



DECEPTIONGRID™

v. 7.2

Release Notes

TrapX® Security, July 2021

trapx.com

Contents

Preface	3
What's New in Version 7.2	4
Upgrade	6
Upgrade Notes	6
Upgrade Instructions	6
Post-Upgrade Notes	7
Resolved Issues	8
Minor Versions	11
Support	12
Documentation Feedback	12
About TrapX Security®	12

Preface

TrapX Security® is pleased to announce the release of DeceptionGrid™ version 7.2. This is an important release including new features and resolutions of known issues.

These release notes list new features and issues in DeceptionGrid version 7.2.

What's New in Version 7.2

DeceptionGrid 7.2 introduces significant **architectural improvements** to security, performance, and stability.

In addition, it includes the following new features and capabilities:

- **DeceptionGrid in Kubernetes:** TrapX now provides DeceptionGrid Appliances as Kubernetes pods for deployment in a Kubernetes environment, enabling quickly raising multiple Appliances as needed, increasing stealth in an organizational containerized servers environment, and helping in trapping attackers' lateral movements between pods, such as from rogue pods.
- **Enhanced detection and alerting:** Emulation traps now detect and record specific, detailed event information upon the following attack types:
 - **ARP Scans**
 - **Solar Winds Sunburst backdoor**
 - **Kaseya supply chain attack**
 - **PrintNightmare exploit**
- **TSOC Access Control List (ACL):** You can now limit login to TSOC to be only from specified source IP addresses or IP ranges.
- **WinRM emulated service and deception token:** Windows emulations (Station and Server) now include a WinRM emulated service, that upon connection records the attacker's name. For an enriched event alert, the service can be proxied to a Full OS trap. A deception token registers the trap in endpoint TrustedHosts.
- **Repeat event suppression:** To avoid large numbers of events from repeated attacks, you can suppress events (trap events and NIS events) appearing to represent continued repeat attacks (by same source and destination).
- **SAML Compatibility:** TSOC SAML authentication is now compatible with Identity Providers (IdPs) such as CyberArk Idaptive that provide metadata in a separate URL from the identity URL.
- **Subnet connectivity reporting:** The Active Defense Scorecard now indicates per-subnet when a trap is not reachable.
- **Event MITRE details:** Events in the Event Analyzer now display full details of correlations with MITRE tactics and techniques.
- **Cached Credentials tools:** The downloaded token distribution archive now includes the following tools, preconfigured with the credentials defined in Cached Credentials tokens:
 - A tool for configuring the credentials in the organizational Active Directory
 - Configuration for organizational SIEM alerting.
- **Comprehensive Appliance backup:** Appliance backup to TSOC now includes spin data and logs (size limited).

- **Per-domain Active Directory tokens:** Different Appliances can now be configured with different Active Directory domains, for which separate deception tokens will be created.
- **ForeScout compatibility:** TSOC can now be integrated with the current version of ForeScout CounterACT, version 8.2, for event display in CounterACT, disconnect (divert) of infected endpoints, and TSOC asset inventory.

Upgrade

In This Section

[Upgrade Notes](#).....6

[Upgrade Instructions](#).....6

[Post-Upgrade Notes](#)7

Upgrade Notes

For full functionality of new features and resolved issues, it is required to upgrade TSOC and all Appliances and Full OS traps to version 7.2.

Upgrade to version 7.2 is supported from all released builds of version 7.1. Subsequent upgrade to released minor versions (see [Minor Versions on page 11](#)) is supported from all released builds of version 7.2.

TSOC must be upgraded first, to be able to begin upgrading Appliances. Appliances of previous versions will not continue to work reliably with the current version of TSOC.

Before upgrading, make sure virtual hardware conforms to requirements as in the *DeceptionGrid Installation Guide* (unchanged from previous version).


