Introduction to SNMPv3

Why It's Time to Upgrade and Configure Zebra Printers for Enhanced Security

Introduction

Organizations' networks, their connected devices, and the data they hold are valuable targets for cyber-criminals.

In 2023, there was a 72% increase in data breaches compared to 2021, which previously saw the highest number of breaches of all time.[1] And the damage these attacks can cause is significant – both reputationally and financially: Globally, individual data breaches cost an average of $4.88 million in 2024.[2]

Ensuring the security of an organization's network management protocols is therefore essential. And as threats evolve, so must defenses.

SNMPv3 (Simple Network Management Protocol version 3) is the latest version of the standards-based SNMP protocol. SNMPv3 is widely used in enterprise environments where network security is a priority when managing and monitoring network-connected devices. It offers better security features, including support for authentication, encryption and access control.

[1] Identity Theft Resource Center 2023 Data Breach Report
[2] IBM Cost of a Data Breach Report 2024

SNMPv3: an Overview

Building on its predecessors, SNMPv3 provides commercial-grade secure access to network devices.

SNMPv3 uses encryption to prevent data breaches and authentication to ensure that only intended recipients can receive data packets. Additionally, it provides data security features like integrity checking to ensure that data remains unaltered during transit, origin verification to validate the source of a request or response, timeliness checking and protection against eavesdropping by unauthorized external actors.

Exploring the Benefits of SNMPv3

SNMPv3's secure management capabilities are important for safely configuring and controlling an organization's network and the devices connected to it, such as printers. IT network managers can enjoy peace of mind, knowing that their network's integrity, performance and the data it holds are not at risk.

By validating a sender's identity, its authentication protocols ensure all messages received are from trusted sources while its encryption technology protects both data integrity and the confidentiality of management operations. This makes it very difficult for unauthorized individuals or eavesdroppers to access any sensitive data on an organization's network.

SNMPv3 also allows administrators to define access control, ensuring that only authorized personnel can view or amend particular items of network or device information. This significantly reduces the risk of accidental or malicious changes to that information.

Moreover, SNMPv3 offers regulatory compliance benefits. By providing security features that protect sensitive information and prevent unauthorized access, it can assist highly regulated industries such as healthcare, finance and government in adhering to regulations like HIPAA, MiFID II, and GDPR.

Mainstream Managed Print Service (MPS) providers use SNMP to interact with the devices they manage. Leveraging SNMPv3 allows them to enhance their service offering by addressing the security requirements of their customers in their network environments, ultimately leading to more efficient service provision and greater customer satisfaction.

Link-OS™ Printer Operating System

Get maximum performance and value from your Zebra printers year after year by upgrading Link-OS to the latest version, which now includes the implementation of SNMPv3.

Zebra's unique Link-OS printer operating system enables Zebra DNA, Zebra's suite of software capabilities that provide a full lifecycle of exceptional experiences for every kind of user. With built-in applications, utilities and tools, Zebra DNA gets your printers up and running quickly, so you can print without hassle, securely and confidently.

Why You Should Keep Your Printers' Link-OS Operating System Up to Date

New features and technologies: By embracing the latest upgrades, you'll get support for new features and functionality – including support for emerging protocols such as SNMPv3, IPv6, compatibility improvements, and the latest Zebra DNA applications, utilities and tools to improve workflows for every user.

Optimum printer performance: Link-OS upgrades address the latest bugs and any performance issues. Keeping your printers' Link-OS operating system up to date helps your printers run better and smoother to reduce support time.

The latest security support: Regularly upgrading your printers' Link-OS operating system is a proactive measure that fortifies your printers' defenses, helping you protect your sensitive data and infrastructure against the latest cyber threats and vulnerabilities.

It's easy to keep your Link-OS printers up to date. With so many ways to upgrade, you can pick the path that's right for your operations – whether your printers are in a single location, in multiple buildings throughout a campus or in multiple facilities across the world.

For more information on Link-OS, and to upgrade and configure your printers' operating system for a more secure network environment, please visit:

www.zebra.com/link-os

Configuring and Enabling SNMPv3

The latest version of Zebra's Link-OS printer operating system includes SNMPv3 support. More information on how to upgrade your Link-OS printers to the latest firmware version can be found on the **Zebra Support and Downloads page**.

Once you have upgraded Link-OS, some configuration is required to enable SNMPv3:

- The printer must first have Protected Mode configured, which requires setting the Protected Mode admin password
- Protected Mode and SNMPv3 configuration is managed using JavaScript Object Notation (JSON)
- To configure SNMPv3, the "setup-snmpv3-user" operation is used to create, update or delete the admin user.
- Once the admin user is created, SNMPv3 is automatically enabled.

Our PrintSecure Administration Guide has been updated to include detailed information for SNMPv3 configuration. You can download it **here**.

Take the SNMPv3 Step

Simple to deploy, more robust, and designed with dynamic, modern networks in mind, moving to SNMPv3 is an important step as part of a best-practice strategy to protect corporate networks, devices and data.

For more information, contact your Zebra representative or visit **www.zebra.com** to find a partner.

NA and Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
contact.apac@zebra.com

EMEA Headquarters
zebra.com/locations
contact.emea@zebra.com

Latin America Headquarters
zebra.com/locations
la.contactme@zebra.com