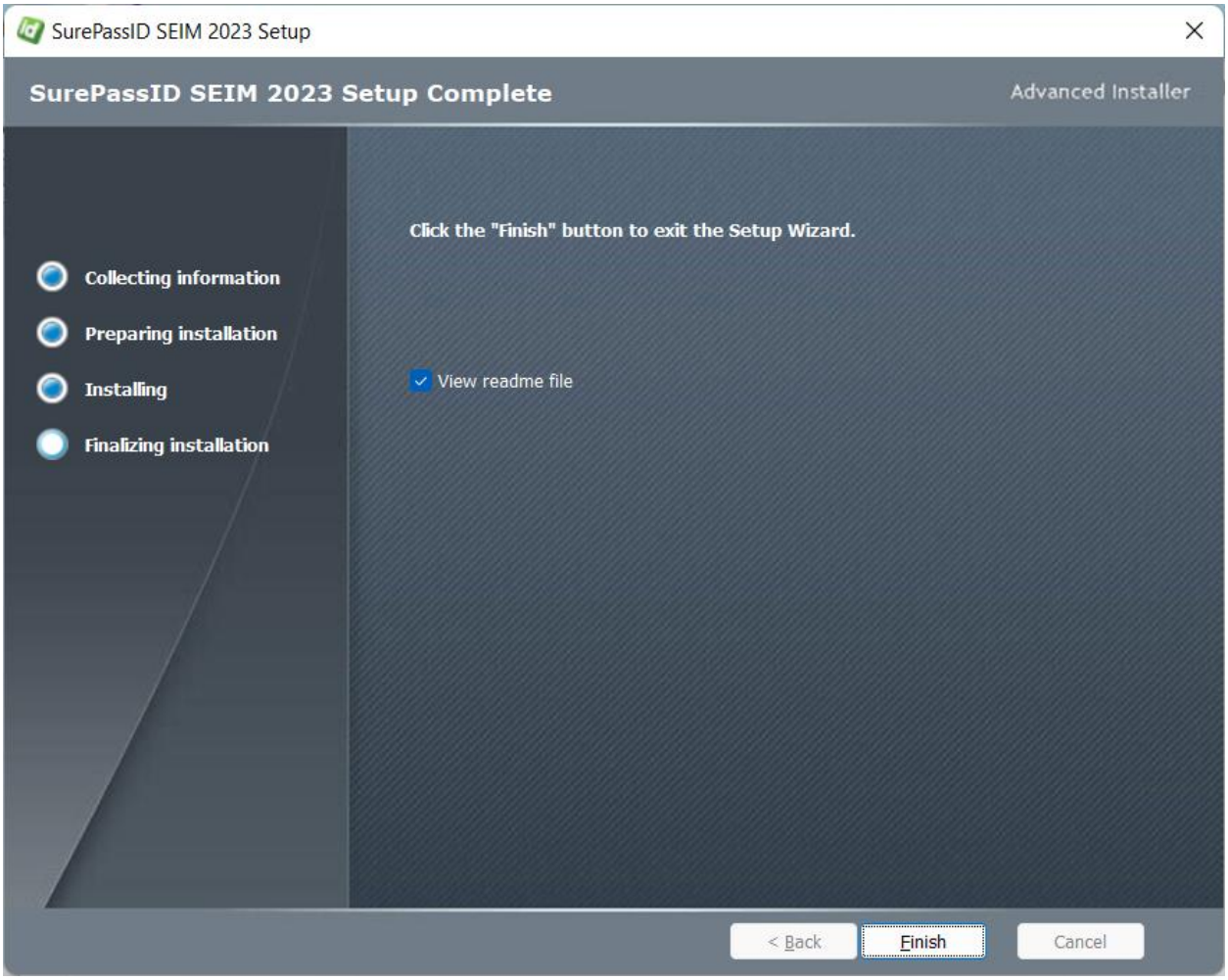


Follow the prompts until you get to the **User Access Control screen.**

<u>You must verify that the publisher is SurePassID Corp. If not, then press the No button.</u>

When you press the **Yes** button the SEIM 2023 will be installed.

