Technical white paper

HP FutureSmart 4 and 5 - Administrative Password Security Features

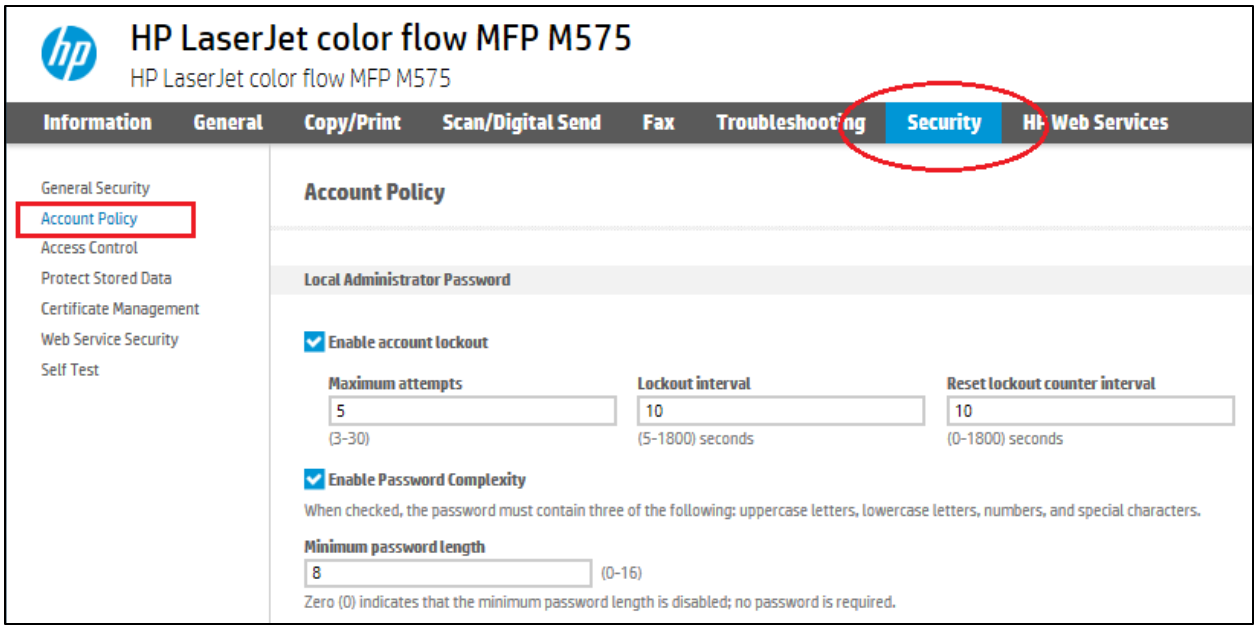
Table of contents

Overview

Three password administrative security features are included in HP FutureSmart 4 and 5 firmware for HP LaserJet Enterprise and Managed printers:

- Account Lockout
- Password Complexity
- Minimum Password Length

These settings are available in the device's Embedded Web Server (EWS) on the **Security** tab under the **Account Policy** menu.



The features apply to the following administrative accounts:

- Local Administrator Password (aka. EWS or device password)
- Remote Administrator Password used for HP Web Jetadmin, HP Security Manager, and HP Digital Sending Software
- SNMPv3 Authentication and Privacy passphrases

NOTE: These features are ON by default when upgrading to HP FutureSmart 4 or 5 firmware bundles.

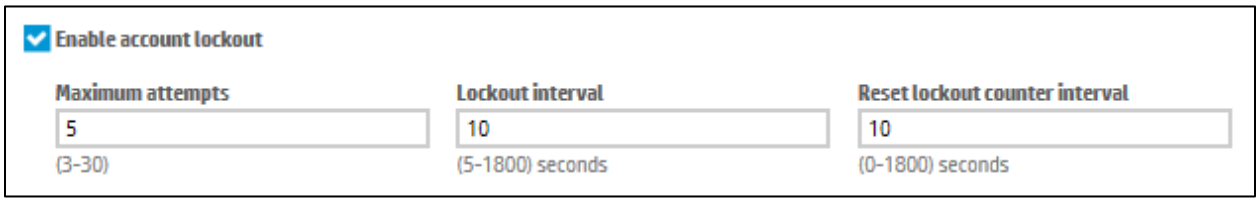
NOTE: To set blank or simple passwords, in the **Account Policy** menu clear the **Enable Password Complexity** check box AND set the Minimum Password Length to "0".

