SurePassID Support Guide

SurePassID Authentication Server 2020

Table of Contents

SurePassID, Corp.
13750 W. Colonial Drive
Winter Garden, FL 34787
+1 (888) 200-8144
www.surepassid.com

Introduction

This guide explains the SurePassID support model. Its purpose is to provide a reference for system administrators.

Information on the following topics is provided:

- **Support Options**
  - An explanation of the SurePassID service tiers.
- **Customer/SurePassID Support Responsibilities**
  - Division of support responsibilities for system administrators and end users. Also addresses White Label Customers and Managed Service Providers (MSPs).
- **How do I submit a support ticket to SurePassID?**
  - Detailed explanations of the methods for submitting support tickets to SurePassID.
- **Updates, Patching and Maintenance**
  - Policies and procedures that SurePassID uses for occasional patching and maintenance of the server codebase and mobile applications.
- **Scheduled Downtime**
  - Scheduled downtime if needed by SurePassID or customers.
- **Common vulnerabilities and Exposures (CVE) Contingency Plan**
  - How SurePassID will deal with the contingency of a CVE discovery.

Other SurePassID Guides

This SurePassID guide has companion guides that provide additional detail on the SurePassID system:

SurePassID Portal

- Developer API Guide
- FIDO U2F Mobile API Guide
- System Administration Guide
- Local Agent Guide
  - High performance RADIUS Server
  - Windows Event Log Synchronization
  - Active Directory Synchronization
- Desktop Authenticator Guide
- Google Authenticator Guide
- SurePassID Mobile Authenticator Guide
- Mobile API Connector
- Windows Credential Provider Guide
- Self-Service Portal

Support Options

The level of service is specified in your SurePassID contract. In addition to standard service (Bronze Coverage) which is included with all subscription licenses, there are two levels of premium service (Gold and Silver Coverages) which are available at additional cost:

Level of Service	Service Scope	Price of Coverage*
Gold Coverage	✓ Receive Telephone and Email Support with free remote assistance using online meeting software such as GoToMeeting, where applicable. ✓ Receive support for service requests up to **Expert Level.** ✓ Service requests receive the highest level of priority and will be responded to **within two (2) hours** following the submittal of the request. ✓ **24/7/365 support service**.	$1/user/month
Silver Coverage	✓ Receive Telephone and Email Support with free remote assistance using online meeting software such as GoToMeeting, where applicable. ✓ Receive support for service requests up to **Advanced Level.** ✓ Service requests receive a higher level of priority than Bronze service requests and will be responded to **within one (1) business day** following the day of the request.	$0.50/user/month
Bronze Coverage	✓ Receive Email support. ✓ Receive support for service requests up to **Basic Level**. ✓ Service requests will be responded to within five (5) business days following the day of the request.	Included with all subscription licenses.

**All pricing subject to change. Based on SurePassID pricing effective Q1 2020.*

Customer/SurePassID Roles & Responsibilities

SurePassID works closely with you and your internal IT personnel to ensure that issues are ticketed, worked, and resolved. Our support model is based on the division of roles and responsibilities below.

System Administrators

SurePassID is Level 1 support for system administrators with SurePassID-related issues. We are successful if you are successful, so we also encourage you to seek our help whenever our domain expertise may be helpful.

End Users

Unless specified otherwise in your SurePassID subscription agreement, SurePassID does not provide support for end users**. Only the customer's system administrators or designated helpdesk personnel are authorized to help end users enroll, activate, reactivate, or troubleshoot SurePassID-related issues**.

These are key customer responsibilities:

- **Level 1 support** for any issue, whether end user-related or software-related.
- **Assign specific internal technical support staff** who will be responsible to create new support tickets and serve as the liaison(s) to SurePassID.
- **Manage the issues/tickets submitted by end users and administrators**. This includes priority setting/changing, providing log details, screen shots, and other details to help SurePassID diagnose and resolve the issue.
- **Recreate potential issues and document the set of steps required to recreate the issue**. For issues that are intermittent, SurePassID will work with you to generate documentation which will help diagnose the issue.

White Label Customers and MSPs

In addition to all of the above, White Label customers and MSPs are responsible for:

- **End user procedure documentation**. SurePassID provides initial documentation for standard or customized software/functionality. Customers are encouraged to "make it their own" by rebranding (if desired) and incorporating internal references specific to their policies and procedures.

