Funzioni di sicurezza Lexmark

Sicurezza all'avanguardia per stampanti e multifunzione Lexmark

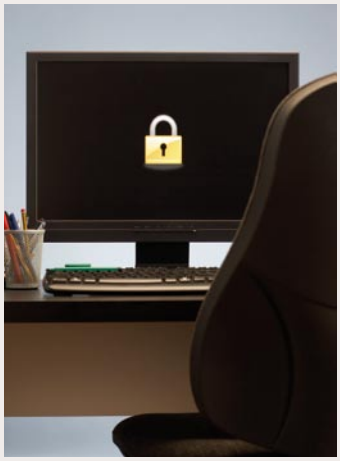
I dati aziendali sono il bene più prezioso.
Lexmark vi aiuta a custodirli.

LEXMARK™

Funzioni di sicurezza Lexmark

Siete in procinto di aggiungere un nuovo dispositivo alla vostra rete. Sarà sicuro? Qualche dubbio sorge. Sarà possibile impedire gli accessi non autorizzati? La sicurezza della rete risulterà compromessa? Come si fa a saperlo? Prima di introdurre una nuova stampante o multifunzione in azienda sono tante le domande che bisogna porsi. Come ogni cosa che si serve della rete, le stampanti e i multifunzione sono dispositivi complessi e comportano dei rischi se non vengono protetti adeguatamente.

Lexmark crea i dispositivi di rete tenendo sempre presente il problema della sicurezza. Le nostre stampanti e i multifunzione sono dotati di un'ampia gamma di funzioni avanzate che proteggono dati e documenti per tutto il flusso di lavoro, dal trasferimento in rete dei dati fino al momento in cui le pagine stampate arrivano sul vassoio di uscita. Date uno sguardo a questa brochure per rendervi conto di quanto stiamo facendo per la sicurezza della vostra azienda.



Gestione remota sicura

Potenti funzioni per gestire i dispositivi con efficienza e in tutta sicurezza

Per gestire in modo efficiente ed efficace un parco stampanti di rete, la gestione remota è un must. Occorre però che tale gestione sia anche sicura. È necessario che la configurazione del dispositivo sia consentita solo a chi è autorizzato e impedita a chi non lo è.

Il processo di gestione del dispositivo va inoltre protetto in modo che il traffico di rete associato alla gestione remota non possa essere intercettato, sottratto o utilizzato in modo improprio. I dispositivi Lexmark includono tutta una serie di funzioni che facilitano la gestione remota e la rendono più sicura. Tali funzioni possono essere configurate mediante la pagina Web integrata del dispositivo.

Registro di controllo I dispositivi Lexmark hanno l'abilità di tenere traccia degli eventi potenzialmente pericolosi. Monitoraggio degli eventi per tipo, funzioni di esportazione, registrazione di tutti i comportamenti, sono solo alcune delle funzioni del registro. L'abilitazione di un registro di controllo riduce l'esposizione ai rischi mediante il monitoraggio degli eventi, l'individuazione dei potenziali rischi e l'integrazione con il sistema di rilevamento delle intrusioni per un monitoraggio proattivo in tempo reale. Sono oltre 100 le variabili e gli eventi registrati nel dispositivo.

Aggiornamenti firmware con firma digitale Le stampanti e le multifunzione Lexmark analizzano automaticamente gli aggiornamenti firmware scaricati. I firmware non correttamente preparati e firmati da Lexmark vengono rifiutati. In tal modo i firmware non approvati non verranno mai eseguiti sui dispositivi e questo ne eviterà l'esposizione a software pericolosi, quali virus e worm.

Gestione dei certificati Stampanti e multifunzione utilizzano certificati per le autenticazioni HTTPS, SSL, IPSec e 802.1x.

La funzione di gestione dei certificati consente ai dispositivi l'integrazione con un'infrastruttura a chiave pubblica (PKI) mediante la configurazione di comunicazioni affidabili per 802.1x, IPSec, l'autenticazione dei certificati per la convalida dei domain controller, i protocolli SSL LDAP ed EWS o altri servizi che utilizzano SSL.

HTTPS Criptando il traffico su Web, la gestione remota attraverso la pagina Web integrata dei dispositivi può essere effettuata in tutta sicurezza.