When installation is complete you will see the following screen:



Press the **Finish** button to complete the installation**.**

The SEIM 2023 will be installed in the following folder:

C:\Program Files (x86)\SurePassID Corp\SurePassID SEIM 2023

The EventLogSync.exe is located in that folder.

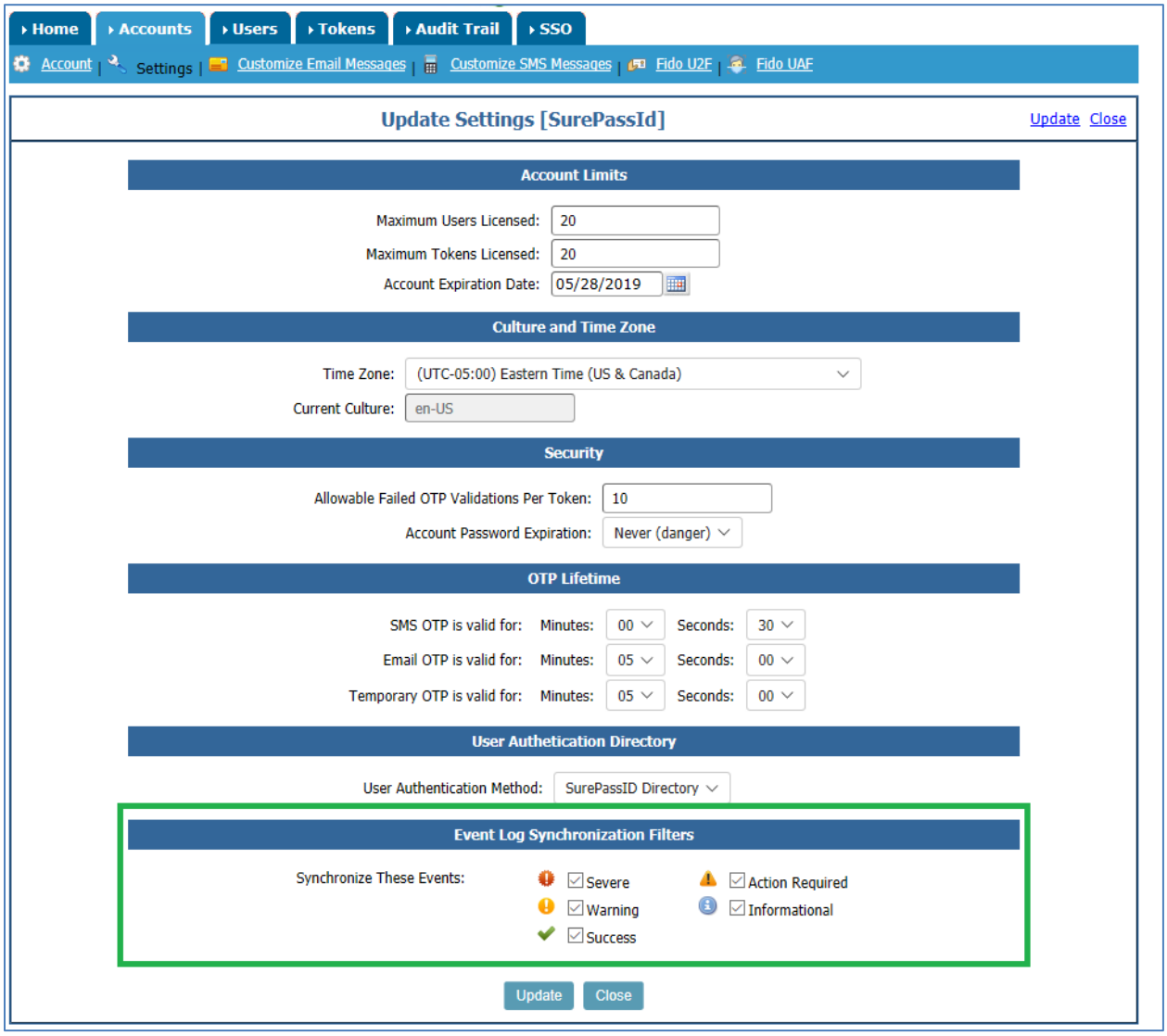
Configuring the SIEM Application

The SIEM application is an application that pulls information from the SurePassID Audit Trail and sends it to a number of different logging systems referred to as targets. SIEM application is delivered as a command line application or an Azure Web Job.