Account Lockout

The Account lockout feature protects the device administrative accounts by providing safeguards to prevent brute force hacking attempts. After a set number of failed authentication attempts the system prevents further authentication attempts for a specific interval.

The account lock feature applies to the following passwords:

- EWS password
- Remote configuration password
- SNMPv3 authentication and privacy passphrases.



- **Maximum attempts (3-30 seconds) Default = 5 attempts**
  How many failed log-on attempts until the account enters a locked-out state.
  NOTE: Back-to-back login attempts with the same credentials are ignored and treated as single login request
- **Lockout interval (5-1800 seconds) Default = 10 seconds**
  How long (in seconds) a locked-out account remains locked-out
- **Reset lockout counter interval (0 -1800 seconds) Default = 10 seconds**
  How long (in seconds) after a failed logon attempt before the counter tracking failed logon attempts is reset to zero

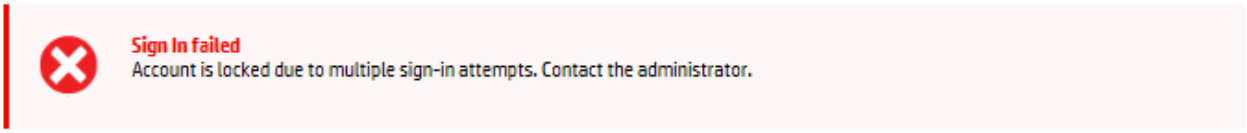
The **Reset lockout counter interval** setting defines a time window for **Maximum attempts** that, if exceeded, the account will be locked for the duration of the **Lockout interval**.

For example, if the **Reset lockout counter interval** is 60 secs and the number of unsuccessful attempts exceeds the **Maximum attempts** value within 60 secs, the account will be locked for the duration of the **Lockout interval**.

Otherwise, the **Maximum attempts** counter will be reset to 0 after 60 secs.

NOTE: The Reset lockout counter interval cannot be greater than the Lockout interval.

Exceeding the maximum configured sign-in attempts presents the following error:



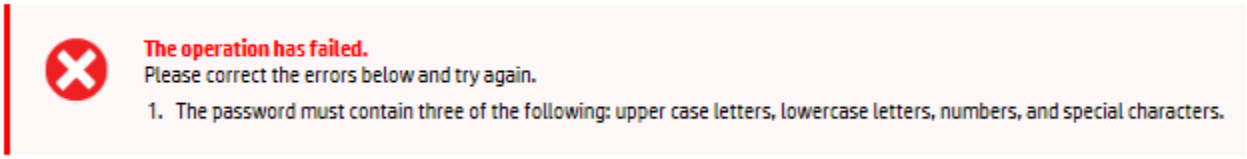
NOTE: For SNMPv3 requests during the lockout state, all SNMPv3 requests will be dropped without returning error or success.