SNMPv3 SNMP è un protocollo di gestione rete standard. La versione 3 di tale protocollo comprende un'ampia gamma di funzioni di sicurezza. Le stampanti e le multifunzione Lexmark supportano il protocollo SNMPv3, compresi i componenti di autenticazione e di crittografia dei dati e pertanto consentono una gestione sicura dei dispositivi in remoto. Sono supportati anche i protocolli SNMPv1 e SNMPv2 che è possibile configurare e/o disabilitare in maniera indipendente.

IPv6 Stampanti e multifunzione supportano il protocollo IPv6 per consentire la connessione alle reti IPv6.

Reimpostazione sicura della password La funzione permette di reimpostare il controllo accessi nel menu di sicurezza del dispositivo in modo da consentire l'accesso nel caso in cui la password dell'amministratore venga persa o dimenticata o se si perde la connessione in rete. A tale scopo si utilizza un'impostazione del firmware sulla pagina Web integrata del dispositivo e si regola un ponticello sulla scheda di sistema del dispositivo.

Password di riserva La password di riserva consente di accedere al menu di sicurezza del dispositivo indipendentemente dal metodo di protezione utilizzato o della sua disponibilità. Ad esempio, se una rete o un server LDAP non è disponibile l'amministratore può sempre accedere al menu di sicurezza e apportare modifiche per consentire l'accesso al dispositivo.

LEXMARK™

Funzioni di sicurezza Lexmark

Interfacce di rete sicure

Protezione dei dispositivi contro hacker e virus

Il controllo di un dispositivo di rete implica il processo di protezione delle sue interfacce di rete. Tale processo comprende l'eliminazione delle funzioni e delle caratteristiche non necessarie o non utilizzate per impedirne l'abuso, bloccando le interfacce rimanenti e proteggendo i dati nel dispositivo. Nelle stampanti e multifunzione Lexmark è presente tutta una serie di meccanismi che facilitano il processo di controllo dei dispositivi.

Filtraggio delle connessioni TCP È possibile configurare le stampanti e i multifunzione in modo da consentire connessioni TCP/IP solo da un particolare elenco di indirizzi. In questo modo il dispositivo è protetto contro le stampe o le operazioni di configurazione non autorizzate. Il filtraggio delle connessioni TCP si imposta compilando il campo dell'elenco ristretto dei server.

Filtraggio porte Il traffico di rete del dispositivo può essere controllato attraverso la configurazione delle sue porte di rete. Mediante il filtraggio del traffico di determinate porte di rete è possibile bloccare esplicitamente protocolli quali telnet, FTP, SNMP, HTTP e così via.

802.1x L'autenticazione della porta 802.1x consente a stampanti e multifunzione di connettersi a reti cablate e wireless solo dopo aver effettuato l'autenticazione. L'autenticazione della porta 802.1x può essere utilizzata con la funzione WPA (Wi-Fi Protected Access) di un server di stampa wireless opzionale e ottenere così una protezione WPA Enterprise.

IPSec Il protocollo IPSec protegge il traffico in entrata e in uscita dei dispositivi Lexmark mediante crittografia e autenticazione. Con IPSec è possibile trasmettere in rete i dati acquisiti con lo scanner criptandoli e proteggendo così i contenuti che potranno essere inviati a qualsiasi destinazione, inclusi i server su cui è eseguito Lexmark Document Distributor, posta elettronica e archivi di rete.

SNTP I dispositivi Lexmark supportano l'uso del protocollo Secure Network Time Protocol (SNTP), utilizzato per la sincronizzazione degli orologi dei diversi dispositivi in rete. Per consentire l'implementazione del protocollo SNTP e rispettarne i requisiti, i dispositivi Lexmark forniscono un campo di autenticazione e autorizzazione per la procedura di configurazione.

Separazione fax/rete Lexmark offre un'ampia gamma di dispositivi multifunzione con funzioni sia per rete che per modem fax. Negli ambienti di rete in cui la sicurezza è cruciale, la combinazione di queste due funzioni su un solo dispositivo può rappresentare un problema, ma le multifunzione Lexmark sono progettate in modo che i componenti hardware e firmware tengano separati i meccanismi, impedendo le interazioni dirette tra modem e adattatore di rete. Per di più, il modem può accettare solo dati immagine associati a una trasmissione fax. Gli altri dati, ovvero quelli per l'accesso remoto o gli aggiornamenti del firmware o di rete, vengono dichiarati non validi e provocano la disconnessione telefonica.