The system supports the following log targets:

- Windows Event Log
- Syslog Format – TCP (TLS and plain text transports)
    - Splunk
    - Loggly
    - Elastic Search
    - All Syslog based listeners
- Windows Azure Sentinel
- Rapid7 – Native
- File System Formats
    - Delimited text file
    - Json – Proper Json formatted file for log ingestion
    - Json Splunk – Alternate format for ingesting into Splunk

SIEM only retrieves specific events that your SurePassID account is configured for. This allows you to only retrieve a subset of audit log information (such as errors only) and not all audit trail records. The audit events that are eligible for synchronization are set in your SurePassID Account Settings as highlighted in green below:



EventLogSync.exe creates a trace log each day it runs. This file is good for trouble shooting connectivity issues, reviewing process health, etc. The trace logs are stored in the trace folder and there is a new log file created for each day the EventLogSync runs. The location of the trace folder is:

C:\Program Files (x86)\SurePassID Corp\SurePassID SEIM 2023\Trace

Running SurePassID EventLogSync App

EventLogSync.exe can be run via the command line or via the app configuration file (EventLogSync.exe.config).

The EventLogSync can read the SurePassID log information via the MFA server REST API as well as the Direct Connect via the database directly. If you are using SurePassID in the cloud you must use the REST API. If you are running SurePassID MFA server on-prem or in your private cloud you can use either method. However, the database direct connectivity is preferred as it is much faster than the REST API. The -syncapi parameter is determines which method is used.

To run the application from the command line and use the following syntax:

```
EventLogSync    [-ln=login-name]
                [-lp=login-password]
                [-dbconnection=sqlserver-connection-string]
                [-syncapi=api-protocol]
                [-restendpoint=sp-server-endpoint]
                [-targettype=log-target-type]
                [-targetfilesystemformat =log-target-file-system-format]
                [-targetendpoint=log-target-endpoint]
                [-targetport=log-target-port]
                [-maxsyncitems=record_count]
                [-sd=syslog_account-identifier]
                [-runoption=run-option]
                [-continuosrunwaittime=wait-time-between-runs]
```

The command line parameters are explained below.

MFA Server Connection

- **-ln** – SurePassID account login name
- **-lp** – SurePassID account password
- -**syncapi** – The parameter sets the method to get SEIM data from SurePassID MFA server.
    - **REST**- This parameter uses the MFA server REST api

- **Database** – This parameter is used for Direct Connect access to the database

- **-dbconnection** – SQL Server database connection string. All the possible connection string options are documents here: SQL Server Database Connections.

  NOTE: It is strongly recommended that you create a unique SQL Server account (limited access) to the MFA server database. See Database User Permissions in a subsequent section.

  - Sample SQL Server authentication:
    Data Source=<sqlserver_server>;
    Initial Catalog=<surepassid_database>;
    User id=SIEM_User;
    Password=<surepassid_sqlserver_password>;Integrated Security=false

  - Sample SQL Server windows authentication (service or managed service accounts):
    Data Source=<sqlserver_server>;
    Initial Catalog=<surepassid_database>;
    Integrated Security=true