Password Complexity

This feature enforces complex passwords requiring 3 of the 4 following categories:

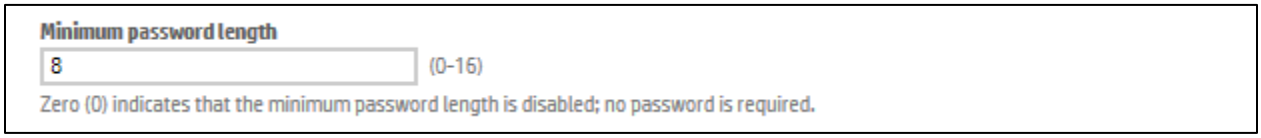
- Upper case characters
- Lower case characters
- Numbers
- Special characters

Configuring a password that does not contain three of the required categories presents the following error:

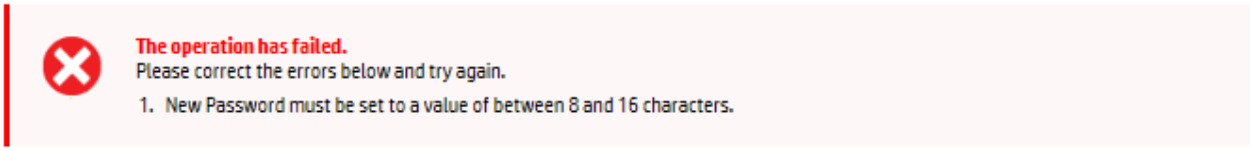


Minimum Password Length

This feature enforces a minimum password length between 1- 16 characters long. The default setting is 8 characters. A Zero (0) minimum password length disables the minimum password length feature.



Configuring a password with less characters than specified presents the following error:



SNMPv3 password policy configuration

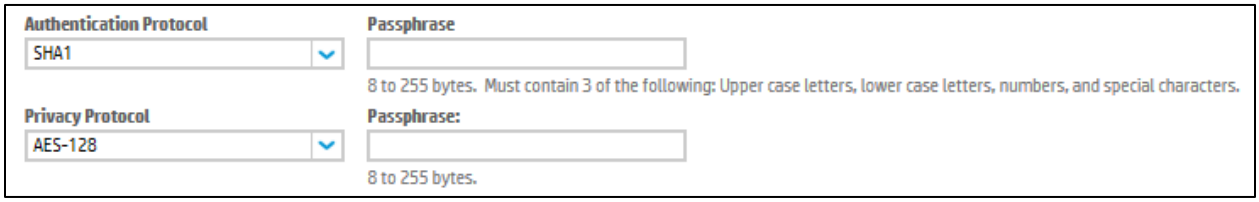
The password security features apply to SNMPv3 Authentication and Privacy protocol passphrases. The features are always enabled using the feature defaults. The Authentication and Privacy passphrases have the following properties:

Authentication Passphrase:

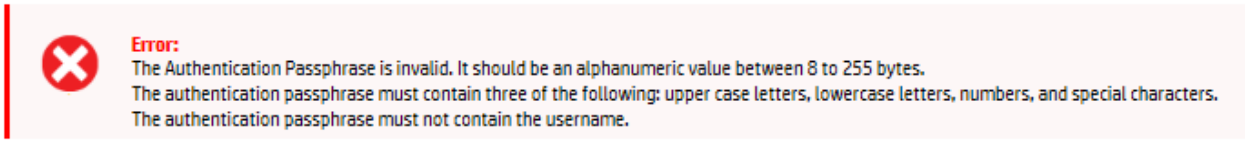
- Account Lockout – always enabled. After a request with invalid credentials further requests are dropped for a fixed 10 sec period
- Password Complexity - always enabled
- Minimum password length - always enabled
  - 8 characters (default)
    OR
  - Configured value of the Local Administrator or Remote Configuration password if either is greater than 8 characters.

Privacy Passphrase:

- Account lockout – NA
- Password Complexity - NA
- Minimum password length - always enabled
  - 8 characters (default)
    OR
  - Configured value of the Local Administrator or Remote Configuration password if either is greater than 8 characters.