Upgrade Instructions

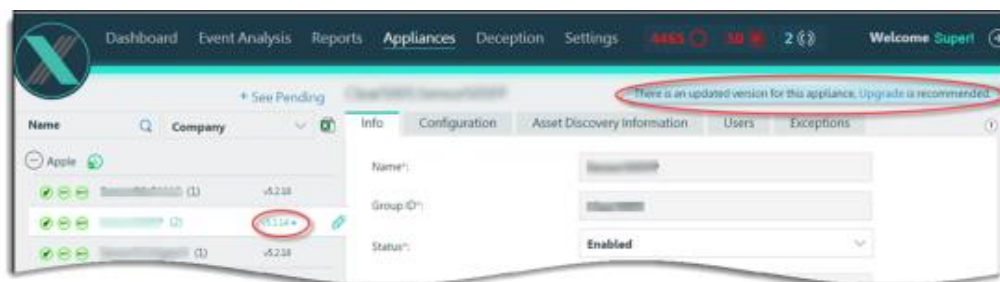
To upgrade to the current release:

1. For extra security, it is recommended to save a snapshot of the TSOC server. If your Appliances are also virtual, save snapshots of them as well.
2. Make sure servers meet requirements as in Upgrade Notes above.
3. If at any point in the past any DeceptionGrid component was restored from a snapshot, restart that component.
4. Log into TSOC as a Super Admin.
5. In TSOC, click the upgrade message:



Follow instructions until the process is complete, including the TSOC server being restarted.

6. In TSOC, go to **Appliances**. Appliances and Full OS traps that are not yet upgraded are marked with , and upon selecting them, an upgrade message appears:



For each relevant Appliance, in the message click **Upgrade** and follow instructions.

7. After upgrading a full OS trap, return it to Active mode and create a new baseline snapshot.

Post-Upgrade Notes

As with all new versions, if before upgrade you downloaded a Deception Token package for external distribution, to ensure compatibility with the upgraded TSOC and traps make sure to download a new package for distribution and make sure your distribution systems and scripts conform to current documentation.

Resolved Issues

The following issues are newly resolved in version 7.2. Issues that were resolved in updates to 7.1 are also included.

Component	Description
TSOC	Trap Managers can now see Deception Tokens of their assigned VLAN Alias traps.
TSOC	In the TSOC Server Administration Menu, for restoring an Appliance backup, available backups are now listed correctly.
TSOC	Exported events to CSV now include Destination IP addresses.
TSOC	Exceptions can now be created from false-positive SMB events on child interfaces.
TSOC	Retrieving Appliance logs from TSOC no longer fails in rare cases.
TSOC	When the high-interaction Linux autoreverts during an attack, it now appears at the correct severity level.
TSOC	Saved changes to Forescout integration for inventory now appear immediately in the TSOC page.
TSOC	TSOC server DNS issues have been resolved.
TSOC	New trap tokens of labeled traps are now immediately listed in Tokens and Campaigns pages.
TSOC	Trap type changes in the trap wizard no longer affect the filters in the parent Appliances page.
TSOC	Successive deception token installation on Mac endpoints no longer results in multiple endpoint item rows in Deception > Deployment.
TSOC	The All Connection and Scan Attempts report now includes all relevant events.
TSOC	Attack Visualization now displays the correct icon for Axis Network Camera trap.
TSOC	Links from Remote Overview to the Event Analyzer now produce filtered event lists.
TSOC	The Appliance page now displays content correctly even when Appliances are not grouped (Group by: None).
TSOC	Attack Intelligence can now be correctly searched by Subject.
TSOC	Filtering the Event Analyzer by MITRE tactic no longer requires clicking Search twice.
TSOC	TSOC Mail settings now accept passwords with ampersand (&).
TSOC	The Remote Overview dashboard now displays correct Detection Coverage device number information.
TSOC	Label changes now appear immediately in Appliances page.
TSOC	The Active Defense Scorecard progress bar no longer indicates a negative value.

