

# HP Trusted Platform Module

Plug in and protect



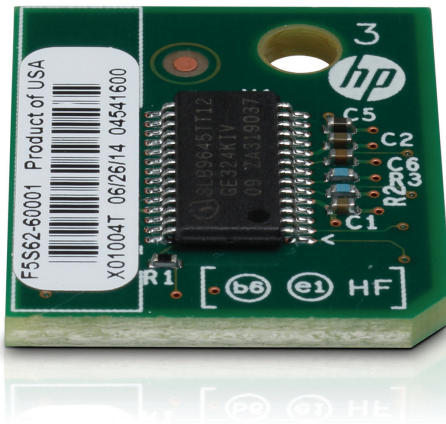
Add an extra level of security to safeguard sensitive information. The HP Trusted Platform Module (TPM) strengthens protection of encrypted credentials and data stored on your printer or MFP.<sup>1</sup>

## Recognize and manage risks

The value of data to your organization cannot be understated. The more data that you acquire and share, the more security risks and requirements you face. Your imaging and printing environment is not immune to costly security breaches.<sup>2</sup> And while security gaps can leave sensitive data dangerously exposed, the HP Trusted Platform Module (TPM) can help guard against such exposures.

With the TPM, you can:

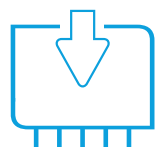
- **Safeguard sensitive user data.** The TPM is an easy-to-install security chip that enables secure storage of information, such as passwords and security keys. By automatically sealing device encryption keys to the TPM, the printer or multifunction printer (MFP) strengthens protection of encrypted credentials and data that it stores.<sup>3</sup> The TPM “wraps” encryption keys with its own storage root key, which is stored within the TPM.
- **Provide secure device identity.** Certificate private keys are both generated by and protected by the TPM, so you can be assured that even your most sensitive client information, data, and documents are safeguarded. The printer or MFP uses the created certificates to prove it is the device it claims to be. Because the certificate private keys never leave the TPM, the identity certificates cannot be spoofed or copied, helping ensure that information received from the device is genuine and that information sent to the device is going to the intended destination.
- **Gain peace of mind.** The TPM is designed to meet international industry standards, specifically the TPM 1.2 standard set by the Trusted Computing Group (TCG).<sup>4</sup> When it comes time to dispose of your printer or MFP, you are able to make the printer or MFP stop using the TPM. When this happens, the TPM will permanently delete the storage root key, and any data that was protected by it cannot be retrieved by anyone who subsequently has access to the device.



## Install quickly and easily

Start safeguarding your sensitive user data right away—installation requires minimal technical expertise. Simply attach the TPM accessory to the device formatter and turn on the device. The TPM automatically pairs with your printer or MFP upon installation. The relevant security keys, passwords, and certificates will automatically be secured by the TPM.

### Installation



1 Snap in TPM



2 Turn on the device



3 Secure keys, passwords, and certificates

## Product specifications

<b>Part number</b>	F5S62A
<b>Supported printers and MFPs</b>	Supported with the latest firmware update using HP FutureSmart 3.0 (version 3.4 and higher) and HP FutureSmart 4.0: HP LaserJet: M506, M604, M605, M606, M607, M608, M609, M712, M806 HP LaserJet MFP: M527, M631, M632, M633, M830 HP LaserJet Managed: M506dnm, M506xm, M830zm HP LaserJet Managed MFP: M527cm, M527dnm HP Color LaserJet: M552, M553, M651, M652, M653, M855 HP Color LaserJet MFP: M577, M681, M682, M880 HP Color LaserJet Managed: M553dnm, M553xm, M880zm, M880zm+ HP Color LaserJet Managed MFP: M577cm, M577dnm HP OfficeJet: X555 HP OfficeJet MFP: X585 HP PageWide Color: 556 HP PageWide Color MFP: 586
<b>Dimensions</b>	0.85 x 0.71 x 0.24 in (21.62 x 18.03 x 6.2 mm)
<b>Weight</b>	0.06 oz (1.71 g)
<b>What's in the box</b>	HP Trusted Platform Module, Install Guide
<b>Warranty</b>	One-year, on-site limited warranty
<b>Environmental ranges</b>	Recommended temperature: Operating: 56 to 86° F (13 to 30° C); Storage: 32 to 104° F (0 to 40° C) Humidity: Operating: 10 to 80% RH, Storage: 10 to 90% RH
<b>Standards and certifications</b>	Designed to the TPM 1.2 standard set by the Trusted Computing Group. <sup>4</sup>

### Learn more

[hp.com/go/jetadvantage](http://hp.com/go/jetadvantage)

<sup>1</sup> Use of the HP Trusted Platform Module accessory may require a firmware upgrade.

<sup>2</sup> The average annualized cost of cybercrime in 2018 was \$13 million. Source: Study conducted by Accenture and Ponemon Institute, "2019 Cost of Cybercrime Study," [accenture.com/us-en/insights/security/cost-cybercrime-study](http://accenture.com/us-en/insights/security/cost-cybercrime-study). 5 billion records were exposed in more than 6,500 breaches in 2018. Source: 2018 Year End Data Breach QuickView Report by Risk Based Security / Cyber Risk Analytics, [riskbasedsecurity.com/2018-ye-breach-quickview-report](http://riskbasedsecurity.com/2018-ye-breach-quickview-report), February 2019.

<sup>3</sup> HP is not liable for maintaining recovery keys. Customers are strongly encouraged to perform the recommended procedures to back up customer keys and data.

<sup>4</sup> The Trusted Computing Group (TCG) is an international industry standards group that develops specifications amongst its members. The TCG publishes the specifications for use and implementation by the industry.

Sign up for updates  
[hp.com/go/getupdated](http://hp.com/go/getupdated)



Share with colleagues

