

FireID

FireID Authentication Server
Release Notes

Version 2.6.3



www.fireid.com



TABLE OF CONTENTS

1. INTRODUCTION	1
2. NEW FEATURES	1
2.1 LICENSE EXPIRY NOTIFICATION.....	1
2.2 MULTIPLE PASSTHROUGH PROVIDERS.....	1
2.3 RADIUS MIGRATION PROVIDER.....	2
2.4 PIN ENFORCEMENT ON MOBILE APPLICATION.....	2
3. KNOWN ISSUES	3

FireID Authentication Server Release Notes

VERSION 2.6.3

1. Introduction

This document describes the changes and enhancements to the FireID Authentication Server Version 2.6.3.

2. New Features

2.1 License Expiry Notification

Issue	Area	Subject
US1206	User Interface	License Expiry Notification
<p>The FireID Authentication Server now features explicit license expiry notifications. For example, warning messages will appear when a server's license is within one month of its expiry date or has fewer than ten users remaining on its license.</p> <p>Once a server license has expired, the FireID Authentication Server will display a red error message. The user will then be redirected to the About page on first login, where the relevant exceeded license component will be highlighted.</p>		

2.2 Multiple Passthrough Providers

Issue	Area	Subject
US1394	Authentication	Multiple Passthrough Providers
<p>The FireID Authentication Server now supports multiple External Authentication Providers, configured in a sequence in which passthrough providers are queried for static passwords. This will allow Systems Administrators to configure fail over services for their static password provider and configure passthrough in a High Availability configuration.</p> <p>These providers are listed in order of priority, with only one provider given priority at any time. Systems administrators may also set providers to inactive status.</p> <p>It is important to note that the total timeout value for all providers should not exceed 5000ms. Doing so will result in failed authentication requests due to security reasons.</p>		

2.3 RADIUS Migration Provider

Issue	Area	Subject
US1339	Authentication	RADIUS Migration Provider
<p>The FireID Authentication Server now features a RADIUS Migration Provider. This feature is distinct from the existing RADIUS passthrough system.</p> <p>If a migration provider exists, all authentication requests for users not on the FireID Authentication Server are passed through to the RADIUS migration provider.</p> <p>A RADIUS Migration Provider may also be used as a passthrough authenticator, in which case it will authenticate users not on the FireID Authentication Server and users on the FireID Authentication Server without a password. This will not happen by default, but only if passthrough is selected. Please note that a RADIUS migration provider will always authenticate users that are not on the FireID Authentication Server.</p> <p>The RADIUS Migration Providers are configured on the same screen as the External authentication providers. The system allows one RADIUS Migration Provider, and only the configured RADIUS Migration Provider will be displayed.</p>		

2.4 PIN Enforcement on Mobile Application

Issue	Area	Subject
US1395	Mobile Application	PIN Enforcement on Mobile Application
<p>Systems Administrators can now configure PIN enforcement in the token setup wizard on the FireID Authentication Server. Using this option will force users to set a PIN code when installing the FireID mobile application on their phones.</p> <p>The setting for this functionality is located in the token setup wizard. This is a simple checkbox which is labelled "Enforce PIN on mobile application".</p>		

3. Known Issues

1. FireID Authentication Servers versions 2.1.x are unable to upgrade to this version. Should you need to upgrade to v2.6.3, please contact FireID support via email: support@fireid.com.
2. Please also note that the SOAP API V1 has been deprecated. FireID recommends using the SOAP API V2.



WWW.FIREID.COM

INFO@FIREID.COM

+27 21 880 2647

2ND FLOOR

BLOCK C, OCTO PLACE

ELECTRON ROAD

TECHNOPARK

STELLENBOSCH 7600

WESTERN CAPE

SOUTH AFRICA