



## Threat Protection System Release Notes

Version 5.2.2

This release includes all issues fixed in *Threat Protection System Release Notes Version 5.2.0*. For details about those changes, refer to the v5.2.0 Release Notes on the [Online Help Center](#).

### Important notes

- If you are upgrading from an earlier, nonsequential TOS, refer to the release notes of any interim releases for additional enhancements.
- Before you upgrade your device to the latest TOS, maximize the space on your device by removing outdated TOS versions and packet traces that are no longer required. This ensures a successful upgrade and allows for a TOS rollback, if necessary. You can remove previous TOS versions using the SMS, the LSM, or the CLI.
- All TPS devices must be running a minimum of v5.0.1 before installing this version.
- Use SMS v5.2.0 and later to manage a TPS device with this release.

### Release contents

The following items have been repaired in this release.

Description	Reference
This release repairs an FPGA issue that failed to scrub abandoned network connections, which caused the FPGA connection table to become congested. The performance of 8200TX and 8400TX devices became degraded, and a reboot was required to recover from the condition.	TIP-47474
The <code>chpasswd</code> command no longer fails with the following message: <code>ERROR: DEFAULT: Invalid localuser.</code>	SEG-71654

## Product support

For assistance, contact the [Technical Assistance Center \(TAC\)](#).

© Copyright 2020 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks of their respective owners.