



Autenticazione con scheda

Guida dell'amministratore

Sommar

Panoramica.....	4
Prerequisiti di impostazione.....	5
Accesso al server Web incorporato.....	5
Aggiunta di un account utente interno.....	5
Impostazione di gruppi per account utente interni.....	5
Creazione di un modello di protezione.....	6
Configurazione dei controlli di accesso.....	6
Configurazione dell'applicazione.....	8
Accesso alla pagina di configurazione dell'applicazione.....	8
Configurazione dell'autenticazione amministratore.....	8
Configurazione della schermata di accesso.....	9
Autenticazione basata sulla stampante.....	9
Autenticazione servizio Web.....	11
Autenticazione Servizio identità.....	12
autenticazione tramite PIN.....	13
Autenticazione tramite LDAP.....	14
Impostazione delle preferenze dell'applicazione.....	15
Visualizzazione delle aree di autenticazione per gli account utente.....	15
Esportazione o importazione di un file di configurazione.....	16
Gestione dell'applicazione.....	17
Accesso alla pagina di stato dell'applicazione.....	17
Gestione degli account utente e delle stampanti client.....	17
Riassegnazione dei ruoli per la stampante.....	18
Uso dell'applicazione.....	20
Registrazione degli utenti.....	20
Registrazione di un PIN.....	20
Accesso manuale alla stampante.....	20
Risoluzione dei problemi.....	21

Domande frequenti.....	25
Avvertenze.....	27
Indice.....	28

Panoramica

Utilizzare l'applicazione per proteggere l'accesso a una stampante usando un lettore di schede. Quando gli utenti effettuano l'accesso tramite contatto sul lettore, le loro credenziali vengono autenticate utilizzando uno dei seguenti elementi:

- Una stampante principale. Se la stampante principale non è in linea, la stampante di backup assume il ruolo della stampante principale finché questa non torna in linea.

Nota: durante l'impostazione delle stampanti, assicurarsi che si trovino sulla stessa rete.

- Server LDAP (Lightweight Directory Access Protocol), server LDD (Lexmark™ Document Distributor) o fornitori del servizio di identità a seconda dell'autenticazione impostata dall'organizzazione.

Questo documento fornisce le istruzioni per la configurazione, l'utilizzo e la risoluzione dei problemi relativi all'applicazione.

Prerequisiti di impostazione

È necessario disporre dei diritti di amministrazione per configurare l'applicazione.

Accesso al server Web incorporato

- 1 Ottenere l'indirizzo IP della stampante. Effettuare una delle seguenti operazioni:
 - Individuare l'indirizzo IP sulla schermata iniziale della stampante.
 - Visualizzare l'indirizzo IP nella sezione TCP/IP del menu Rete/Porte.
- 2 Aprire un browser web e immettere l'indirizzo IP della stampante.

Aggiunta di un account utente interno

È necessario disporre di un account utente interno quando si utilizza l'autenticazione basata su stampante.

- 1 Da Embedded Web Server, fare clic su **Impostazioni** o **Configurazione**.
- 2 A seconda del modello di stampante, svolgere una delle seguenti operazioni:
 - Fare clic su **Protezione** > **Impostazioni di protezione** > **Account interni** > **Aggiungi un account interno**.
 - Fare clic su **Protezione** > **Modifica impostazioni di protezione** > **Account interni** > **Aggiungi un account interno**.
- 3 Immettere le informazioni dell'account, quindi fare clic su **Invia**.
- 4 Se necessario, dalla sezione Gestisci account interni, digitare un nome del blocco personalizzato, quindi specificare le credenziali dell'utente richieste.
- 5 Fare clic su **Inoltra**.

Impostazione di gruppi per account utente interni

- 1 Da Embedded Web Server, fare clic su **Impostazioni** o **Configurazione**.
- 2 A seconda del modello di stampante, svolgere una delle seguenti operazioni:
 - Fare clic su **Protezione** > **Impostazioni di protezione** > **Account interni** > **Impostazione di gruppi per l'uso con account interni**.
 - Fare clic su **Protezione** > **Modifica impostazioni di protezione** > **Account interni** > **Impostazione di gruppi per l'uso con account interni**.
- 3 Immettere un nome di gruppo, quindi fare clic su **Aggiungi**.
- 4 Aggiungere gli account interni al gruppo.
- 5 Fare clic su **Inoltra**.

