UNDERSTANDING SNMPv3

and HP Web Jetadmin

CONTENTS

OVERVIEW

SNMPv3 (Simple Network Management Protocol, version 3) is a secure management protocol that is used to encrypt data and require user authentication on devices being managed from within applications like HP Web Jetadmin. HP Web Jetadmin is fully compatible with SNMPv3, but there are some administrative best practices and rules that should be understood and followed. This document relates to HP Web Jetadmin 10.x versions. HP recommends keeping your HP Web Jetadmin installation at the latest version available at www.hp.com/go/webjetadmin. More information can be found by visiting the HP Web Jetadmin support page.

Best practices

When using HP Web Jetadmin to manage SNMPv3 devices, HP Web Jetadmin should be the only configuration agent used in setting up SNMPv3. Notes later in this document show the complexities that exist when SNMPv3 settings are managed from outside of HP Web Jetadmin.

INTRODUCTION TO SNMPV3

SNMP is the primary means HP Web Jetadmin uses to communicate with and manage devices. As the administrator manages devices with HP Web Jetadmin features, HP Web Jetadmin communicates with the devices through functions known as Set and Get operations. Of course, this description is merely preliminary because the SNMP communication protocol is based on a very structured and mature RFC (Request for Comment, Internet Engineering Task Force). Basic SNMP will be called SNMPv1/2 in this document.

SNMPv3 provides a layer of security for device management communication, including cryptographic authentication and data confidentiality (encryption). SNMPv1/2 transmits all data on the network, including data that might be sensitive, in plain text. This means that tools such as network sniffers may be used to monitor the SNMPv1/2 transmissions, such as Get and Set SNMP Community Names. SNMPv3 adds data encryption, which reduces the risk of data being sniffed from the network. Also, with SNMPv3, authentication between the device and HP Web Jetadmin is enforced.

SNMPv1/2 Get and Set Community Names are passed through the network as clear text characters. In practice, these items have been used as passwords, but actually provide only limited security value. In environments with elevated security risks, SNMPv3 should be given serious consideration over the less secure Get and Set items. SNMPv3 credentials make sniffing data very difficult, which adds security to device management communication.

USING HP WEB JETADMIN TO MANAGE SNMPV3 SETTINGS

All HP devices that are capable of management via applications such as HP Web Jetadmin are set to SNMPv1/2 by default. In order to enable SNMPv3, the device must first be configured by an application such as HP Web Jetadmin.

In Figure 1, a device is set up for SNMPv3 using the **SNMP Version Access Control** configuration option in HP Web Jetadmin. Note that in this figure only one device (within a device list) is selected for the SNMPv3 setup.

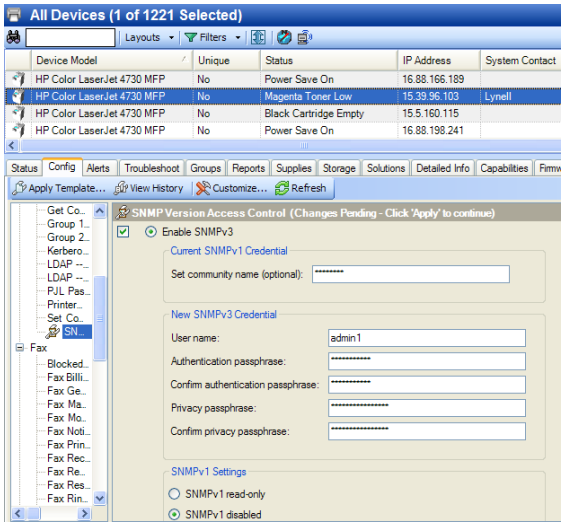

Figure 1—SNMP setup (single device)

To communicate with an SNMPv3 device, HP Web Jetadmin must have the following elements:

- **User Name**—The account identity allowed access via SNMPv3. Example: admin1.
- **Authentication Passphrase**—The first secure string that is stored securely to the device and that must be validated at each SNMPv3 communication from this point forward. The item is used to allow the device to authenticate the sending entity (HP Web Jetadmin) and the communication being sent. Example: oncewasasmallcat.
- **Privacy Passphrase**—The second secure string that is stored securely to the device and that must be validated at each SNMPv3 communication from this point forward. This item is used to encrypt the communication being sent to and from the device. Example: oncewasasmalldog.

