



Universal Personal Authenticator

FireID Mobile Authentication System Version 2.1.2 Release Notes





- 1. INTRODUCTION 1
- 2. NEW FEATURES 1
 - 2.1 *Compound Authentication* 1
 - 2.2 *Authentication Server Diagnostics* 1
 - 2.3 *Enhancements to Active Directory Import* 2
 - 2.4 *Disallowing DOS Lockout Attack* 2
 - 2.5 *Portability of the FireID Server Application across Application Servers* 2
 - 2.6 *Replace JRadius with TinyRadius* 3
 - 2.7 *Open Source Licenses* 3
- 3. RESOLVED ISSUES 4
- 4. KNOWN ISSUES 5

1. Introduction

This document describes the changes and enhancements to the FireID Mobile Authentication System (MAS) software version 2.1.2.

2. New Features

2.1 Compound Authentication

Issue	Area	Subject
n/a	Authentication Server	Compound Authentication
<p>The Authentication Server now provides Compound Authentication, which further enhances the security of a FireID-protected resource. When making use of this feature, users will have to enter their static password followed by an OTP. This method of authentication will ensure greater security.</p>		

2.2 Authentication Server Diagnostics

Issue	Area	Subject
n/a	Authentication Server	Authentication Server Diagnostics
<p>Users are now able to run a set of network tests within the FireID Server for trouble shooting purposes. This will allow the FireID Support team to deliver better support to clients.</p>		

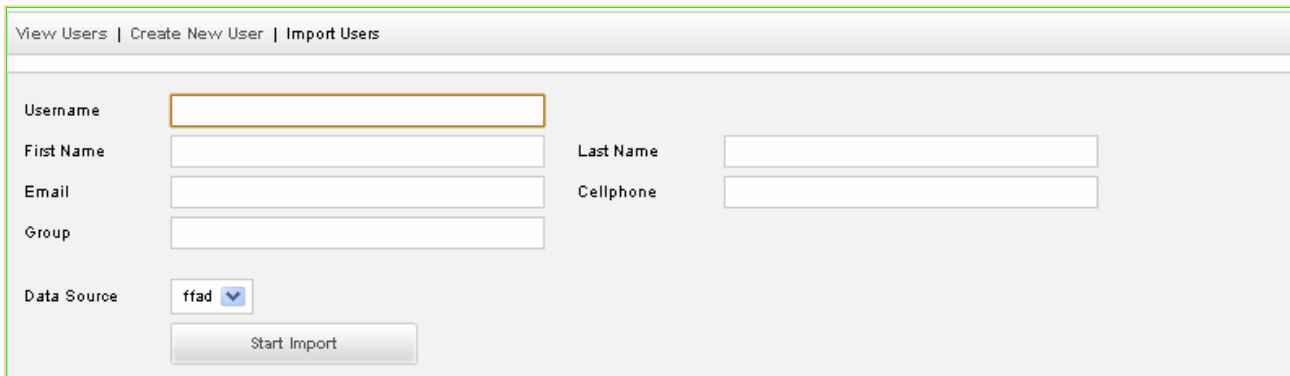
Setup | Services | Settings | RADIUS | Proxy | Data Sources | Certificates | Backups | External Auth | **Diagnostics** | About

Running Diagnostics

- Testing Internet Connection via Server ✔
- Testing Connection to Provisioning via Server ✔
- Error Log [Toggle Results](#)
- wget to google ✔ [Toggle Results](#)
- wget to Provisioning 🔄

2.3 Enhancements to Active Directory Import

Issue	Area	Subject
n/a	Authentication Server	Enhancements to Active Directory Import
<p>Users are now able to search for particular users before doing a bulk import. This provides greater flexibility during the import process.</p>		



2.4 Disallowing DOS Lockout Attack

Issue	Area	Subject
n/a	Authentication Server	Disallowing DOS Lockout Attack
<p>The FireID Authentication server now features a new mechanism to disallow DOS Lockout Attacks. After more than 5 unsuccessful auth attempts, a user's account gets locked for one hour. During this hour login attempts are unsuccessful, even if correct credentials given. This results in a system behavior where users are never locked out completely, but still making it impossible to try a large number of guessed OTP's.</p>		

2.5 Portability of the FireID Server Application across Application Servers

Issue	Area	Subject
n/a	Authentication Server	Portability of the FireID Server application across Application Servers
<p>The FireID Server is no longer restricted to running on Glassfish, and is now portable across Application Servers. This provides clients with a greater flexibility when choosing on which platform to run FireID.</p>		

2.6 Replace JRadius with TinyRadius

Issue	Area	Subject
n/a	Authentication Server	Replace JRadius with TinyRadius
<p>The combination of JRadius with FireID plugin in combination with FreeRadius will be replaced by a single TinyRadius handler. The current radius setup is complex and brittle. The new setup is more stable and fault handling is more transparent. The FireID download is also significantly smaller and the Radius service will not have to be restarted when a new Radius client is added.</p>		

2.7 Open Source Licenses

Issue	Area	Subject
n/a	Authentication Server	Open Source Licenses
<p>Systems Administrators are now able to view additional Open Source licensing information on the About page.</p>		

3. Resolved Issues

Issue ID	Area	Subject
DE102	Authentication Server	The Server constantly shows an 'Update Available' message even though there is no update.
DE109	Authentication Server	Updating settings under System Administration results in an error message with an 'http status 500' error.
DE132	Authentication Server	Users with only one role in the system are unable to login.
DE144	Authentication Server	Systems Administrators obtain an error when trying to import users from a DataSource that is currently not available.
DE145	Authentication Server	Clicking on the 'Select Page' field when importing users results in an error message.
DE146	Authentication Server	Clicking on the Import button without any selected users results in the 'Previous Thousand' link to appear.
DE151	Authentication Server	The auto-logout feature does not work in Internet Explorer when restoring a backup.
DE177	Authentication Server	Systems Administrators are logged out of the server if they try to download log files during the pre-activation checks.
DE216	Authentication Server	Users are not able to see nor download log files when given the 'Audit Trails' role.
DE221	Authentication Server	Browsing to the 'About' screen causes root users to be logged off when using multiple tabs in IE6.
DE224	Authentication Server	Root users are unable to login if they restore to a previous version.
US371	Authentication Server	The system does not validate for valid email address and cellphone numbers for all chosen users when systems administrators use the Action Drop-down box on the User Management page in combination with the check boxes to deploy tokens.
US398	Authentication Server	Systems Administrators are not automatically logged out of the web interface when initiating a Restore operation.

4. Known Issues

Issue ID	Area	Subject
DE100	Authentication Server	Backup functionality allows users to create multiple backups with the same name. However, Backups are time-stamped, ensuring their uniqueness.
DE103	Authentication Server	The Radius Server does not restart automatically, Systems Administrators should restart it from the Server console.
DE122	Authentication Server	The Audit trails do not include entries for failed authentication attempts.
DE125	Authentication Server	The system does not display an error message when users with incorrect email addresses are provisioned.
DE222	Authentication Server	Systems Administrators are unable to delete proxies if they remove the hostname/IP first.