

Technical Bulletin CS-19-04

Versity & Google's Factory Reset Protection

This technical bulletin explains Google's Factory Reset Protection and what it means for your Versity handset.

System Affected

Spectralink Versity – all models

Description

In the consumer world, prior to Lollipop 5.1, anyone can steal a phone and perform a factory default from the recovery or the bootloader and use the phone for their own. They don't need to know the previous owner's PIN/password to access the Settings menu to do the reset, since doing a reset from Recovery bypasses the Android lock-screen.

To prevent this scenario, Android 5.1 introduced Factory Reset Protection. Anyone can still wipe the data from the phone from the recovery or bootloader. However, Google stores a "token" tied to the previous owner's Google account that cannot be cleared from the recovery or other "backdoor" ways of performing a factory reset (what Google terms "untrusted" resets). Therefore, on startup a would-be thief cannot get past the Google Setup Wizard unless they know any Google account email and password of the previous owner(s) or the lock-screen PIN/pattern/password. Should the legal owner want to wipe his phone before selling it, the token can be cleared from the "trusted" factory reset option in the Settings menu. (By removing the Google account, enabling OEM unlocking or removing the PIN/pattern/passwork from the lockscreen.)

Requirements for Factory Reset Protection (must have all three):

- At least one Google account
- Pattern/pin/password
- OEM Unlocking disabled

OEM Unlocking is disabled by default for security and most admins will use some sort of password for security. Therefore, adding a Google account to the phone winds up enabling FRP, which may be an unexpected and possibly undesirable side-effect.

To prevent the necessity for backdoor resets or tracking down former employees, EMMs can utilize Enterprise FRP through Android for Work which configures a Corporate Google account on the device. A Corporate Google account enables the EMM to manage a handset that was abandoned by a former employee or reset via an untrusted factory reset, etc. Consult the EMM documentation on how to utilize this feature.

Without an EMM Corporate account, any Verity with FRP enabled and reset via an untrusted factory reset must be RMA'd if the user credentials are not known. To prevent the RMA requirement, when that Verity changes hands, the admin or employee must arrange to wipe the device or at least remove the employee's Google account so that the device can be reassigned.

Note that it is not necessary for an employee to share their whole Google account and password in order to do a trusted factory reset on a device, only the PIN is needed for access.

If you'd like additional information about Factory Reset Protection, please review the following document.

[Help prevent others from using your device without permission¹](#)



¹ <https://support.google.com/nexus/answer/6172890?hl=en>

Document Status Sheet

Document Control Number: CS-19-04

Document Title: Versity & Google's Factory Reset Protection

Revision History: I01 – Released *May 29, 2019*
I02 – Released
I03 – Released

Date: *May 29, 2019*

Status: Draft Issued Closed

Distribution Status: Author Only Internal Partner Public

Copyright Notice

© 2019 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink's products are trademarks and/or service marks of Spectralink Corporation and are common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Spectralink.

All rights reserved under the International and pan-American Copyright Conventions. No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Spectralink Corporation.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

Warranty

The *Product Warranty and Software License and Warranty* and other support documents are available at <http://support.spectralink.com>.

Contact Information

US Location

+1 800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

info@spectralink.com

Denmark Location

+45 7560 2850

Spectralink Europe ApS
Bygholm Soepark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

UK Location

+44 (0) 20 3284 1536

Spectralink Europe UK
329 Bracknell, Doncastle Road
Bracknell, Berkshire, RG12 8PE
United Kingdom

infoemea@spectralink.com