- **-restendpoint** – SurePassID Authentication server endpoint URL. In most cases, you will not need to change this unless you are using a custom SurePassID installation. Not required if you are using **-dbconnection**. The values are:
  - **sandbox** – The SurePassID sandbox cloud (mfa-sandbox.surepassid.com) system.
  - **prod** – The SurePassID production cloud system.
  - **on premises system** – The on-premises or custom SurePassID server endpoint. The format of this parameter is usually:

https://<surepassid-server>/AuthServer/REST/OATH/OathServer.aspx

Synchronization Targets

- **-targettype** – The log target to sync with.
  - **e**=Windows Event Log
  - **s**=syslog
  - **l**=log4net
  - **f=**file system
  - **m=**Microsoft Sentinel
- **-targetfilesystemformat** – the format options for targettype=f

- **t=**delimted text file
- **j=**json
- **s=**json fomat for Splunk ingestion

Synchronization Process Options

- **-maxsyncitems** – Count of records that EventLogSync will process in each processing run. 0=process all records that are eligible for sync. The default is 0.
- **-runoption** – EventLogSync can be configured to perform one processing run and stop, or it can be configured to run continuously performing an endless number of processing runs. Regardless, it will always try to process **maxsyncitems** records each time it runs**.** If running continuously, EventLogSync can sleep between processing runs. The amount of time that is sleeps is determined by **continuousrunwaittime**. o=run once, c=continuous. Default is run once.

-continuousrunwaittime – The count of seconds that EventLogSync to wait between processing runs when operating in continuous mode.

Syslog Specific

- **-targetendpoint** - The IP of the target system listener endpoint.
- **-targetport** - The port that target system listener endpoint. Default is 6514.
- **-sd** - Syslog systems can require that the calling entity must provide an account identifier as part of the Structured Data Element to add log records. The form is usually uuid@41058. However, this value can be anything and is determined by target syslog provider. For systems that require this (such as Loggly) you must provide this parameter (to identify your Loggly tenant) or syncing will fail.

Note: **When you start EventLogSync.exe** You will be presented with the **User Access Control screen.**

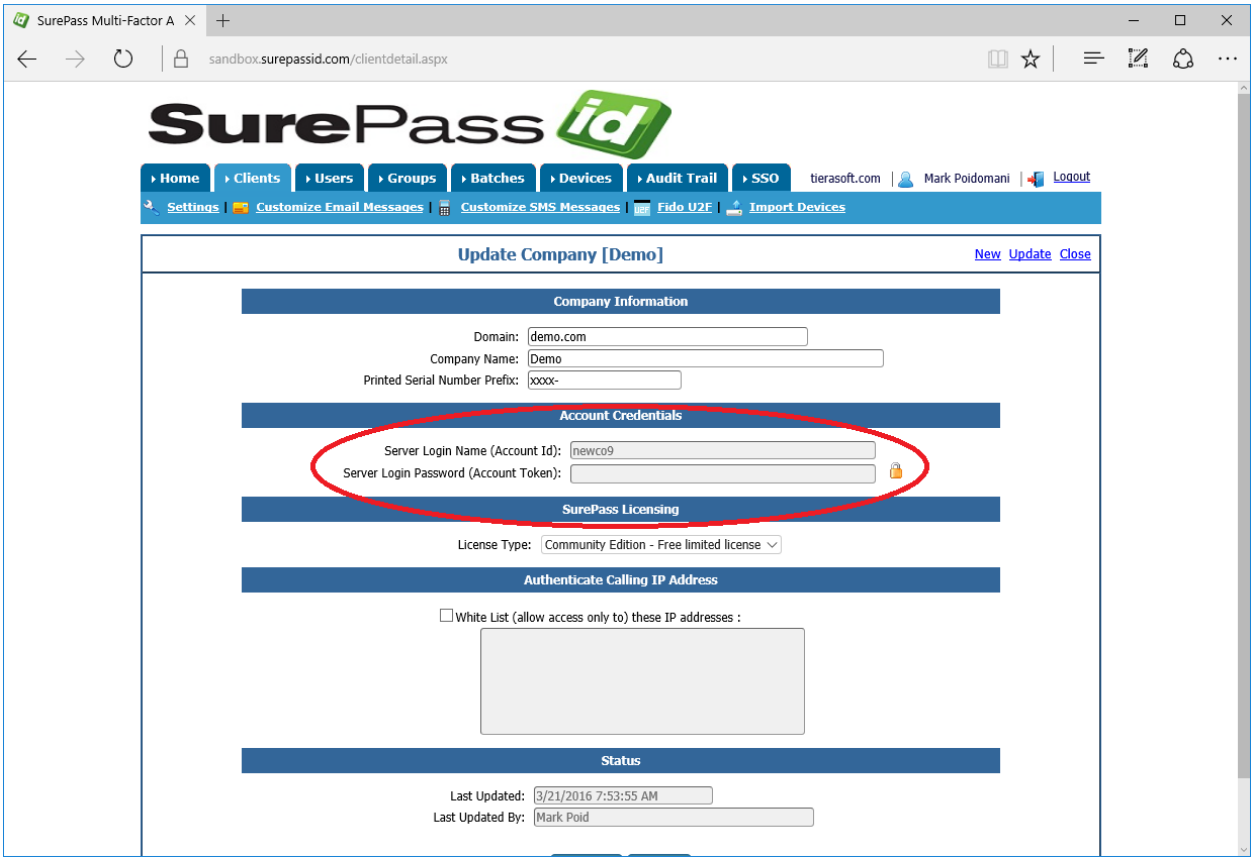
You must verify that the publisher is SurePassID Corp. If not, then press the No button.