Funzioni di sicurezza Lexmark

Protezione dei dati su disco rigido

Crittografia, pulizia e protezione dei dati archiviati

Per ampliare la funzionalità dei dispositivi, Lexmark ha dotato alcune delle sue stampanti e multifunzione di dischi rigidi che consentono di archiviare le immagini dei documenti per l'elaborazione dei lavori. E per proteggerli offre efficaci controlli che ne migliorano la sicurezza o che impediscono a utenti in mala fede di ottenere l'accesso fisico al disco rigido.

Crittografia del disco rigido È possibile impostare la crittografia per i dischi rigidi delle stampanti e dei multifunzione. Il dispositivo genera al proprio interno una chiave AES (Advanced Encryption Standard) a 256 bit che cripta tutti i dati presenti sul disco rigido. La chiave è memorizzata in modo non contiguo e consente di accedere ai contenuti del disco rigido solo sul dispositivo originale. I dati presenti su un disco rigido rubato risulteranno inaccessibili anche qualora venisse installato su un modello di stampante o multifunzione identico.

Pulizia sicura del disco rigidoè possibile cancellare completamente i dati sul disco rigido in modo da non lasciare dati residui leggibili. La pulizia del disco prevede tre modalità: manuale, automatica e pianificata. Viene fornita una pulizia a più passaggi, conforme agli standard NIST (National Institute of Standard Technology) e del Dipartimento della Difesa (DoD).

Supporto con bloccaggio fisico Le stampanti e i multifunzione Lexmark consentono l'uso di sistemi di bloccaggio fisico. In questo modo si blocca anche la gabbia metallica in cui sono alloggiati i dischi rigidi e i componenti opzionali, impedendone la manomissione e il furto.

Cancellazione della memoria non volatile: Offre uno strumento per cancellare tutti i contenuti archiviati nei vari moduli di memoria flash presenti sul dispositivo. Tale funzione elimina completamente tutte le impostazioni, soluzioni, lavori e fax sul dispositivo. Questa funzione è stata progettata per quando il dispositivo Lexmark viene ritirato, riciclato o comunque rimosso da un ambiente sicuro.

Accesso protetto

Operazioni quotidiane più semplici e sicure

Le scansioni di rete e i dati di stampa possono rappresentare uno degli aspetti più importanti nella sicurezza delle reti. I documenti contengono abitualmente informazioni sensibili, ad esempio dati finanziari, informazioni che consentono di identificare clienti o dipendenti e informazioni sui clienti.

I dispositivi di stampa e di elaborazione delle immagini in genere sono collocati in aree molto trafficate e dotate soltanto di protezioni fisiche elementari. In questo scenario, è facilissimo che i dati riservati finiscano, accidentalmente o intenzionalmente, nelle mani sbagliate.

I dispositivi Lexmark forniscono funzioni standard che ne possono ridurre notevolmente la vulnerabilità.

Porte USB protette Stampanti e multifunzione laser Lexmark consentono l'uso di dispositivi USB. Tali dispositivi potrebbero destare preoccupazione in ambienti di rete in cui la sicurezza è cruciale. Invece le porte host USB Lexmark sono dotate di diversi meccanismi che ne impediscono l'uso improprio. Tali meccanismi di protezione comprendono, tra l'altro, limitazione agli accessi mediante l'autenticazione, parametri relativi ai tipi di file, pianificazione delle interazioni con il dispositivo, interdizione dei supporti di avvio e possibilità di disattivare completamente la porta host USB.

Ricerca nella rubrica LDAP Quando si inviano e-mail o fax, è possibile ricercare gli indirizzi dei destinatari. I multifunzione Lexmark utilizzano il protocollo LDAP a tal scopo per interrogare i server di directory aziendale.

Secure LDAP Tutto il traffico LDAP in entrata e in uscita dai dispositivi Lexmark può essere protetto con i protocolli TLS/SSL. Le informazioni LDAP, quali credenziali, nomi, indirizzi e-mail e numeri di fax, scambiate attraverso una connessione TLS/SSL vengono criptate per garantirne riservatezza.

