

High level comparison		DP Pro Workgroup (SaaS and on-premise)	DP Pro Enterprise
GENERAL	<i>Centralized management</i>	<ul style="list-style-type: none"> • Cloud-based Software-as-a-Service; or, • On-premise, standalone solution 	<ul style="list-style-type: none"> • Active Directory-integrated
	<i>Centralized log collection and reporting</i>	✓	✓
	<i>Qualification for operating in FIPS-compliant mode</i>	✓	✓
FULL DISK ENCRYPTION	<i>Centrally-managed Full Disk Encryption with pre-boot authentication and One Step Logon into Windows/ domain</i>	✓	✓
	<i>Out-of-band IT-assisted recovery options (e.g. for forgotten credentials), even with no network or Internet connection</i>	✓	✓
	<i>Emergency data recovery options (e.g. in case of hardware failure)</i>	✓	✓
STRONG AUTHENTICATION	<i>Centrally-managed strong authentication for PC logon</i>	<ul style="list-style-type: none"> • Supports Windows password, fingerprints, smartcards, face recognition 	<ul style="list-style-type: none"> • Supports Windows password, fingerprints, smartcards, face recognition
	<i>Centrally-managed Single Sign-On (SSO)/ Strong authentication for Applications (e.g. web apps, Windows apps, Terminals, etc.)</i>	<ul style="list-style-type: none"> • Supports Windows password, fingerprints, smartcards, face recognition 	<ul style="list-style-type: none"> • Supports Windows password, fingerprints, smartcards, face recognition
	<i>Windows/ Domain password self-service recovery at PC logon</i>	✓	✓
	<i>Out-of-band IT-assisted recovery options for PC logon (e.g. for forgotten credentials), even with no network or Internet connection</i>	✓	✓
	<i>Integration with one-time passwords for authentication into RADIUS applications (tokens or other supported credentials)</i>	-	✓
	<i>Roaming of users' logon data (e.g. domains' username and passwords) and authentication credentials across multiple PCs</i>	-	✓
	<i>Redirection of strong authentication credential data over thin clients/ Citrix/ Terminal Services/ RDP</i>	-	✓
	<i>Support for shared workstations (e.g. kiosks) where users log on to a common Windows account</i>	-	✓
DIGITAL SIGNATURE AND ENCRYPTION	<i>Digital signature of email messages and documents (Office and PDF)</i>	✓	✓
	<i>Encryption of email messages and documents (Office and PDF)</i>	✓	✓

Feature-by-feature comparison		DP Pro Workgroup (SaaS and on-premise)	DP Pro Enterprise
GENERAL	<i>Management interface</i>	<ul style="list-style-type: none"> • Through web-based console 	<ul style="list-style-type: none"> • Through Active Directory MMC
	<i>Database</i>	<ul style="list-style-type: none"> • SQL database 	<ul style="list-style-type: none"> • Active Directory for PC and user data • SQL database for event logs
	<i>Qualification for operating in FIPS-compliant mode</i>	√	√
FULL DISK ENCRYPTION	<i>Encryption of the entire hard drive, including empty sectors</i>	√	√
	<i>Pre-boot authentication</i>	√	√
	<i>Central management of encryption policies (e.g. ON/OFF)</i>	√	√
	<i>Encryption algorithm</i>	<ul style="list-style-type: none"> • AES algorithm; key length 256 	<ul style="list-style-type: none"> • AES algorithm; key length 256
	<i>One Step Logon (aka Single Sign-On) from pre-boot to Windows/ domain</i>	√	√
	<i>Centralized backup of drive encryption keys</i>	√	√
	<i>Out-of-band IT-assisted recovery options (e.g. for forgotten credentials), even with no network or Internet connection</i>	√	√
	<i>Emergency data recovery options (e.g. in case of hardware failure)</i>	√	√
	<i>Centralized collection of Full Disk Encryption status and event logs</i>	√	√
	<i>Centralized reporting on encryption status and activity</i>	√	√
STRONG AUTHENTICATION FOR PC LOGON	<i>Strong authentication at PC logon</i>	√	√
	<i>Policy-based management, centrally enforced (e.g. Use two-factor authentication for domain logon)</i>	√	√
	<i>Windows/ Domain password self-service recovery at PC logon</i>	√	√
	<i>Out-of-band IT-assisted recovery options for PC logon (e.g. for forgotten credentials), even with no network or Internet connection</i>	√	√
	<i>Roaming of users' logon data (e.g. domains' username and passwords) and authentication credentials across multiple PCs</i>	-	√