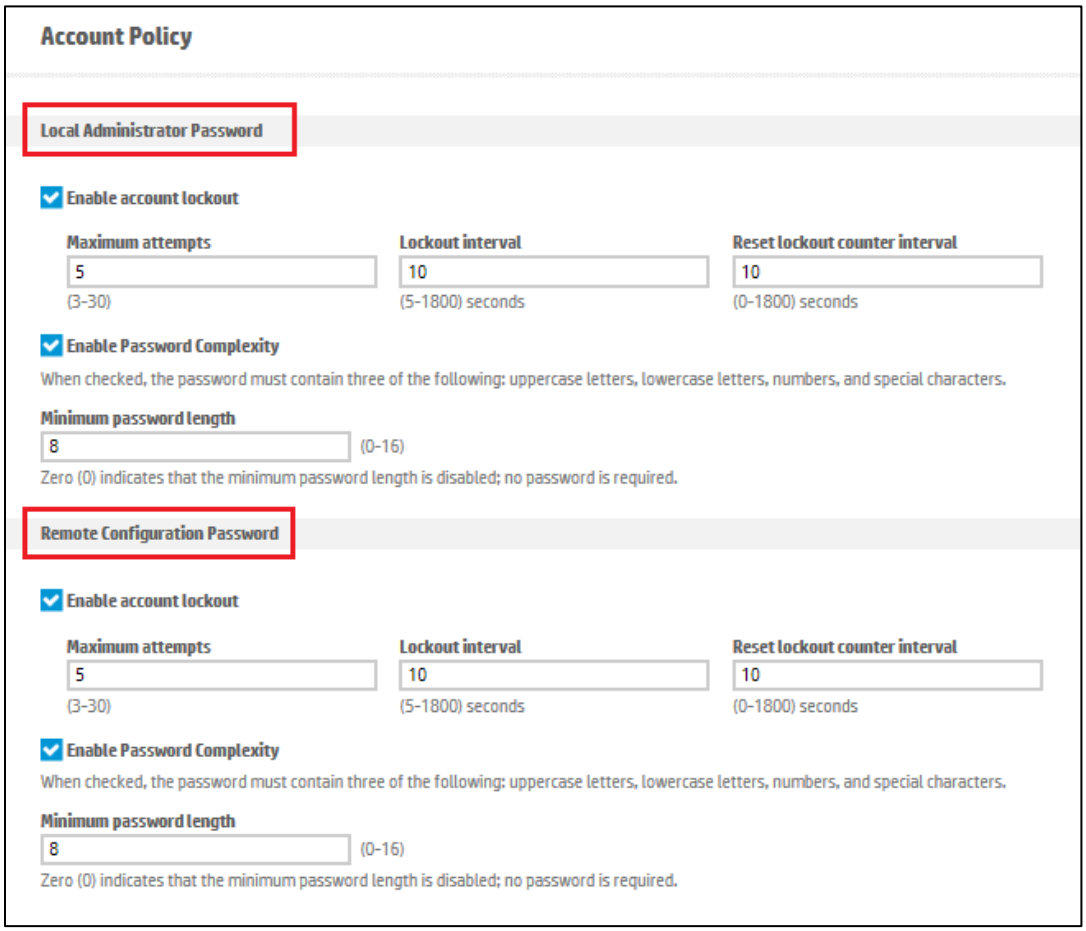


Configuring SNMPv3 passphrases that do not meet the default or specified criteria for Password Complexity or Minimum password length requirements presents the following error(s):