Autenticazione e autorizzazione: effettuare l'autenticazione prima di accedere a funzioni quali copia, fax, scansione verso e-mail, scansione verso cartella di rete, script dei flussi di lavoro e/o applicazioni integrate consente di limitarne l'uso. I dispositivi Lexmark possono essere configurati in modo che gli utenti debbano effettuare l'autenticazione con account interni, password e/o PIN oppure utilizzando una directory aziendale mediante NTLM, Kerberos 5, LDAP e/o LDAP+GSSAPI.

Funzioni di sicurezza Lexmark

Questi metodi di autenticazione sono sicuri se eseguiti mediante un canale SSL e compatibili con Active Directory e altre piattaforme di directory server. In aggiunta all'autenticazione è possibile utilizzare un'autorizzazione utente o per gruppi che limiti l'uso di particolari funzioni del dispositivo a determinati utenti o membri di un gruppo appartenenti all'infrastruttura di directory aziendale.

Inserimento automatico dell'indirizzo e-mail del mittente Quando si esegue l'autenticazione per effettuare la scansione verso e-mail di un documento, viene ricercato automaticamente l'indirizzo del mittente e inserito nel campo "Da". Così il destinatario conosce l'autore del messaggio, che non risulta anonimo né generato dal multifunzione.

Modelli di sicurezza I modelli di sicurezza consentono di limitare gli accessi e sono composti da uno o più elementi basilari. Essi sono definiti dagli amministratori del dispositivo e sono presenti nel menu a discesa di controllo accessi. Vengono applicati a particolari menu e flussi di lavoro sul dispositivo Lexmark. I modelli di sicurezza possono coprire un'ampia gamma di funzioni e consentono di controllare le più importanti funzioni di sicurezza di un dispositivo Lexmark.

Controllo accessi Il controllo accessi consente di scegliere da un menu a discesa i modelli di sicurezza disponibili per controllare l'accesso remoto a particolari menu, funzioni e flussi di lavoro. Consente inoltre di disattivare completamente le funzioni.

Sono disponibili oltre 50 controlli di accesso per offrire la massima flessibilità in qualunque ambiente. Tra i controlli di accesso disponibili sono inclusi quelli per le funzioni (copia, stampa, fax, scansione verso e-mail, FTP, lavori sospesi, rubrica), i menu di sicurezza, gli aggiornamenti firmware, le applicazioni integrate, le impostazioni dei menu (report, carta, impostazioni, rete/porte e così via), il blocco del pannello operatore, le impostazioni di gestione remota e altri ancora.

Limiti di accesso È possibile impedire l'uso non autorizzato di un dispositivo limitando il numero di accessi consecutivi non riusciti. Superato il limite, il dispositivo viene bloccato per un periodo di tempo stabilito dall'amministratore. La configurazione di tali impostazioni è possibile utilizzando i limiti di accesso sul dispositivo. Queste impostazioni consentono inoltre di regolare i timeout per l'accesso remoto e la schermata iniziale. Se è attivato il registro di controllo il dispositivo tiene traccia degli eventi in relazione ai limiti di accesso.

Blocco del pannello operatore La funzione consente di impostare un dispositivo in stato di blocco per impedire attività operative e di configurazione. Non sarà possibile effettuare scansioni o copie, né intervenire sulla configurazione mediante il pannello operatore e i lavori in arrivo non rimarranno in mostra nel cassetto di uscita. Se il dispositivo è dotato di disco rigido le stampe e i fax in arrivo vengono memorizzati sul disco invece che stampati. Il dispositivo potrà essere sbloccato mediante l'immissione di credenziali utente autorizzate. A quel punto i lavori sospesi verranno stampati e il dispositivo riprenderà il normale funzionamento.

Stampa riservata I lavori di stampa sono tenuti in RAM o sul disco rigido finché il destinatario non inserisce il PIN corretto e rilascia la stampa. È possibile impostare una validità, compresa tra un'ora e una settimana, per i lavori sospesi. Inoltre si può impostare un limite per il numero di volte che è possibile inserire un PIN errato, prima che i processi corrispondenti vengano eliminati.