Creazione di un modello di protezione

Un modello di protezione è composto da blocchi di protezione, come account interni, Kerberos, LDAP, LDAP+GSSAPI e Active Directory. Questi modelli sono applicati al controllo di accesso per garantire la protezione delle funzioni e delle applicazioni della stampante.

- 1 Da Embedded Web Server, fare clic su **Impostazioni** o **Configurazione**.
- 2 A seconda del modello di stampante, effettuare una delle seguenti operazioni:
 - Fare clic su **Protezione** > **Impostazioni di protezione** > **Modelli di protezione** > **Aggiungi un modello di protezione**.
 - Fare clic su **Protezione** > **Modifica impostazioni di protezione** > **Modelli di protezione** > **Aggiungi un modello di protezione**.
- 3 Digitare il nome di un modello di protezione, quindi selezionare una delle seguenti impostazioni di autenticazione:
 - Per l'autenticazione basata sulla stampante su un'impostazione autonoma, selezionare un blocco account interno.
 - Per l'autenticazione basata sulla stampante con Rilascio stampe senza server Lexmark Print Management (LPM) su un'impostazione Active Directory, selezionare un blocco LDAP+GSSAPI.
 - Per l'autenticazione tramite LDAP, selezionare un blocco LDAP.
- 4 Fare clic su **Salva modello**.

Nota: Per modificare un modello di protezione esistente, fare clic sul modello di protezione, quindi aggiungere o modificare l'autorizzazione per il modello.

Configurazione dei controlli di accesso

Nota: Quando si utilizza la funzione **Accesso amministratore**, accertarsi di aver configurato il modello di protezione per gli account interni. Per ulteriori informazioni, vedere ["Creazione di un modello di protezione" a pagina 6](#).

- 1 Da Embedded Web Server, fare clic su **Impostazioni** o **Configurazione**.
- 2 A seconda del modello di stampante, svolgere una delle seguenti operazioni:
 - Fare clic su **Protezione** > **Impostazioni protezione** > **Controlli di accesso**.
 - Fare clic su **Protezione** > **Modifica impostazioni di protezione** > **Controlli accesso**.
- 3 Fare clic su **Applicazioni periferica** o **Soluzioni periferica**, quindi effettuare le seguenti operazioni:
 - Impostare App 1 o Soluzione 1 su un account interno o su un modello di protezione LDAP+GSSAPI o Active Directory.
 - Impostare App 2 o Solution 2 sul modello di protezione dell'applicazione.

Nota: Il modello di protezione dell'applicazione è il modello con CardAuth come impostazione di autenticazione. Per ulteriori informazioni, vedere ["Creazione di un modello di protezione" a pagina 6](#).

 - Impostare App 3 o Solution 3 su un modello di protezione LDAP.

Note:

- Se Rilascio stampe LPM è installato, impostare il controllo di accesso di Rilascio stampe sul modello di protezione dell'applicazione.

- Le stampanti che supportano Embedded Solutions Framework (eSF) versione 2.x necessitano dell'applicazione eSF Security Manager per configurare il controllo dell'accesso. Per un elenco di queste stampanti, consultare il file *Leggimi*.

4 Fare clic su **Inoltra**.

Configurazione dell'applicazione

Prima di iniziare, effettuare le seguenti operazioni:

- Disabilitare Schermata sfondo e inattiva e qualsiasi applicazione di autenticazione esistente.
- Eseguire le seguenti installazioni:
 - Programma di installazione di Autenticazione con scheda
 - Driver del lettore di schede
 - Lettore di schede
 - eSF Security Manager

Nota: Le stampanti che supportano eSF versione 2.x necessitano dell'applicazione eSF Security Manager per configurare il controllo di accesso. Per un elenco di queste stampanti, consultare il file *Leggimi*.

Accesso alla pagina di configurazione dell'applicazione

- 1 Da Embedded Web Server, fare clic su **Impostazioni** o **Configurazione**.
- 2 A seconda del modello di stampante, eseguire una delle operazioni seguenti:
 - Fare clic su **Applicazioni** > **Gestione applicazioni**.
 - Fare clic su **Soluzioni periferica** > **Soluzioni (eSF)**.
 - Fare clic su **Embedded Solutions**.
- 3 Fare clic su **Autenticazione scheda** > **Configura**.