Local Administrator and Remote Configuration Passwords

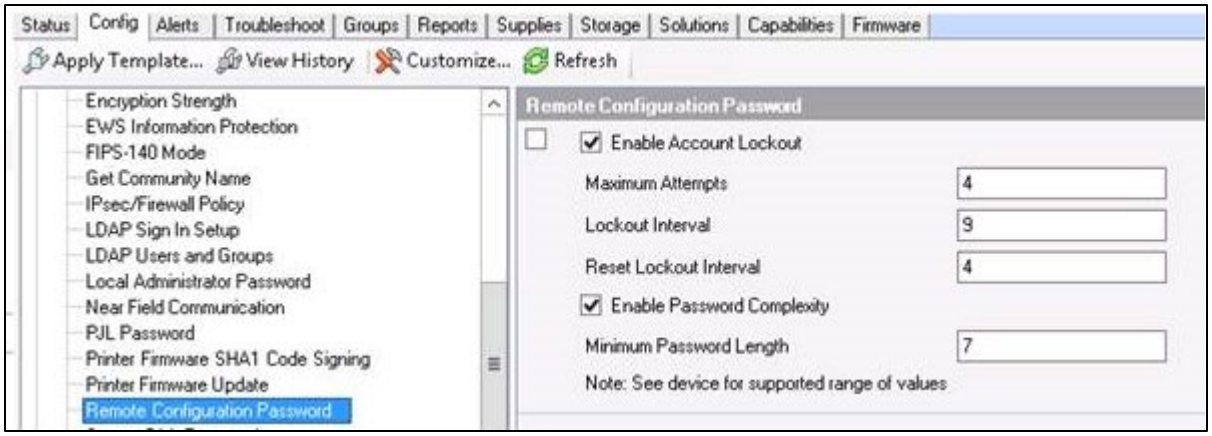
There are separate configuration sections for the Local Administrator Password and the Remote Configuration Password. This allows configuration of the Remote Configuration password to better accommodate HP Web Jetadmin, HP Security Manager, and HP Digital Sending Software.



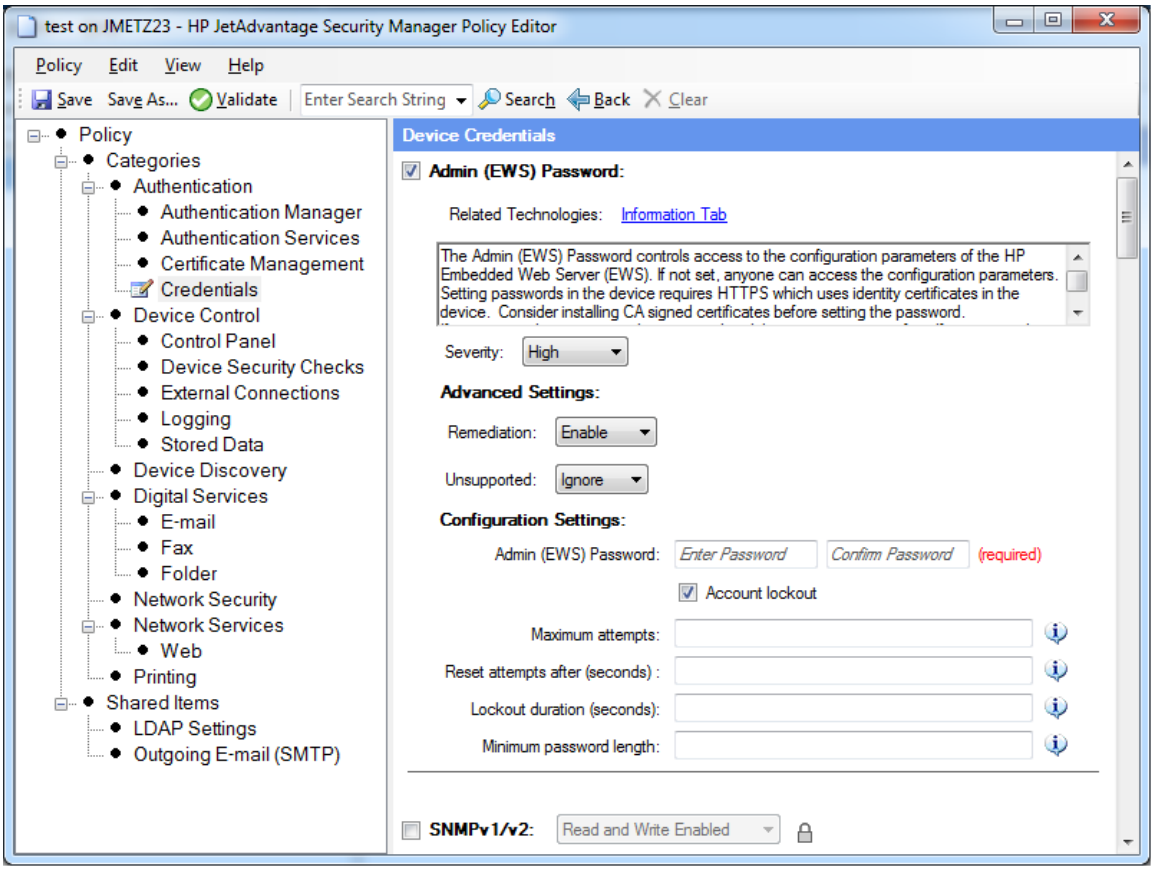
HP Web Jetadmin and HP Security Manager support