When SNMPv3 is enabled on the device, write-mode access via SNMPv1/2 is disabled and configuration of device parameters is only possible through SNMPv3. SNMPv3 settings are used to either completely disable SNMPv1/2 communication or to disable write-mode, leaving SNMPv1/2 readable by any managing agent, such as another installation of HP Web Jetadmin. The setting shown in Figures 1 and 2, **SNMPv1 read-only**, can be used to allow read-access. Some cases might require that SNMPv1 be completely disabled in order to protect all device data. This is possible by selecting the **SNMPv1 disabled** option.

HP Web Jetadmin can be used to configure SNMPv3 on many devices at once. When the **SNMP Version Access Control** configuration option is displayed with multiple devices selected from a device list, HP Web Jetadmin displays blank values until the administrator adds values (credentials) to these fields. Figure 2 shows the **SNMP Version Access Control** configuration option as displayed by the HP Web Jetadmin **Create Device Configuration Template** wizard. In this case, a template is configured for storing SNMPv3 settings that can be applied to devices at a later time. Notice that there are three choices in this configuration item when it is displayed as a template or when multiple devices are selected from a device list:

- **Enable SNMPv3**
- **Modify SNMPv3**
- **Disable SNMPv3**

Templates can be applied directly to one or more devices, to a device group, and through a Group Policy. With a Group Policy, the template settings take effect when a device is added as a member of a device group or removed from a device group membership. A common practice with Group Policies is to set up an automatic group that applies these templates when HP Web Jetadmin automatically populates devices into groups based on group filter criteria.

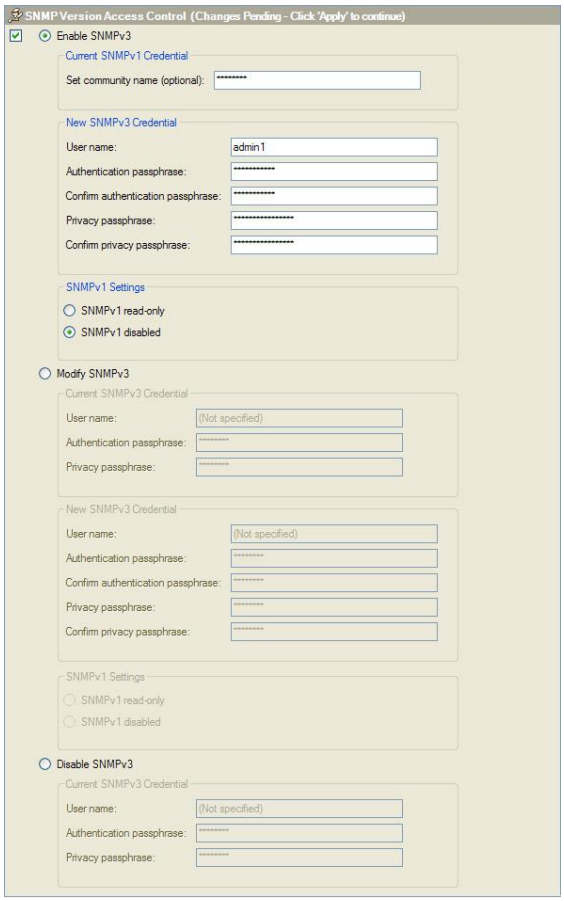

Figure 2—SNMPv3 in the HP Web Jetadmin configuration template

HP WEB JETADMIN AND CREDENTIALS

In addition to the differences between SNMPv3 and SNMPv1/2, it is important for administrators to consider how HP Web Jetadmin interacts with

devices that have credentials and security features set via the Credentials Store. Important points include:

- If a device is discovered using SNMPv3 or configured with SNMPv3 by HP Web Jetadmin, the mode of communication from that point forward includes SNMPv3.
- SNMPv3 credentials are stored uniquely in the HP Web Jetadmin Credentials Store. HP Web Jetadmin begins each communication session by retrieving these credentials and using them to both authenticate and communicate securely with the device.