Configurazione dell'autenticazione amministratore

Nota: Quando si utilizza la funzione **Accesso amministratore**, assicurarsi di aver configurato il modello di protezione per Accesso interni, PIN e Password. Per ulteriori informazioni, vedere ["Creazione di un modello di protezione" a pagina 6](#).

- 1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2 Nella sezione Autenticazione utente, impostare **Controllo accesso amministratore** sul metodo di accesso preferito.

Note:

- Assicurarsi di aver configurato il controllo di accesso selezionato con un modello di protezione. Per ulteriori informazioni, vedere ["Creazione di un modello di protezione" a pagina 6](#).
- Selezionando **Disabilitato**, si nasconde l'opzione **Accesso amministratore** dal pannello della stampante.

- 3 Fare clic su **Applica**.

Configurazione della schermata di accesso

La schermata di accesso può essere configurata per eseguire le seguenti operazioni:

- Consentire agli utenti di utilizzare le funzioni di copia e fax senza effettuare l'accesso.
- Consentire agli utenti di selezionare il metodo di accesso da utilizzare.
- Aggiungere uno sfondo per la schermata di accesso e personalizzare il messaggio di accesso.
- Disattivare l'avviso che si riceve quando non è presente alcun lettore di schede collegato.

1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.

2 Dalla sezione Schermata di accesso, configurare le impostazioni.

Nota: Per ulteriori informazioni su ciascuna impostazione, vedere la guida contestuale.

3 Fare clic su **Applica**.

Attivazione delle funzioni di copia o fax senza effettuare l'accesso

Se le opzioni "Consenti copia senza accesso" o "Consenti fax senza accesso" sono abilitate, effettuare le seguenti operazioni:

1 Da Embedded Web Server, fare clic su **Impostazioni** o **Configurazione**.

2 A seconda del modello di stampante, effettuare una delle seguenti operazioni:

- Fare clic su **Protezione** > **Impostazioni di protezione** > **Controlli accesso** > **Accesso alle funzioni**.
- Fare clic su **Protezione** > **Modifica impostazioni di protezione** > **Controlli di accesso**.

3 Impostare le funzioni di copia o fax su **Nessuna protezione**.

4 Fare clic su **Invia**.

Autenticazione basata sulla stampante

Utilizzare l'autenticazione basata sulla stampante quando si convalidano gli utenti tramite una stampante principale.

Configurazione dell'autenticazione utente basata sulla stampante

Prima di iniziare, accertarsi delle seguenti condizioni:

- Il controllo di accesso di App 1 o Soluzione 1 è impostato su un account interno o su un modello di protezione LDAP+GSSAPI o Active Directory.
- Il controllo di accesso di App 2 o Soluzione 2 è impostato sul modello di protezione dell'applicazione.

Nota: Per ulteriori informazioni, vedere ["Configurazione dei controlli di accesso" a pagina 6](#).

1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.

2 Dalla sezione Schermata di accesso, impostare Metodo di accesso su **Scheda o Accesso manuale**.

3 Nella sezione Autenticazione utente, effettuare le seguenti operazioni:

- Impostare Convalida Scheda su **Basata sulla stampante**.
- Impostare Controllo accesso registrazione scheda su **App 1 o Soluzione 1**.

- Impostare Controllo accesso manuale su **App 1** o **Soluzione 1**.
- Impostare Controllo accesso sessione su **App 2** o **Soluzione 2**.

Note:

- Se Controllo accesso registrazione scheda è impostato su **Nessuno**, non è possibile registrare la scheda sulla stampante.
- L'impostazione di Controllo accesso manuale su **Nessuno** richiede solo una scheda per accedere anche se Metodo di accesso è impostato su **Scheda o Accesso manuale**.
- Per ulteriori informazioni su ciascuna impostazione, vedere la guida contestuale.

4 Fare clic su **Applica**.

Impostazione del ruolo della stampante

Nota: Una stampante client richiede una stampante principale e una stampante di backup.

1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.

2 Nella sezione Convalida scheda basata sulla stampante, selezionare un ruolo per la stampante.

- **Principale:** la stampante gestisce l'elenco degli utenti registrati.
- **Backup:** se la stampante principale non è in linea, la stampante di backup assume il ruolo di stampante principale finché quella principale non torna in linea.
- **Client:** nella stampante non sono memorizzate le informazioni degli utenti. Per convalidare le credenziali dell'utente è richiesta una stampante principale o di backup.

