

FireID

# FireID Authentication Server Release Notes

Version 2.6.5



[www.fireid.com](http://www.fireid.com)



## TABLE OF CONTENTS

<b>1. INTRODUCTION</b>	<b>1</b>
<b>2. NEW FEATURES</b>	<b>1</b>
2.1 OTP RESYNCHRONISATION ENHANCEMENTS	1
2.2 SERVER INFORMATION BANNER	1
2.3 USER GROUPS FOR RADIUS AUTHENTICATION	2
2.4 RADIUS MIGRATION PROVIDER	2
2.5 RADIUS SUPPORT FOR MS-CHAP V2 AUTHENTICATION	2
2.6 PERSISTENT UPGRADE LOGS	3
<b>3. KNOWN ISSUES</b>	<b>3</b>

# FireID Authentication Server Release Notes

VERSION 2.6.5

## 1. Introduction

This document describes the changes and enhancements to the FireID Authentication Server Version 2.6.5.

## 2. New Features

### 2.1 OTP Resynchronisation Enhancements

Issue	Area	Subject
US1174	Authentication	OTP Resynchronisation Enhancements
<p>A number of enhancements have been added to the OTP Resynchronisation functionality. Firstly, the number of OTPs required for resynchronisation can be customised via the <code>authserv.otp.numberofSuccessiveOtpsToAutoSync</code> setting, which by default is set to 3.</p> <p>Secondly, administrators are now able to resynchronise users by clicking on the Resynch button in a user's profile. The administrator will then specify a number of OTPs supplied by the user in order for the resynchronisation to be effective.</p> <p>Lastly, should the user enter the same OTP a number of times, this will not cause the failure count to increase.</p>		

### 2.2 Server Information Banner

Issue	Area	Subject
US1194	User Interface	Server Information Banner
<p>The FireID Authentication Server now features a server information banner which displays the server's name and IP address. This is to enable systems administrators running multiple servers to easily recognise on which server they are working.</p>		

## 2.3 User Groups for RADIUS Authentication

Issue	Area	Subject
US1539	Authentication	User Groups for RADIUS Authentication
<p>The FireID Authentication Server now supports user groups that can be associated with RADIUS clients for authentication. User groups can be associated with one or more RADIUS clients. This means users are only authenticated if they are members of a user group which the RADIUS client is allowed to authenticate. Conversely, if a user group is not associated with a RADIUS client, users who belong to that group will be unable to authenticate via this RADIUS client.</p>		

## 2.4 RADIUS Migration Provider

Issue	Area	Subject
US1539	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>		

## 2.5 RADIUS Support for MS-CHAP V2 Authentication

Issue	Area	Subject
US1549	Authentication	RADIUS Support for MS-CHAP V2 Authentication
<p>The FireID Authentication Server now supports the MS-CHAP V2 protocol for RADIUS authentication. Please note that this protocol is only valid for OTP authentication, hence Compound and Static Password authentication methods will not work. This setting should be set on the RADIUS client when setting the RADIUS connection.</p>		

## 2.6 Persistent Upgrade Logs

Issue	Area	Subject
DE586	Audit Trail	Persistent Upgrade Logs

Previously, every time a server-upgrade command was run, the /var/log/fireid/upgrade.log was over-written by the latest upgrade operation. The FireID Authentication Server now records all upgrade operations in this log file.

## 3. Known Issues

1. Please note that the SOAP API V1 has been deprecated. FireID recommends using the SOAP API V2.
2. During a server upgrade to v2.6.5, the following message will be displayed, please ignore it:

```
W: GPG error: http://packages.fireid.com hardy-stable Release: The
following signatures were invalid: KEYEXPIRED 1279886693
W: You may want to run apt-get update to correct these problems
```



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