Using the REST API to Sync with SurePassID MFA Server

If you are using the SurePassID cloud version, then you must the REST API to sync with SurePassID MFA Server.

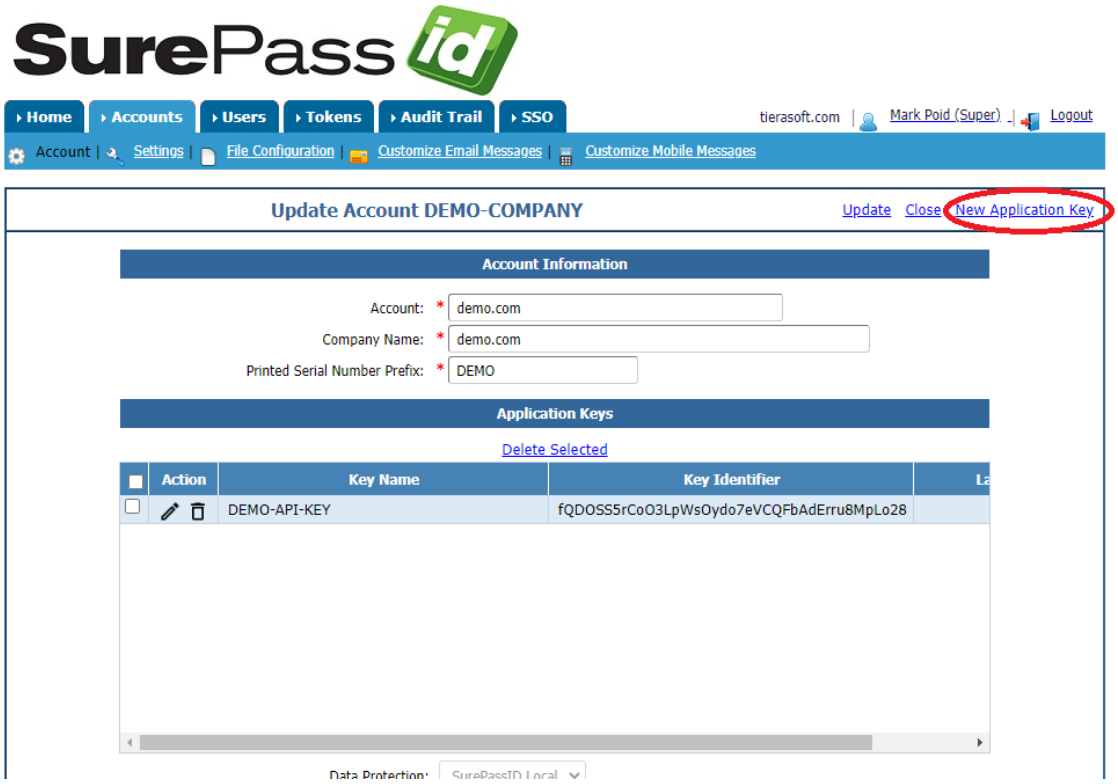
To sync events from SurePassID to another event log source you need to identify your SurePassID account via specifying the **-ln** and **-lp** parameters.