Note:

- Se si dispone di una sola stampante, impostarla come principale.
- Se si dispone di due stampanti, impostarne una come principale e l'altra come backup.
- In caso di tre o più stampanti, impostarne una come principale, un'altra come backup e le restanti come client.

3 Digitare il nome host o l'indirizzo IP della stampante principale e di backup.

Note:

- Durante l'impostazione di una stampante di backup, è obbligatorio indicare il nome host o l'indirizzo IP della stampante principale.
- Durante l'impostazione delle stampanti client, è obbligatorio indicare il nome host o l'indirizzo IP delle stampanti principale e di backup.
- Prima di assegnare una stampante client a una nuova stampante principale, eliminare la stampante client da quella precedente.

4 Fare clic su **Applica**.

Autenticazione servizio Web

Utilizzare l'autenticazione del servizio Web quando si convalidano gli utenti tramite un server LDD.

Configurazione dell'autenticazione utente tramite il servizio Web

Prima di iniziare, accertarsi che il controllo di accesso di App 2 o Soluzione 2 sia impostato sul modello di protezione dell'applicazione. Per ulteriori informazioni, vedere ["Configurazione dei controlli di accesso" a pagina 6](#).

- 1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2 Nella sezione Schermata di accesso, impostare Metodo di accesso su **Accesso con scheda o manuale**.
- 3 Nella sezione Autenticazione utente, effettuare le seguenti operazioni:
 - Impostare Convalida scheda su **Servizio Web**.
 - Impostare Controllo accesso registrazione scheda e Controllo accesso per accesso manuale sul controllo di accesso preferito.
 - Impostare Controllo accesso sessione su **App 2 o Soluzione 2**.

Note:

- Se Controllo accesso registrazione scheda è impostato su **Nessuno**, non è possibile registrare la scheda sulla stampante.
 - L'impostazione di Controllo accesso per accesso manuale su **Nessuno** richiede solo una scheda per accedere anche se Metodo di accesso è impostato su **Accesso con scheda o manuale**.
 - Per ulteriori informazioni su ciascuna impostazione, vedere la guida contestuale.
- 4 Selezionare **Verifica certificato** per convalidare tutte le connessioni al server. Se non viene selezionata l'opzione Verifica certificato, l'autorità di certificazione (CA) non verrà convalidata.

Nota: l'impostazione Verifica certificato è applicabile solo alla convalida del servizio d'identità e del servizio Web.
 - 5 Nel menu Modalità di verifica, selezionare **catena o peer**.

Nota: il valore predefinito è catena.
 - 6 Caricare il certificato SSL del server per stabilire una connessione sicura al server.
 - 7 Nel campo Host di verifica, digitare i nomi host aggiuntivi (diversi dall'URL del server predefinito) per verificare le voci nel certificato. Utilizzare le virgole per separare più nomi host.

Nota: per impostazione predefinita, tale white list contiene solo l'URL del server. Digitare altri nomi host nel campo Host di verifica per includerli nella white list.
 - 8 Fare clic su **Applica**.

Configurazione delle impostazioni del servizio Web

- 1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2 Dalla sezione Impostazioni servizio Web, configurare le impostazioni.

Nota: Per ulteriori informazioni su ciascuna impostazione, consultare la guida contestuale.

3 Fare clic su **Applica**.

Autenticazione Servizio identità

Utilizzare Autenticazione Servizio identità durante la convalida degli utenti tramite un server Servizio identità, ad esempio il server LPM Software as a Service (SaaS).

Configurazione dell'autenticazione utente tramite Servizio identità

Prima di iniziare, accertarsi che il controllo di accesso di App 2 o Soluzione 2 sia impostato sul modello di protezione dell'applicazione. Per ulteriori informazioni, vedere ["Configurazione dei controlli di accesso" a pagina 6](#).

- 1** Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2** Nella sezione Schermata di accesso, impostare Metodo di accesso su **Accesso con scheda o manuale**.
- 3** Nella sezione Autenticazione utente, effettuare le seguenti operazioni:
 - Impostare Convalida scheda su **Servizio identità**.
 - Impostare Controllo accesso per registrazione scheda su **Servizio identità**.
 - Impostare Controllo accesso per accesso manuale su **Servizio identità**.
 - Impostare Controllo accesso sessione su **App 2** o **Soluzione 2**.