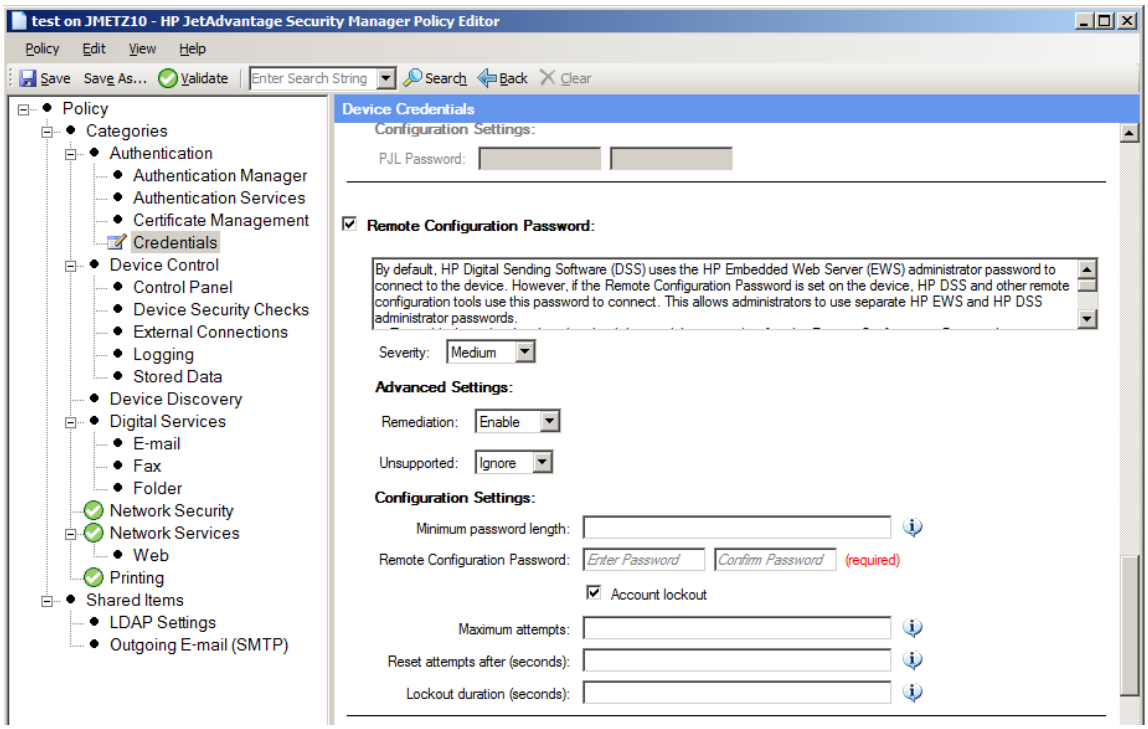
The HP FutureSmart 4 and 5 password administration security features can be configured using the fleet tools HP Web Jetadmin and HP Security Manager.

HP Web Jetadmin configuration is available **in Version 10.4 sr2 or later.**



HP Security Manager **Version 2.1.5 or newer** supports the password administration security features.





www.hp.com/support/
Current HP driver, support, and security alerts
delivered directly to your desktop

Revision 2; January 2022