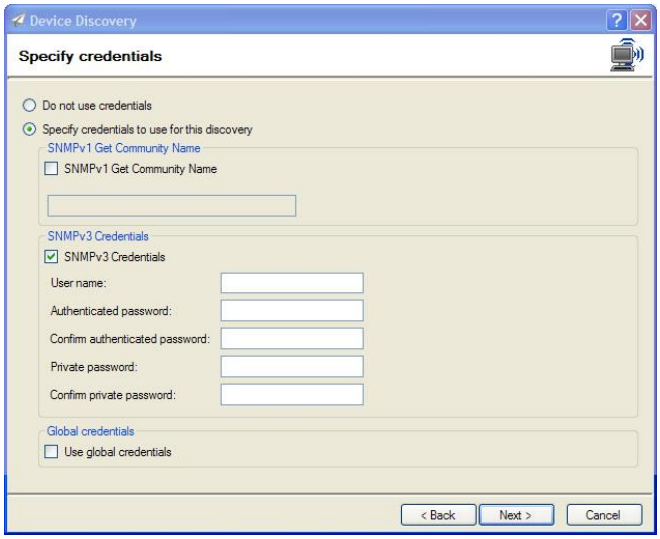

Figure 3—HP Web Jetadmin requires SNMPv3 credentials

- The Passphrase portion of SNMPv3 credentials are added to HP Web Jetadmin using character strings, such as: oncewasasmallcat. The HP Embedded Web Server (EWS) interface requires users to enter these as 16-byte hexadecimal strings. These two interfaces differ significantly. For more information, see SNMPv3 passphrases vs. keys on page 5.
- All SNMPv3 credentials remain in the Credentials Store until they are:
  - No longer valid and then removed
  - Changed by an administrator via HP Web Jetadmin
  - Cleared from the Credentials Store by the administrator

When HP Web Jetadmin no longer has a valid password in the Credential Store or when no valid credential value exists, HP Web Jetadmin prompts the administrator to add a valid credential through the interface shown in Figure 3. Adding credentials via the **Needed Credentials** dialogue is simple. After the credential enables communication with the device, HP Web Jetadmin stores it and continues using it as a seamless background operation. For more information about the Credentials Store, see the *Security and HP Web Jetadmin* white paper. This white paper is available from the HP Web Jetadmin support page (in English).

DISCOVERING SNMPv3 DEVICES

The HP Web Jetadmin instance that performs discovery on a network might not always be the SNMPv3 configuration agent. It is possible for devices to be initially configured via one HP Web Jetadmin instance, while a new instance discovers devices. In any case, HP Web Jetadmin must have SNMPv3 discovery enabled or it will not discover devices configured in SNMPv3. To enable HP Web Jetadmin to discover and manage devices using SNMPv3, go to **Tools** > **Options** > **Device Management** > **Device Discovery**, enable **Discover SNMPv3 devices**, and click **Apply**. The system is now capable of discovering and managing SNMPv3 devices.

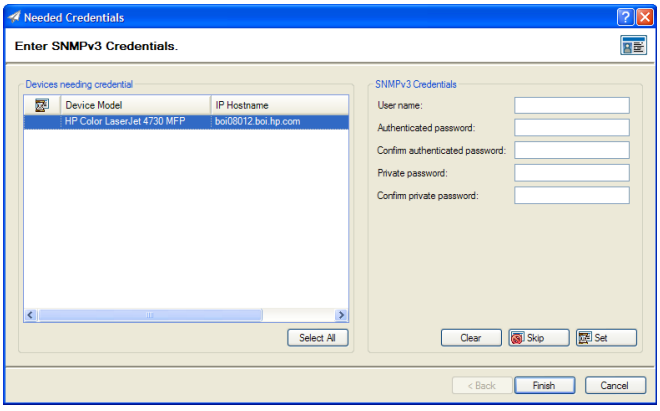

Figure 4—Adding SNMPv3 credentials to discovery

Another aspect of discovering SNMPv3 devices is ensuring that the credential is included in the discovery itself. HP Web Jetadmin needs the SNMPv3 credential for