Note:

- Se Controllo accesso registrazione scheda è impostato su **Nessuno**, non è possibile registrare la scheda sulla stampante.
 - L'impostazione di Controllo accesso per accesso manuale su **Nessuno** richiede solo una scheda per accedere anche se Metodo di accesso è impostato su **Accesso con scheda o manuale**.
 - Per ulteriori informazioni su ciascuna impostazione, vedere la guida contestuale.
- 4** Selezionare **Verifica certificato** per convalidare tutte le connessioni al server. Se non viene selezionata l'opzione Verifica certificato, l'autorità di certificazione (CA) non verrà convalidata.

Nota: l'impostazione Verifica certificato è applicabile solo alla convalida del servizio d'identità e del servizio Web.

- 5** Nel menu Modalità di verifica, selezionare **catena** o **peer**.

Nota: il valore predefinito è catena.

- 6** Caricare il certificato SSL del server per stabilire una connessione sicura al server.

- 7** Nel campo Host di verifica, digitare i nomi host aggiuntivi (diversi dall'URL del server predefinito) per verificare le voci nel certificato. Utilizzare le virgole per separare più nomi host.

Nota: per impostazione predefinita, tale white list contiene solo l'URL del server. Digitare altri nomi host nel campo Host di verifica per includerli nella white list.

- 8** Fare clic su **Applica**.

Configurazione delle impostazioni di Servizio identità

- 1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2 Se necessario, nella sezione Impostazioni servizio identità, selezionare **Abilita schermata inattiva**.
Nota: Le stampanti che supportano eSF versione 2.x necessitano dell'applicazione eSF Security Manager quando l'opzione **Abilita schermata inattiva** è disabilitata. Per un elenco di queste stampanti, consultare il file *Leggimi*.
- 3 Digitare il nome host o l'indirizzo IP del provider del servizio identità.
- 4 Se necessario, digitare il nome host o l'indirizzo IP del provider del servizio badge.
- 5 Caricare il certificato SSL del server per stabilire una connessione sicura al server.
- 6 Se il fornitore del servizio di identità fornisce un ID client e un Segreto client, digitare le informazioni nei campi corrispondenti.
- 7 Impostare il criterio di accesso per l'applicazione.
 - **Continua:** consente di proseguire utilizzando la stampante anche se la connessione al server Servizio identità non viene eseguita.
 - **Errore:** consente di tornare alla schermata di accesso se la connessione al server Servizio identità non viene eseguita.
- 8 Per consentire agli utenti di accedere alla stampante tramite un account di servizio separato, selezionare **Usa account di servizio**, quindi immettere le credenziali dell'account di servizio.
- 9 Fare clic su **Applica**.

autenticazione tramite PIN

Configurazione dell'autenticazione utente tramite PIN

Prima di iniziare, accertarsi che il controllo di accesso di App 2 o Soluzione 2 sia impostato sul modello di protezione dell'applicazione. Per ulteriori informazioni, vedere "[Configurazione dei controlli di accesso](#)" a [pagina 6](#).

- 1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2 Dalla sezione Schermata di accesso, impostare Metodo di accesso su un'opzione che supporti l'autenticazione tramite PIN.
- 3 Nella sezione Autenticazione utente, effettuare le seguenti operazioni:
 - Impostare Convalida scheda sul metodo di autenticazione preferito.
 - Impostare Controllo accesso registrazione scheda sul controllo di accesso preferito.
 - Impostare Controllo accesso PIN su **App 1** o **Soluzione 1**.
 - Impostare Controllo accesso manuale sul controllo di accesso preferito.
 - Impostare Controllo accesso sessione su **App 2** o **Soluzione 2**.

Note:

- Se Controllo accesso PIN è impostato su **Nessuno**, non è possibile registrare il PIN sulla stampante.

- Per ulteriori informazioni su ciascuna impostazione, vedere la guida contestuale.

4 Fare clic su **Applica**.

Configurazione delle impostazioni PIN

- 1** Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2** Nella sezione Impostazioni PIN del menu Credenziali necessarie, selezionare un metodo di accesso.
 - ID utente e PIN: richiede un nome utente e un PIN per l'autenticazione.
 - Solo PIN: richiede un PIN per l'autenticazione.
- 3** Digitare l'indirizzo del server Web, quindi selezionare la lunghezza minima del PIN.
- 4** Digitare i messaggi di errore PIN non valido.
- 5** Fare clic su **Applica**.