Feature-by-feature comparison (cont'd)		DP Pro Workgroup <i>(SaaS and on-premise)</i>	DP Pro Enterprise
STRONG AUTHENTICATION FOR PC LOGON (CONT'D)	<i>Ability for IT to manage users' credentials enrollment (i.e. "attended enrollment")</i>	-	✓
	<i>Support for shared workstations (e.g. kiosks) where users log on to a common Windows account</i>	-	✓
	<i>Centralized collection of Strong Authentication status and event logs</i>	✓	✓
	<i>Centralized reporting on authentication status and activity</i>	✓	✓
	<i>Supported credentials</i>	<ul style="list-style-type: none"> • Windows password • Fingerprints • Smartcards • Face recognition 	<ul style="list-style-type: none"> • Windows password • Fingerprints • Smartcards • Face recognition
SINGLE SIGN-ON (SSO)/ STRONG AUTHENTICATION FOR APPLICATIONS	<i>Single Sign-On into all applications (e.g. Web apps, Windows apps, Terminals, etc.), without modifying the applications</i>	✓	✓
	<i>Strong authentication into all applications (e.g. Web apps, Windows apps, Terminals, etc.), without modifying the applications</i>	✓	✓
	<i>Policy-based management, centrally enforced (e.g. Use two-factor authentication for application logon)</i>	✓	✓
	<i>Ability for Administrators to "train" applications for SSO/ strong authentication and deploy data to managed computers</i>	✓	✓
	<i>Supported credentials</i>	<ul style="list-style-type: none"> • Windows password • Fingerprints • Smartcards • Face recognition 	<ul style="list-style-type: none"> • Windows password • Fingerprints • Smartcards • Face recognition
	<i>Integration with OATH one-time passwords for RADIUS applications (software tokens, smart phone tokens and/or in combination with other supported credentials)</i>	-	✓
	<i>Redirection of strong authentication credential data over thin clients/ Citrix/ Terminal Services/ RDP</i>	-	✓
	<i>Roaming of users' logon data (e.g. applications' username and passwords) and strong authentication credentials across multiple computers</i>	-	✓
	<i>Support for shared workstations (e.g. kiosks) where users log on to a common Windows account</i>	-	✓
	<i>Ability for IT to manage users' credentials enrollment (i.e. "attended enrollment")</i>	-	✓

Feature-by-feature comparison (cont'd)		DP Pro Workgroup <i>(SaaS and on-premise)</i>	DP Pro Enterprise
SINGLE SIGN-ON (SSO)/ STRONG AUTHENTICATION FOR APPLICATIONS (CONT'D)	<i>Centralized collection of Strong Authentication status and event logs</i>	√	√
	<i>Centralized reporting on authentication status and activity</i>	√	√
DIGITAL SIGNATURE FOR EMAIL AND DOCUMENTS	<i>Digital signature of email messages and documents (Office and PDF)</i>	√	√
	<i>Encryption of email messages and documents (Office and PDF)</i>	√	√
	<i>Policy-based management, centrally enforced (e.g. use two-factor authentication for digital signature)</i>	√	√
	<i>Centralized collection of encryption and signature status and event logs</i>	√	√
	<i>Centralized reporting on encryption and signature status and activity</i>	√	√
MISC. REQUIREMENTS	<i>Supported client software</i>	<ul style="list-style-type: none"> • DP Pro Workstation for Workgroup; or, • HP ProtectTools 5.04 or later 	<ul style="list-style-type: none"> • DP Pro Workstation for Enterprise; or • DigitalPersona Pro Kiosk; or, • HP ProtectTools 5.04 or later
	<i>Server Operating System</i>	<ul style="list-style-type: none"> • Windows 7 (32- & 64-bit) • Windows Server 2008 and R2 (32- & 64-bit) <i>(Not relevant for SaaS option)</i>	<ul style="list-style-type: none"> • Windows Server 2003 (32- & 64-bit) • Windows Server 2008 and R2 (32- & 64-bit)
	<i>Client Operating System</i>	<ul style="list-style-type: none"> • Windows 7 (32- & 64-bit) • Windows Vista (32- & 64-bit) • Windows XP SP3 (32-bit) 	<ul style="list-style-type: none"> • Windows 7 (32- & 64-bit) • Windows Vista (32- & 64-bit) • Windows XP SP3 (32-bit)
	<i>Browsers</i>	<ul style="list-style-type: none"> • Internet Explorer 6 or later • Firefox 2 or later 	<ul style="list-style-type: none"> • Internet Explorer 6 or later • Firefox 2 or later
	<i>Fingerprint readers</i>	<ul style="list-style-type: none"> • Most sensors built into notebooks • Select peripherals 	<ul style="list-style-type: none"> • Most sensors built into notebooks • Select peripherals
	<i>Smartcards</i>	<ul style="list-style-type: none"> • PKCS#11 and CSP cards from major providers 	<ul style="list-style-type: none"> • PKCS#11 and CSP cards from major providers
	<i>One-time password tokens</i>	<ul style="list-style-type: none"> • Any OATH-compliant hardware or software token, including Windows, Android, iPhone, Blackberry, Palm, Windows mobile 	<ul style="list-style-type: none"> • Any OATH-compliant hardware or software token, including Windows, Android, iPhone, Blackberry, Palm, Windows mobile
	<i>Digital certificates</i>	<ul style="list-style-type: none"> • Any X.509 digital certificate 	<ul style="list-style-type: none"> • Any X.509 digital certificate