If you are using an older version of SurePassID MFA Server, you will see the following info for your account as shown below.

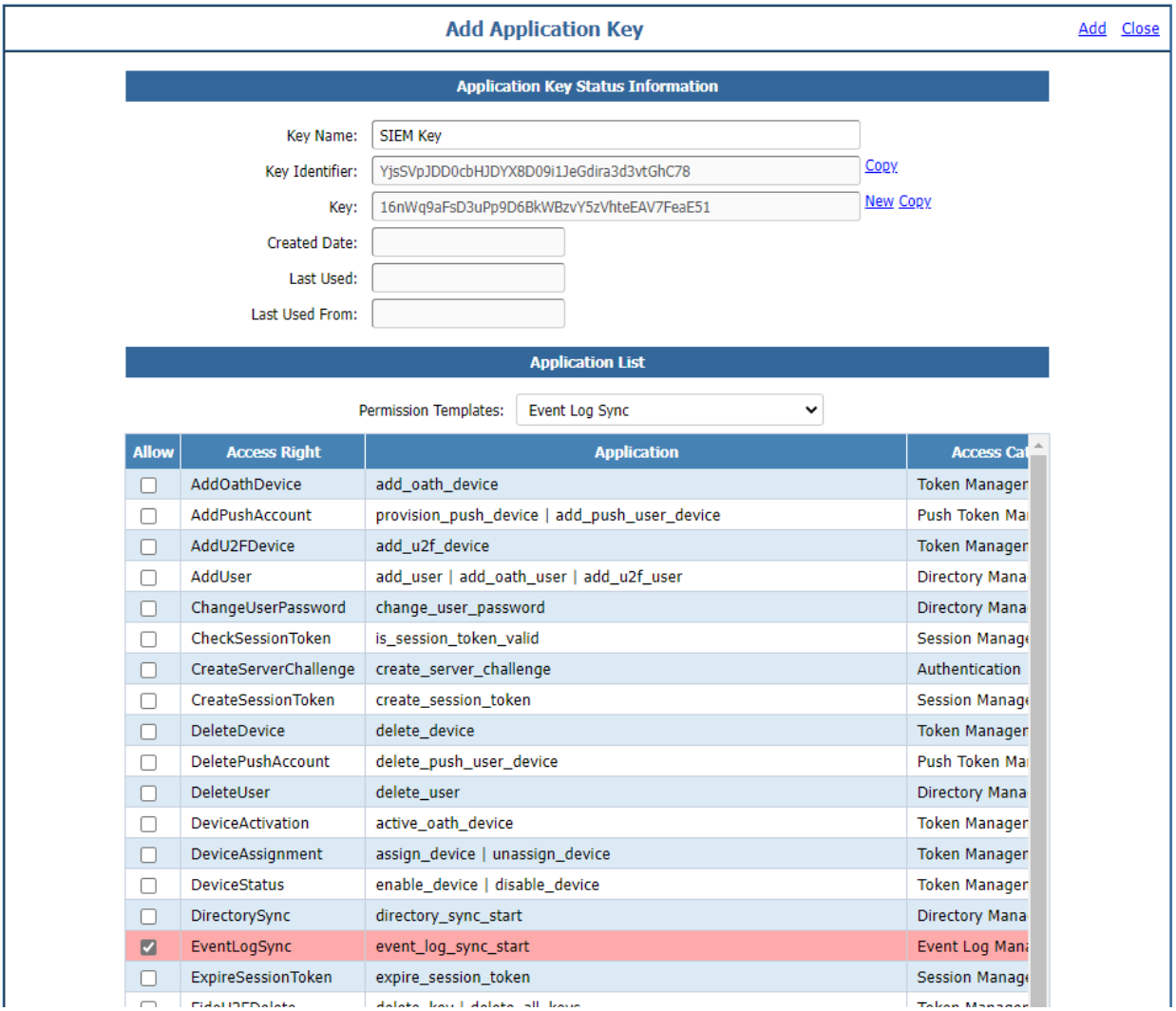


The **Server Login Name** parameter is the -**ln** and the **Server Login Password** parameter is the -**lp**. To view the **Server Login Password**, click the 'lock' icon to toggle the display of the password.

If you are using the latest version of SurePassID you will see the following info for your account:



All application requests to the MFA Server require an **Application Key**. To create a new **Application Key** just for **EventLogSync** app (recommended) click the **New Application Key** link and see the form below:



The **Key Name** is the friendly name to identify this key. It is not used for any security purposes. For instance, you could name it **SIEM Key**.

Select the **Event Log Sync** from the **Permissions Templates** drop down list.

The **Key Identifier** parameter is the -**In** and the **Key** parameter is the -**Ip**. and press the **Add** button.

Copy **Key Identifier** and **Key** for later use when configuring **EventLogSync** app. One you click the **Add** button the **Key** will not longer be viewable. If you forget the **Key**, you can delete this **Application Key** and add a new one.

A word of caution. Once an **Application Key** is deleted any application that is currently using that **Application Key** will no longer be permitted access to the MFA Server and the application will fail. An **Application Key** cannot be recovered. A new one must be created, and the application must be updated to use the new **Application Key**.

Using Direct Connect to Sync with SurePassID MFA Server

SurePassID on-premises users can optionally use the Direct Connect Sync option to sync directly from the SurePassID database to external sync sources. To use Direct Connect Sync you must specify the **-dbconnection** parameter on the command-line. Direct Connect Sync has the following advantages over the REST API Sync:

- More efficient and high throughput rate than the REST API
- More flexible connection options to meet your compliance and governance requirements.
- Capable of syncing additional SurePassID system management specific events not available via the REST API Sync.

Direct Connect Database User Permissions

The SQLServer account that will access the MFA database requires the following permissions:

SELECT ON the following tables:

- Partner
- PartnerSettings
- PartnerUserAudit

UPDATE ON the following tables:

- PartnerSettings,
- PartnerUserAudit

If you plan to use SQLServer authentication you would run the following script after creating a strong password and entering it between the single quotes following PASSWORD=:

```
CREATE LOGIN [SIEM_User] WITH PASSWORD = 'replace with strong password', DEFAULT_DATABASE=[SurePassDB_2022], DEFAULT_LANGUAGE=[us_english], CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF

CREATE USER SIEM_User FOR LOGIN SIEM_User WITH DEFAULT_SCHEMA=[dbo]

GRANT SELECT ON [Partner] TO SIEM_User
```

```
GRANT SELECT ON [PartnerSettings] TO SIEM_User
GRANT SELECT ON [PartnerUserAudit] TO SIEM_User
GRANT UPDATE ON [PartnerSettings] TO SIEM_User
GRANT UPDATE ON [PartnerUserAudit] TO SIEM_User
EXEC sp_addrolemember 'db_datareader', 'SIEM_User'
```

The script **Create_SEIMUserSqlServer_Auth.sql** can be found here:

C:\Program Files (x86)\SurePassID Corp\SurePassID SEIM 2023\Database Scripts

If you plan to use Windows authentication (STRONGLY RECOMMENDED) you would run the following script after adding a windows account (Managed Service Account would be good. e.g. SIEM_User) to allow access to the database:

```
GRANT SELECT ON [Partner] TO SIEM_User
GRANT SELECT ON [PartnerSettings] TO SIEM_User
GRANT SELECT ON [PartnerUserAudit] TO SIEM_User
GRANT UPDATE ON [PartnerSettings] TO SIEM_User
GRANT UPDATE ON [PartnerUserAudit] TO SIEM_User
EXEC sp_addrolemember 'db_datareader', 'SIEM_User'
```