Autenticazione tramite LDAP

Utilizzare l'autenticazione tramite LDAP quando si convalidano gli utenti tramite un server LDAP.

Configurazione dell'autenticazione utente tramite LDAP

Prima di iniziare, accertarsi delle seguenti condizioni:

- Il controllo di accesso di App 2 o Soluzione 2 è impostato sul modello di protezione dell'applicazione.
- Il controllo accesso di App 3 o Soluzione 3 è impostato su un modello di protezione LDAP.

Nota: Per ulteriori informazioni, vedere ["Configurazione dei controlli di accesso" a pagina 6](#).

- 1** Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2** Dalla sezione Schermata di accesso, impostare Metodo di accesso su **Scheda o Accesso manuale**.
- 3** Nella sezione Autenticazione utente, effettuare le seguenti operazioni:
 - Impostare Convalida scheda su **LDAP**.
 - Impostare Controllo accesso registrazione scheda su **App 3 o Soluzione 3**.
 - Impostare Controllo accesso manuale su **App 3 o Soluzione 3**.
 - Impostare Controllo accesso sessione su **App 2 o Soluzione 2**.

Note:

- Se Controllo accesso registrazione scheda è impostato su **Nessuno**, non è possibile registrare la scheda sulla stampante.
- L'impostazione di Controllo accesso manuale su **Nessuno** richiede solo una scheda per accedere anche se Metodo di accesso è impostato su **Scheda o Accesso manuale**.
- Per ulteriori informazioni su ciascuna impostazione, vedere la guida contestuale.

4 Fare clic su **Applica**.

Configurazione delle impostazioni LDAP

- 1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2 Dalla sezione Impostazioni LDAP, configurare le impostazioni.

Note:

- se è selezionato **Utilizza Rubrica**, l'applicazione utilizza le impostazioni LDAP che sono già configurate negli account di rete della stampante.
- Per ulteriori informazioni su ciascuna impostazione, vedere la guida contestuale.

- 3 Fare clic su **Applica**.

Impostazione delle preferenze dell'applicazione

- 1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2 Provare una o più delle soluzioni seguenti:
 - Per personalizzare la schermata iniziale della stampante, configurare le relative impostazioni.
 - Per visualizzare i messaggi di registrazione, dalla sezione Impostazioni avanzate, selezionare **Mostra messaggio di registrazione introduttivo** e **Mostra messaggio di registrazione completata**.
 - Per ascoltare un *segnale acustico* dopo aver effettuato l'accesso, nella sezione Impostazioni avanzate, selezionare **Abilita segnale acustico dopo l'accesso**, quindi regolare la frequenza del segnale acustico.
 - Per utilizzare un profilo dopo aver effettuato l'accesso, nella sezione Impostazioni avanzate, nel campo Profilo di accesso, digitare un nome di profilo.

Nota: Per ulteriori informazioni su ciascuna impostazione, vedere la guida contestuale.

- 3 Fare clic su **Applica**.

Visualizzazione dei profili disponibili

- 1 Da Embedded Web Server, fare clic su **Impostazioni** o **Configurazione**.
- 2 Fare clic su **Gestisci scelte rapide** > **Gestisci scelte rapide profilo**.

Visualizzazione delle aree di autenticazione per gli account utente

La funzione Utilizza area di autenticazione selezionata è applicabile solo se i metodi di accesso per la registrazione della scheda e per l'accesso manuale sono Kerberos, Active Directory o LDAP+GSSAPI. Questa funzione è inoltre applicabile solo se l'opzione Convalida scheda è impostata su Servizio Web o Basata su stampante.

Per la registrazione della scheda, se questa funzione è attivata, l'ID del badge registrato è nel formato nomeutente@areadiautenticazione.

Per l'accesso manuale, se questa funzione è attivata, il nome dell'utente visualizzato nel pannello di controllo della stampante è nel formato nomeutente@areadiautenticazione.

Queste impostazioni non si applicano ad Accesso con PIN e Registrazione con PIN.

Per attivare questa funzione, effettuare le seguenti operazioni:

- 1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2 Nella sezione Impostazioni avanzate, selezionare **Utilizza area di autenticazione selezionata**.
- 3 Fare clic su **Applica**.