even basic management communication, beginning with proper discovery. A few options exist to bring about a successful SNMPv3 device discovery. First, the discovery interface itself has a tool dedicated to adding credentials to a specific discovery or to a discovery template. Figure 4 shows the device discovery settings interface that allows adding SNMPv3 and other credentials. This pane is available as live discoveries are run or in the **Create Discovery Template** wizard when you want to store discovery settings. Another way to ensure SNMPv3 credentials are included in a discovery is to add them to the **Global SNMPv3 Credentials** feature (Figure 5). This feature can be understood as a global try-list. Any time HP Web Jetadmin encounters a device with a credentials set, it first looks into the Credentials Store. If nothing is found in the Credentials Store, it attempts whatever the administrator has configured within the global feature. The global feature is not restricted to SNMPv3 credentials. Any of the other credential types, such as SNMP Community Names or File System Password, can be added.

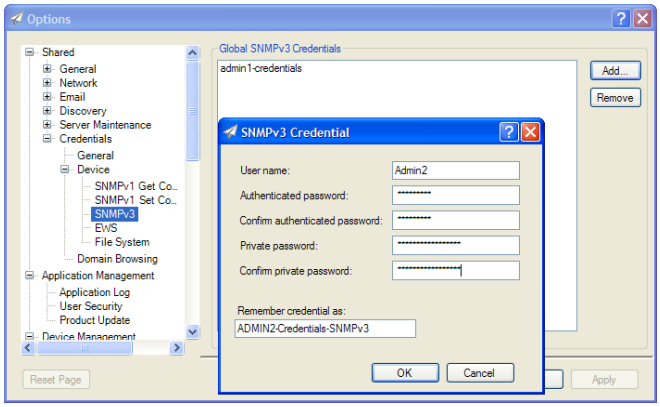

Figure 5—Global SNMPv3 Credentials

NOTE HP Web Jetadmin discoveries are slowed when many credentials are added to the Global SNMPv3 Credentials feature. For each device that lacks credentials in the Credentials Store, HP Web Jetadmin must go through each global value until it either finds a working credential or exhausts the list.

SNMPv3 PASSPHRASES VS. KEYS

The HP EWS management interface allows access to many device settings. Both device and HP Jetdirect management settings can be viewed and adjusted from HP EWS. While you might expect these to be identical to the settings found in the HP Web Jetadmin configuration interface, this is not always the case. For example, HP EWS shows SNMPv3 credentials as hexadecimal keys, while HP Web Jetadmin has credentials configured with passphrases. This is a significant difference. HP does **not** recommend managing SNMPv3 from both interfaces on the same device or even within the same.

Best practices

Use the Global SNMPv3 Credentials feature to ensure that HP Web Jetadmin has enough information to discover your SNMPv3-protected devices. Limit the values you add to the global feature to avoid discovery performance issues.

When the SNMPv3 credential is configured from HP Web Jetadmin, the user adds a user identity and two passphrases to the interface. The passphrases are designed with human usability in mind and can be simple, easy-to-remember strings of letters and/or numbers. (The example given on page 3 was oncewasasmallcat.) When HP Web Jetadmin sets up the device for SNMPv3 security, it transposes that phrase into a hex key using a secure hash technique of MD5 or DES, depending on the phrase. This is done in order to make it nearly impossible to derive the user passphrases from network utilities. So, while HP Web Jetadmin allows the user to work with friendly passphrases, the SNMPv3 communication between HP Jetdirect and HP Web Jetadmin uses very cryptic strings that prevent tampering with devices and data.

Best practices

If HP Web Jetadmin is initially used to configure SNMPv3 on devices, HP Web Jetadmin must **always** be used instead of HP EWS. Administrators can continue to use HP EWS as a management interface with the exception of SNMPv3 settings.

The HP EWS interface, however, requires the user to enter hexadecimal keys rather than passphrases. For security reasons, it does not disclose the key values that are currently stored on the device. This means it is extremely difficult to manage SNMPv3 credentials from both HP EWS and HP Web Jetadmin. Therefore, when HP Web Jetadmin is the primary tool for managing a fleet, HP highly recommends that you use HP Web Jetadmin exclusively for managing SNMPv3 settings as well.