The script **Create_SEIMUserWindows_Auth.sql** can be found here:

C:\Program Files (x86)\SurePassID Corp\SurePassID SEIM 2023\Database Scripts

Command line Options for SurePassID EventLogSync

The table below provides the parameters required for each target type:

Parameter Name	Target System (-targettype)	**REST API** **M**andatory/ **O**ptional	**Direct Connect** **M**andatory/ **O**ptional
-ln	all	M	M
-lp	all	M	M
-syncapi	all	M	M
-dbconnection	-targettype=f	N/A	M
-restendpoint	windows event log, syslog	M	N/A
-targettype	all	M	M
- targetfilesystemformat	For -targettype=f	O	O
-targetendpoint	syslog, log4net	M	M
-targetport	syslog	O	O
-maxsyncitems	all	O	O
-sd	syslog	O	N/A
-runoption	windows event log, syslog	O	O
-continuosrunwaittime	windows event log, syslog	O	O

Command line Options for SurePassID Direct Connect Sync

The table below provides the parameters required for log target parameters for each lop target:

Parameter Name	Target System	**M**andatory/ **O**ptional
-ln	windows event log, syslog	M
-lp	windows event log, syslog	M
-dbconnection	windows event log, syslog	M

-syncapi	windows event log, syslog	M
-targettype	windows event log, syslog	O
-targetendpoint	syslog	M
-targetport	syslog	O
-maxsyncitems	windows event log, syslog	O
-sd	syslog	O
-runoption	windows event log, syslog	O
-continuosrunwaittime	windows event log, syslog	O

Deployment Configurations

SIEM is a Windows console app that can be deployed in a variety of configurations. Some such configurations are:

- Scheduled Task
- Azure WebJob
- AWS Lambda
- Any App (via SurePassID API)

SIEM uses the SurePassID Server REST API (SurePassID cloud system) or direct connection to the database (SurePassID on-prem/private cloud). You can add the same functionality into any app and deploy it in any manner you require. For instance, you could incorporate SIEM into your app and to send the logs to any log target including databases, text files, etc. on any platform using any programming language. Alternatively, you could use curl and sync the SurePassID audit trail directory into syslog on a RHEL 7 or Ubuntu platform. The possibilities are unlimited.

Sample Command examples for SurePassID REST API Sync

Push groups of 100 SurePassID records to windows event log one time:

eventlogsync -ln=<your surepassid account id>

-lp=<your surepassid account token>

-syncapi=REST

-restendpoint=https://sandbox.surepassid.com/AuthServer/REST/OATH/OathServer.aspx

-targettype=e

-systemname=test

-maxsyncitems=100

-runoption=o

Continuously push groups of 100 SurePassID records to windows event log:

eventlogsync -ln=<your surepassid account id>

-lp=<your surepassid account token>

-syncapi=REST

-restendpoint=https://sandbox.surepassid.com/AuthServer/REST/OATH/OathServer.aspx

-targettype=s

-targetendpoint=us.data.logs.insight.rapid7.com

-targetport=13604

-maxsyncitems=100

-targetignorecerterrors=0

-systemname=test

-runoption=c

Sample Command examples for Direct Connect Sync

Push groups of 100 SurePassID records to windows event log one time:

eventlogsync

-ln=<your surepassid account token>

-lp=<your surepassid account key>

- dbconnection=**Data Source="<sqlserver_server>;**

Initial Catalog=<surepassid_database>;
User id=SIEM_User;
Password=<surepassid_sqlserver_password>;Integrated Security=false"

-targettype=e

-systemname=test

-maxsyncitems=100

-runoption=o

Security Considerations

SIEM Application uses TLS 1.2 for transport security. If you need a greater level of security, please contact SurePassID technical support and we can assist in setting up message level security using X509 certificates.

Sample Formats