Flowmon Hardening Guidelines

This document explains recommended steps to secure your Flowmon deployment and reduce the potential attack surface. Flowmon is delivered as an appliance including operating system that is configured in a secure way respecting and reflecting relevant subset of the CIS methodology. Each Flowmon release is tested for vulnerabilities. Following steps will ensure that your Flowmon appliance is well secured.

Measure	Description	Where to configure
WebGUI default password	Change password for admin user.	Configuration Center > System > User Settings
SSH console default password	Change password for flowmon user.	Log into Flowmon via SSH (e.g. using Putty) and run `sysconfig` command to launch interactive configuration utility.
iDRAC default password	If your hardware-based Flowmon appliance is equipped with iDRAC management interface change the default user credentials.	Log into iDRAC management interface and change login credentials.
Admin permissions	Do not create users with admin permissions unless necessary. Do not provide regular users access to the Configuration Center.	Configuration Center > System > User Settings
SNMP community string	Flowmon appliance comes with preconfigured SNMPv2 and community string public. Change the community string. You can also switch to SNMPv3.	Configuration Center > System > SNMP
Identity management	You can connect Flowmon to LDAP to avoid standalone user accounts and provide central authentication.	Configuration Center > System > LDAP
SSL certificate	Flowmon comes with a self-signed certificate for secure access to WebGUI. Replace the certificate for a trusted one that you generate using your certification authority.	Configuration Center > System > Maintenance
Limit remote access	You can configure “Access restriction settings” to limit access to management interface for predefined subnets to IP addresses.	Configuration Center > Remote Access
Web security headers	You can control additional security headers for web-based user interface.	Configuration Center > System > Maintenance
Regular updates	Enable regular update package downloads from services.flowmon.com. Enable notifications for administrators that a new package is available for installation. Keep your Flowmon up to date.	Configuration Center > Versions
Management VLANs	You can connect the Flowmon management interface to dedicated management VLAN with restricted access.	Measure outside of the Flowmon system, depending on your environment.

The root access to Flowmon appliances is not provided to the customer and is kept only as a service account for Flowmon Networks to provide technical support and maintenance. Any unauthorized modifications of the Flowmon appliance may negatively affect the functionality of the appliance and prevent future software updates. Only authorized support personnel may work with the appliance with root permissions. The root account itself is password protected and remote access is restricted. Therefore the customer has full control over who has access to the root account. The following options are available for logging into the root account:

- the local console (requires physical access to the Flowmon appliance or access to the hypervisor hosting the Flowmon appliance),
- the iDRAC server management console (requires access to the iDRAC management console that is under full customer control),
- a privilege escalation (requires the use of sudo from CLI when the flowmon user is properly authenticated, access to the flowmon user is under full customer control).