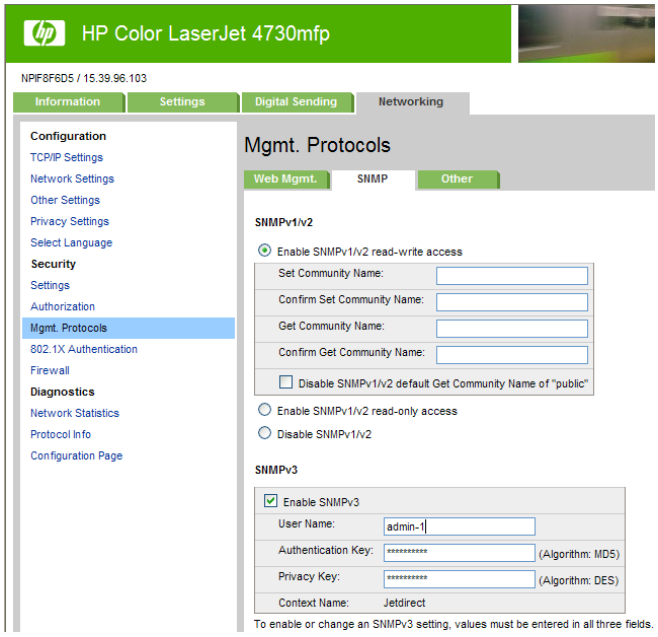

Figure 6—Device configuration via HP EWS

Another big difference between the two SNMPv3 configuration interfaces is the SNMPv1/2 read-write setting. Figure 6 shows a device being configured by HP EWS. Notice that it is possible to leave SNMPv1/2 read-write enabled. HP Web Jetadmin does not allow or recognize this kind of setup (see Figure 1 or Figure). When HP Web Jetadmin is used to configure SNMPv3 on the device, it always disables SNMPv1/2 write-access, either leaving SNMPv1/2 access read-enabled or disabling it altogether. This protects the fleet from unauthorized SNMPv1/2 communication and acts as an extra security step to guard sensitive data on devices.

NOTES

- Administrators need to know about many facets of device security, including protocols, interfaces, firmware, and more. HP offers many documents regarding device security, which can be found on the HP Web Jetadmin support page.
- In addition to SNMP, HP Web Jetadmin also uses the HTTPS protocol to manage some device settings. This is especially true for many newer HP devices. HTTPS communication in this case is encrypted and prevents plain text monitoring and network sniffing. For more information, see Introduction to SNMPv3 on page 2. The *Security and HP Web Jetadmin* white paper, which is available on the HP Web Jetadmin support page (in English), outlines this protocol in more detail.
- In general, HP Web Jetadmin should be used to configure all device security settings. The wide range of settings are best managed with templates, which can save administrators time by reducing repetitive tasks.

Best practices

When using HP Web Jetadmin templates to configure device security, keep security settings in separate templates. Security settings may have to be rotated on a periodic basis according to policy. Keeping these templates separate makes this easier to manage.

TROUBLESHOOTING

- HP Web Jetadmin performance can become noticeably slow when managing devices configured with SNMPv3.
- All HP Web Jetadmin versions can process alerts using polling and SNMPv1/2 traps. SNMPv3 traps are supported from HP Web Jetadmin 10.4 and later.

- When a device discovered with SNMPv1/2 is converted to SNMPv3, a new discovery might be required to re-register that device as configured with SNMPv3.
- **Issue**: HP Web Jetadmin configuration keeps prompting for SNMPv3 credentials when a device does not seem to be SNMPv3.

  Solution: The device might have been configured for SNMPv3 from the device's HP EWS interface. This is not supported. While HP Web Jetadmin always disables SNMPv1/2 write-access, HP EWS allows the configuration of simultaneous SNMPv1/2 and SNMPv3 read-write access. This is usually the root of the problem.

© Copyright 2015 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

c01941786EN, Rev. 3, October 2015