

HP FutureSmart 4 and 5 -Administrative Password Security Features

Table of contents

Overview	2
Minimum Password Length	4
SNMPv3 password policy configuration	5
Local Administrator and Remote Configuration Passwords	6
HP Web Jetadmin and HP Security Manager support	7

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.

	et color flo or flow MFP M57	w MFP M57	5						
Information General	Copy/Print	Scan/Digital Send	Fax	Troubleshooting	Security	HI Web Services			
General Security Account Policy Access Control	Account Policy	1							
Protect Stored Data	Local Administrator Password								
Certificate Management									
Web Service Security	Chable account lockout								
Self Test	Maximum attempts		Lockout interval		Reset lo	ockout counter interval			
	5		10		10				
	(3-30)		(5-1800)	seconds	(0-1800)) seconds			
	Minimum password 8	assword must contain thre length (0-	-16)	wing: uppercase letters, low oled; no password is require:		umbers, and special characters.			

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.

Enable account lockout		
Maximum attempts	Lockout interval	Reset lockout counter interval
5	10	10
(3-30)	(5-1800) seconds	(0-1800) seconds

- 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

Enable Password Complexity

When checked, the password must contain three of the following: uppercase letters, lowercase letters, numbers, and special characters.

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

The operation has failed.
 Please correct the errors below and try again.
 The password must contain three of the following: upper case letters, lowercase letters, numbers, and special characters.

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.

Minimum password length	
8	(0-16)
Zero (0) indicates that the minimum passwo	ord length is disabled; no password is required.

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

The operation has failed.
 Please correct the errors below and try again.
 New Password must be set to a value of between 8 and 16 characters.

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
 - o 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.

Authentication Protocol		Passphrase
SHA1	~	
		8 to 255 bytes. Must contain 3 of the following: Upper case letters, lower case letters, numbers, and special characters.
Privacy Protocol		Passphrase:
AES-128	~	
		8 to 255 bytes.

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):

⊗	Error: The Authentication Passphrase is invalid. It should be an alphanumeric value between 8 to 255 bytes. The authentication passphrase must contain three of the following: upper case letters, lowercase letters, numbers, and special characters. The authentication passphrase must not contain the username.
---	--

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.

cal Administrator Password		
Enable account lockout		
Maximum attempts	Lockout interval	Reset lockout counter interval
5	10	10
(3-30)	(5-1800) seconds	(0-1800) seconds
Enable Password Complexity		
	this three of the following composition latter	
hen checked, the password must con	tain three of the following: uppercase letter	s, lowercase letters, numbers, and special characters.
	tain three of the following: uppercase letter	s, lowercase letters, numbers, and special characters.
nimum password length		s, lowercase letters, numbers, and special characters.
nimum password length	(0-16)	
nimum password length		
inimum password length ro (0) indicates that the minimum pa	(0-16)	
nimum password length	(0-16)	
nimum password length ro (0) indicates that the minimum pa mote Configuration Password	(0-16)	
nimum password length ro (0) indicates that the minimum pa mote Configuration Password	(0-16) ssword length is disabled; no password is re	quired.
nimum password length ro (0) indicates that the minimum pa mote Configuration Password	(0-16)	
nimum password length ro (0) indicates that the minimum pa mote Configuration Password Enable account lockout	(0-16) ssword length is disabled; no password is re	quired.
nimum password length ro (0) indicates that the minimum pa mote Configuration Password Enable account lockout Maximum attempts	(0-16) ssword length is disabled; no password is re Lockout interval	quired. Reset lockout counter interval
nimum password length ro (0) indicates that the minimum pa mote Configuration Password Enable account lockout Maximum attempts 5	(0-16) ssword length is disabled; no password is re Lockout interval	quired. Reset lockout counter interval 10
nimum password length ro (0) indicates that the minimum pa mote Configuration Password Enable account lockout Maximum attempts 5 (3-30) Enable Password Complexity	(0-16) ssword length is disabled; no password is re Lockout interval 10 (5-1800) seconds	quired. Reset lockout counter interval 10

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.

Status	Config	Alerts	Troubleshoot	Groups	Reports	Supplies	Storage	Solutions	Capabilities	Firmware		
SAP	ply Tem	plate	🖉 View Histo	ory 👷	Customiz	e 💋 R	efresh					
	- Encryption Strength			1	^ Loca	al Adminis						
		formation 10 Mode	n Protection				🗹 Enat	ile Account	Lockout			
		nmurity l				Maximum Attempts			4			
		irewall P				Lockout Interval		9				
			d Groups				Reset L	ockout Inter	val		9	
	and the second se		tor Password		1		✓ Enab	le Passwor	d Complexity			
	PJL Pa		CIM1 C. 4. C.				Minimum	Password	Length		9	
		irmware irmware	SHA1 Code Sig Update	gning		=	Note: Se	e device fo	ar supported ra	ange of value	es	

Encryption Strength	^	Remote Configuration Password	
EWS Information Protection FIPS-140 Mode		Enable Account Lockout	
Get Community Name		Maximum Attempts	4
IPsec/Firewall Policy LDAP Sign In Setup		Lockout Interval	9
LDAP Users and Groups Local Administrator Password		Reset Lockout Interval	4
Near Field Communication		Enable Password Complex	sity
PJL Password Printer Firmware SHA1 Code Signing		Minimum Password Length	7
Printer Firmware Update	=	Note: See device for support	ed range of values

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

test on JMETZ23 - HP JetAdvantage Security	Manager Policy Editor				x
Policy Edit View Help					
🚦 🛃 Save Sav <u>e</u> As 🚫 <u>V</u> alidate Enter Searc	:h String 👻 🔎 Searc <u>h</u> 👍 <u>B</u> ack 🗙	<u>C</u> lear			
	Device Credentials ✓ Admin (EWS) Password: Related Technologies: Informate The Admin (EWS) Password cont Embedded Web Server (EWS). If Setting passwords in the device in device. Consider installing CA sig Severity: High Advanced Settings: Remediation: Enable Unsupported: Ignore Configuration Settings: Admin (EWS) Password: Maximum attempts:	ation Tab rols access to the con not set, anyone can a aquires HTTPS which ned certificates before	Coess the configuratio uses identity certificate setting the password.	n parameters.	
● Printing ● Shared Items	Reset attempts after (seconds) : Lockout duration (seconds):			(i) (i)	
 LDAP Settings Outgoing E-mail (SMTP) 	Minimum password length:			Ū,	
	SNMPv1/v2: Read and Write	Enabled 👻 🗛			Ŧ



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

© Copyright 2022 HP Development Company, LP. 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.



Revision 2; January 2022