Component	Description
TSOC	Attack Visualization now correctly represents connections from Remote devices.
TSOC	For events from devices with Remote tokens, Trigger emails now include the device name.
TSOC	Trigger emails are no longer affected by differences between the time zone of the configuring user and the Appliance time zone.
TSOC	The Events Timeline in the General dashboard now counts sessions rather than their constituent individual connections.
TSOC	When TSOC is configured with a custom NTP, TSOC no longer continues to query the default NTP.
TSOC	In a Report with a custom time frame, the end time is no longer ignored.
TSOC	It is now possible to cancel BYOT scans.
TSOC	Restoring Appliance configuration (from TSOC Administration menu) now succeeds.
TSOC	When the Appliance list is ungrouped (Group by: None), Appliance details appear and pagination navigation works correctly.
TSOC	Upon manually reverting the full Linux OS, TSOC no longer reports (erroneously and temporarily) that the Appliance is offline.
TSOC	TSOC no longer attempts to send health monitoring data to Syslog when it is not enabled.
TSOC	Active Defense Scorecard now displays information for subinterfaces even when the parent interface does not have a trap and is not included in Active Defense testing.
Appliance	Active Defense Scorecard no longer displays information for Public Traps, which are not supported for Active Defense Scorecard.
Appliance	Deception tokens of Remote traps on Appliances in Azure are now configured with the correct trap IP address.
Appliance	Reverting a full Linux OS no longer causes configured credentials to be lost.
Appliance	Active Defense Scorecard recommendations are now correct for emulated services proxied to a Full OS trap.
Appliance	Trap response to nmap SMB discovery scans now correctly provides the emulated FQDN.
Appliance	Windows emulations now respond correctly to PsExec connections.
Appliance	Upon connecting an already-configured Appliance to a new TSOC, trap names are no longer lost, and traps now work correctly.
Deception Tokens	The Browser Credentials and VPN deception tokens now successfully install on Firefox.
Deception Tokens	The Browser History deception token now successfully installs on Internet Explorer when Internet Explorer is configured with a proxy white list.
Deception Tokens	TSOC now displays information from token endpoint installations when endpoint date and time formats are non- default.

<i>Component</i>	<i>Description</i>
API / CLI / Shell / SDK	Downloaded events now include relevant files (PCAP and binaries).
API / CLI / Shell / SDK	Commands for working with Full OS Linux now work properly.
API / CLI / Shell / SDK	Retrieved events now include attack details.
CLI / Shell / SDK	Downloaded events now include Scan events.

Minor Versions

No 7.2 minor versions have yet been released.

Support

Support for TrapX products is provided by TrapX or by an authorized TrapX Service Partner. More information and technical support for TrapX products are available at:

- support.trapx.com/portal
- support@trapx.com
- Americas: 1-855-249-4453
EMEA & Asia Pacific: +44-208-819-9849

Documentation Feedback

TrapX Security continually strives to produce high quality documentation. If you have any comments, please contact Documentation@trapx.com.

About TrapX Security®

TrapX Security is the pioneer and global leader in cyber deception technology, with flagship solution DeceptionGrid effectively detecting, deceiving, and defeating advanced cyber attacks and human attackers in real-time. DeceptionGrid provides automated, highly accurate insight into malicious activity unseen by other types of cyber defenses. Deploying DeceptionGrid sustains a proactive security posture, fundamentally halting the progression of an attack. DeceptionGrid changes cyber-attack economics by shifting the cost to the attacker.

The TrapX Security customer base includes worldwide Forbes Global 2000 commercial and government customers in key industries including defense, healthcare, finance, energy, and consumer products. Learn more at www.trapx.com.

Disclaimer

Product specifications are subject to change without notice. This document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, TrapX cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Before consulting this document, check the corresponding Release Notes regarding feature preconditions and/or specific support in this release. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents as well as software files can be obtained by TrapX customers.

Trademarks and Copyright

© Copyright 2021 TrapX Security Ltd. All rights reserved. This document is subject to change without notice. TrapX, TrapX Security, DeceptionGrid and CryptoTrap are trademarks or registered trademarks of TrapX Security in the United States and other countries. Other trademarks used in this document are the property of their respective owners.

Updated 29/7/21