Scheda PrintCryption La soluzione applicativa Lexmark PrintCryption™ rafforza la sicurezza dell'ambiente aziendale proteggendo le informazioni sensibili con le funzioni di crittografia e decrittazione presenti sui dispositivi di rete. Questo livello di sicurezza della stampa è ideale per le aziende che gestiscono informazioni altamente riservate, personali, finanziarie, mediche, tecniche o brevettate.

Sospensione dei fax in arrivo È possibile configurare i dispositivi Lexmark in modo che in orari programmati, i fax in entrata vengano sospesi. Tali fax vengono tenuti sul disco rigido fino a che nel dispositivo Lexmark non vengono inserite le appropriate credenziali. Tra le credenziali sono compresi PIN, password e ID utente e password di rete.

LEXMARK™

Funzioni di sicurezza Lexmark

Principi comuni

IEEE 2600: Molti multifunzione Lexmark hanno ottenuto la certificazione Common Criteria, eppure i nostri prodotti sono progettati per risultare conformi agli standard ambientali operativi più rigidi delineati dal gruppo di lavoro IEEE 2600. Tale gruppo è stato creato per produrre standard di sicurezza per i dispositivi di stampa derivanti dall'esperienza collettiva di dozzine di professionisti provenienti dalle maggiori case produttrici di dispositivi di stampa, da laboratori di collaudo, agenzie statali e altre organizzazioni. Nel 2008, gli standard IEEE 2600 sono stati adottati dal National Information Assurance Partnership e utilizzati come base per la valutazione dei prodotti, nota anche come profilo di protezione.

Informazioni sulle porte host USB Lexmark

Funzioni consentite dalle porte Visualizzazione di immagini da una penna USB, visualizzazione di file flash per nome (se è selezionato un file flash il firmware della stampante viene aggiornato, sempre che gli aggiornamenti firmware siano consentiti nelle impostazioni di sicurezza), selezione dei lavori da stampare e possibilità di eseguire la scansione di dati direttamente su penna USB, se disponibili in un formato di scansione supportato.

Funzioni NON consentite dalle porte Connessione o uso di dispositivi USB che non siano di archiviazione di massa, lettori di schede o periferiche Human Interface, inviare o elaborare flussi di stampa quali PCL, PostScript o altri, inviare dati di qualsiasi genere, registrare dati dalla stampante, eseguire codice o avviare la stampante da un dispositivo USB collegato.

Disattivazione delle unità USB È facile disattivare la porta USB del dispositivo Lexmark attraverso il server Web integrato. Questa operazione risulta particolarmente importante per quelle aziende che hanno adottato criteri e normative di sicurezza che vietano tali funzioni.

Sicurezza di alto livello Per evitare di compromettere la sicurezza, la porta USB sulla parte anteriore del dispositivo è progettata in modo da consentire solo alcuni tipi di operazioni. Gli amministratori dei dispositivi possono poi limitare l'accesso alle porte host USB mediante i controlli degli accessi con la funzione di autenticazione e autorizzazione, funzione che è possibile personalizzare in base ai criteri di protezione delle reti adottati dalle aziende.

Sicurezza dei fax

È possibile accedere ai dati del multifunzione mediante una connessione telefonica esterna?

No! Sebbene alcuni dispositivi consentano l'accesso e il controllo remoto, mediante protocolli del tipo Telnet, i prodotti Lexmark non sono attrezzati per tale attività. I multifunzione Lexmark non consentono alcun tipo di configurazione tramite telefono. Allo stesso modo, non esiste una modalità diagnostica che meccanismi esterni possano utilizzare per controllare il comportamento del modem o per intervenire sulla configurazione. L'unica attività svolta dal modem analogico è l'invio e la ricezione di fax.

La scheda fax e la scheda di rete sono totalmente collegate tra loro?

Le funzioni dell'adattatore di rete interno sono implementate separatamente dal modem. Il modem e la scheda di rete risedono su diversi gruppi di componenti.

La scheda fax è collegata da un cavo a una scheda secondaria, mentre l'adattatore di rete risiede direttamente sulla scheda madre del multifunzione. La connessione fax e le interazioni con l'adattatore di rete possono essere gestite dal firmware Lexmark, configurato in modo da impedire la diretta interazione tra fax e componenti di rete.

È possibile aggiornare il firmware del multifunzione mediante telefono?