Esportazione o importazione di un file di configurazione

- 1 Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2 Importare o esportare il file di configurazione.

Note:

- Se viene visualizzato il messaggio di errore **Memoria esaurita di JVM**, ripetere l'esportazione finché il file di configurazione non viene salvato.
- Se si verifica una condizione di timeout e viene visualizzata una schermata vuota, aggiornare il browser Web, quindi fare clic su **Applica**.

Gestione dell'applicazione

Nota: La pagina di stato dell'applicazione è disponibile solo quando si utilizza l'autenticazione basata sulla stampante.

Accesso alla pagina di stato dell'applicazione

Utilizzare la pagina di stato per monitorare l'attività della stampante.

1 Da Embedded Web Server, fare clic su **Applicazioni > Autenticazione scheda**.

2 Prendere nota delle seguenti informazioni:

- **Stato:** mostra lo stato di attività della stampante.
 - **Non configurata:** la stampante non è stata configurata.
 - **Non in linea:** la stampante non svolge attività né invia comunicazioni.
 - **In linea:** la stampante è attiva.
- **Tempo di attività:** indica da quanto tempo l'applicazione è in esecuzione.
- **(questa stampante):** la stampante corrente.
- **Ultima attività:** l'ultima attività della stampante principale.
- **Numero di utenti:** il numero totale di utenti registrati.
- **Stato registrazione:** indica se la stampante è in linea o non in linea.
- **Ultima sincronizzazione con la stampante principale:** l'ultima volta in cui la stampante di backup si è sincronizzata con la stampante principale.
- **Ultimo contatto con la stampante principale:** l'ultima volta in cui la stampante di backup ha comunicato con la stampante principale.
- **Ultima sincronizzazione come stampante principale:** l'ultima volta in cui la stampante di backup ha svolto il ruolo di stampante principale.
- **Ultima attività come stampante principale:** l'ultima attività della stampante di backup con il ruolo di stampante principale.
- **Durata come stampante principale:** indica per quanto tempo la stampante di backup ha svolto il ruolo di stampante principale.
- **Attualmente servita da:** la stampante client che è stata recentemente in contatto con la stampante principale o di backup.
- **Ultima attività con la stampante di backup:** l'ultima volta in cui la stampante client è stata in contatto con la stampante di backup.

Gestione degli account utente e delle stampanti client

Nota: questa funzione viene visualizzata solo quando una stampante funziona come stampante principale.

1 Da Embedded Web Server, accedere alla pagina di stato dell'applicazione.

2 Effettuare una delle seguenti operazioni:

Eliminazione degli account utente

- a Nella sezione Principale, fare clic su **Elimina utenti**.
- b Digitare uno o più ID utente, quindi eliminarli.

Aggiungere stampanti client

- a Nella sezione Client, fare clic su **Aggiungi client**.
- b Digitare uno o più indirizzi IP della stampante, quindi aggiungerli.

Eliminare stampanti client

Nota: Non è possibile eliminare le stampanti client quando la stampante principale è offline o quando l'applicazione è stata disinstallata.

- a Selezionare una o più stampanti client nella sezione Client.
- b Fare clic su **Elimina client**.

Riassegnazione dei ruoli per la stampante

- 1 Configurare una nuova stampante principale.
 - a Da Embedded Web Server della nuova stampante principale, accedere alla pagina di configurazione dell'applicazione.
 - b Dalla sezione Convalida scheda basata sulla stampante, impostare il ruolo su **Principale**.
 - c Digitare il nome host o l'indirizzo IP della stampante di backup.
 - d Fare clic su **Applica**.
- 2 Assegnare la stampante di backup alla nuova stampante principale.
 - a Da Embedded Web Server della stampante di backup, accedere alla pagina di configurazione dell'applicazione.
 - b Nella sezione Convalida scheda basata sulla stampante, digitare il nome host o l'indirizzo IP della nuova stampante principale.
 - c Fare clic su **Applica**.
- 3 Eliminare la stampante client dalla stampante principale corrente.
 - a Da Embedded Web Server della nuova stampante principale corrente, accedere alla pagina di stato dell'applicazione.
 - b Nella sezione Client, eliminare la stampante client.
- 4 Riassegnare la stampante client alla nuova stampante principale. Effettuare una delle seguenti operazioni:

Uso della pagina di configurazione dell'applicazione

- a Da Embedded Web Server della stampante client, accedere alla pagina di configurazione dell'applicazione.
- b Dalla sezione Convalida scheda basata sulla stampante, impostare il ruolo su **Client**.
- c Digitare il nome host o l'indirizzo IP della nuova stampante principale.