How to Submit a Support Request

There are three ways to submit a support request to SurePassID. All will result in creation of a support ticket, the sending of a confirmation email to you, and ensuing support during the hours of your service coverage window.

helpdesk@surepassid.com

https://support.surepassid.com

+1 (888) 200-8144, option 2

By Email

Send an email to **helpdesk@surepassid.com.** You will receive an acknowledgement email indicating that someone at SurePassID Support will follow up with you.

If you would like to create a SurePassID Portal account to view and manage your tickets, click the View Ticket link in the confirmation email and follow the New User Signup prompt.

Via the SurePassID Portal

If you have already created a SurePassID Portal user account, login to **https://support.surepassid.com**. Select **Submit A Ticket**, select the priority of your request, and enter a description of your issue with optional attached screenshots.

By Phone

Call 888-200-8144, option 2. This will route the call to the support representatives on duty. A ticket will be created over the phone and you will receive a confirmation email (explained above).

Updates, Patching and Maintenance

SurePassID regularly updates its cloud MFA service, server codebase, and mobile apps. These updates are documented in release notes which are available to system administrators via the SurePassID Portal.

Schedule

- **Major software releases** – Quarterly or biannually.
- **Minor updates or patches** – As needed, typically overnight or on weekends.
- **Critical patches** – As soon as possible.

Notification

- **Major software releases** – You will receive 60 days advance notice with details of the pending releases.
- **Minor updates or patches** – You will receive a minimum of 10 days advance notice with details of the pending update or patch.
- **Critical patches** – You will receive a critical patch alert and deployment time frame, along with a request for urgent coordination with SurePassID.

Procedure

- **Major software releases** – SurePassID will coordinate with you to ensure that any required technical activities are performed at a time of your choosing before the major software release is deployed. Customers may request early test deployments of new features or functionality of compelling interest to them.
- **Minor updates or patches** – SurePassID will coordinate with you to ensure that any required technical activities are performed at a time of your choosing before the minor updates or patches are deployed.
- **Critical patches**
    - For Cloud MFA customers, the critical patch will be applied on the designated date/time if a server restart is not required. If a server restart is required, the critical patch will be applied overnight to minimize any user disruption.
    - For On-Prem MFA customers, it is up to the customer to determine when to apply the critical patch in consultation with SurePassID.
    - For customers using a SurePassID Mobile Authenticator app, critical patches are assigned our highest internal priority and deployed as fast as possible, given the potential impact to tens of thousands of users.

Testing, Preparation and Rollback

SurePassID follows a comprehensive software development process that spans testing, verification, vulnerability checking, and documentation. Prior to any software release or patch where databases and/or major functionalities are changed, SurePassID completes and verifies a full system backup. If anything goes wrong after a deployment, a full system restore can be performed to roll back the deployment. Any such development is carefully coordinated between SurePassID and impacted customers.

Scheduled Downtime

SurePassID is a mission-critical, high-availability provider with an overall Service Level Agreement (SLA) performance of >99.99% uptime. However, there are times when customers require scheduled downtime for hardware changes, network reconfigurations, and other reasons. If you require a scheduled downtime, SurePassID will coordinate with you as needed to ensure minimal disruption to your users and business processes.

Common Vulnerabilities and Exposures (CVE) Contingency Plan

SurePassID has undergone regular third-party software vulnerability testing for over 10 years. No CVEs have been found to date. However, we maintain the following action plan should that contingency arise.

- If a CVE is discovered, SurePassID will immediately launch an internal escalation process to determine the severity and potential impact to our customers.
- Our Development team will provide a fix and critical patch or update plan depending on the severity/risk/impact.
- Our Product Management team will perform QC testing and regression testing of all modules affected by the vulnerability and its remediation.
- The SurePassID Product Manager will draft a CVE Notification which addresses the vulnerability, the remediation, and the deployment plan.
- Our Executive Management team will review and approve the CVE Notification.
- All customers will receive the CVE Notification.
- Additionally, our Support team will schedule a CVE Notification event with customers ASAP.

- For Cloud MFA customers, the critical patch or update will be applied on the designated date/time if a server restart is not required. If a server restart is required, the critical patch or update will be applied overnight to minimize any user disruption.
- For On-Prem MFA customers, it is up to the customer to determine when to apply the critical patch or update in consultation with SurePassID.
- For customers using a SurePassID Mobile Authenticator app, the critical patch will be deployed as fast as possible, given the potential impact to tens of thousands of end users. SurePassID will work with customers to ensure that their helpdesks have additional support to communicate and support any changes.