Nessun codice eseguibile può essere accettato dal modem fax o dal firmware Lexmark, che possono ricevere solo dati immagine. Se i dati in entrata non rappresentano immagini, vengono dichiarati non validi. Non è possibile produrre firmware modificato, o qualunque altro tipo di codice, come processo per il fax e farlo arrivare al multifunzione ancora in ordine.

LEXMARK™

Funzioni di sicurezza Lexmark

Modelli / Funzioni di sicurezza	Stampanti a funzione singola														Stampanti multifunzione														
	E260	E360	E46x	T65x	W850	C540	C543	C544	C546	C734	C736	C792	C925	C950	X20x	X264	X363	X364	X463	X464	X466	X543	X544	X546	X548	X65x	X73x	X792	X86x	X925x	X95x
Stampanti monocromatiche	•	•	•	•	•										•	•	•	•	•	•	•				•			•			
Stampanti a colori						•	•	•	•	•	•	•	•	•								•	•	•	•	•	•		•	•	•
Carta di formato A4	•	•	•	•		•	•	•	•	•	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•				
Carta di formato A3					•								•	•														•	•	•	•
Gestione remota sicura																															
Registro di controllo			•	•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Aggiornamenti firmware con firma digitale	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Gestione certificati			•	•	•			•[1]		•	•	•	•	•				•	•	•	•		•[1]	•	•	•	•	•	•	•	•
HTTPS			•	•	•					•	•	•	•	•				•	•	•			•	•	•	•	•	•	•	•	•
SNMPv3			•	•	•					•	•	•	•	•				•	•	•			•	•	•	•	•	•	•	•	•
IPv6	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Reimpostazione sicura della password			•	•	•					•	•	•	•	•				•	•	•				•	•	•	•	•	•	•	•
Password di riserva			•	•	•					•	•	•	•	•				•	•	•				•	•	•	•	•	•	•	•
Interfacce di rete sicure																															
Filtraggio delle connessioni TCP	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Filtraggio porte			•	•	•			•	•	•	•	•	•	•				•	•	•		•	•	•	•	•	•	•	•	•	•
802.1x			•	•	•			•[1]		•	•	•	•	•				•	•	•		•[1]	•	•	•	•	•	•	•	•	•
IPSec			•	•	•					•	•	•	•	•				•	•	•				•	•	•	•	•	•	•	•
Secure SNTP			•	•	•					•	•	•	•	•				•	•	•				•	•	•	•	•	•	•	•
Separazione fax/rete															•	•		•	•	•	•		•	•	•	•	•	•	•	•	•
Protezione dei dati su disco rigido																															
Crittografia del disco rigido (2)				•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Pulizia del disco rigido (2)				•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Supporto con bloccaggio fisico	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Accesso protetto																															
Porte USB protette (Pianificazione dispositivi USB)			•	•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Ricerca nella rubrica LDAP																•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Secure LDAP																			•	•	•			•	•	•	•	•	•	•	•
Autenticazione			•	•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Autorizzazione			•	•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Inserimento automatico dell'indirizzo e-mail del mittente																			•	•	•			•	•	•	•	•	•	•	•
Modelli di sicurezza			•	•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Controllo accessi			•	•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Limiti di accesso			•	•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Blocco del pannello operatore			•	•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Stampa riservata			•	•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Scheda PrintCryption (opzionale)			•	•	•					•	•	•	•	•					•	•	•			•	•	•	•	•	•	•	•
Sospensione dei fax in arrivo																			•[3]	•	•			•	•	•	•	•[3]	•	•	•
Certificazione con criteri comuni (multifunzione)																			•	•	•				•	•		•			

[1] Solo modelli DW
[2] Disponibile su alcuni modelli con disco rigido di serie o che supportano l'aggiornamento con disco rigido opzionale
[3] Opzionale per i modelli X463 e X86xdeV3

LEXMARK™

Funzioni di sicurezza Lexmark

La sicurezza delle stampe è un argomento molto complesso per cui è necessario prendere in considerazione numerosi e importanti aspetti. Le stampanti e le multifunzione Lexmark sono dotate di un'ampia gamma di funzioni all'avanguardia che aiutano a proteggere i dispositivi, l'infrastruttura, i documenti e i dati sensibili.

Timbro dell'azienda

Per ulteriori informazioni relative ai prodotti e ai servizi Lexmark visitare il sito Web www.lexmark.it

LEXMARK™