Nota: Accertarsi che il nome host o l'indirizzo IP della stampante di backup sia corretto.
- d Fare clic su **Applica**.

Uso della pagina di stato della stampante principale

- a** Da Embedded Web Server della nuova stampante principale, accedere alla pagina di stato dell'applicazione.
- b** Nella sezione Client, fare clic su **Aggiungi client**.
- c** Digitare l'indirizzo IP della stampante client, quindi aggiungerla.

Uso dell'applicazione

Registrazione degli utenti

- 1 Mettere a contatto la scheda con il lettore di schede.
- 2 Nel pannello di controllo della stampante, immettere le credenziali.

Nota: Se si utilizza Kerberos, Active Directory o LDAP+GSSAPI per la registrazione della scheda, selezionare un'area di autenticazione.

- 3 Seguire le istruzioni visualizzate sul display.

Registrazione di un PIN

Prima di iniziare, accertarsi che il metodo di accesso sia configurato per supportare l'autenticazione tramite PIN.

- 1 Dal pannello di controllo della stampante, toccare **Accesso con PIN**.
- 2 Seguire le istruzioni visualizzate sul display.

Accesso manuale alla stampante

- 1 Dal pannello di controllo della stampante, toccare una delle seguenti opzioni:
 - **Accesso PIN**
 - **Accesso manuale**
 - **Accesso amministratore**

Nota: Quando si seleziona **Accesso amministratore**, il recupero delle informazioni degli altri utenti dal server LDAP non è applicabile.

- 2 Immettere le credenziali di accesso.

Nota: Se si utilizza Kerberos, Active Directory® o LDAP+GSSAPI per l'accesso manuale, selezionare un'area di autenticazione.

- 3 Seguire le istruzioni visualizzate sul display.

Risoluzione dei problemi

Errore dell'applicazione

Provare una o più delle seguenti soluzioni:

Controllare il registro di sistema

- 1 Da Embedded Web Server, fare clic su **Impostazioni** o **Configurazione**.
- 2 A seconda del modello di stampante, eseguire una delle operazioni seguenti:
 - Fare clic su **Applicazioni** > **Gestione applicazioni**.
 - Fare clic su **Soluzioni periferica** > **Soluzioni (eSF)**.
 - Fare clic su **Embedded Solutions**.
- 3 Fare clic su **Sistema** > **Registro**.
- 4 Selezionare e inviare i filtri appropriati.
- 5 Analizzare il registro, quindi risolvere il problema.

Contattare il rappresentante Lexmark

Non è possibile eseguire l'applicazione con la versione aggiornata di Rilascio stampe SaaS

Provare una o più delle seguenti soluzioni:

Accertarsi che l'opzione Rilascio stampe sia configurata correttamente

Se è stato eseguito l'aggiornamento dell'applicazione Gestione stampe SaaS a Rilascio stampe v2.0 o versione successiva, assicurarsi di disabilitare Schermata sfondo e inattiva. Assegnare il controllo di accesso di Autenticazione scheda a Rilascio stampe e accertarsi che l'opzione Rilascio stampe sia configurata correttamente. Per ulteriori informazioni, consultare la *Guida dell'amministratore di Rilascio stampe*.

Contattare il rappresentante Lexmark

Errore di autenticazione

Provare una o più delle seguenti soluzioni:

Aumentare il timeout della stampante

Se si utilizza il servizio di identità come metodo di convalida della scheda, può essere necessario più tempo perché la stampante comunichi con il provider di servizi identità.

- 1 Da Embedded Web Server, fare clic su **Impostazioni** o **Configurazione**.
- 2 Fare clic su **Impostazioni generali** > **Timeout**.
- 3 Aumentare il valore di timeout dello schermo e la modalità di risparmio energetico.
- 4 Fare clic su **Inoltra**.

Verificare che la stampante sia collegata alla rete

Per ulteriori informazioni, consultare la *Guida per l'utente* della stampante.

Assicurarsi che il server di sicurezza sia in linea e non occupato

Per ulteriori informazioni, contattare l'amministratore di sistema.

L'utente è bloccato

L'utente potrebbe aver raggiunto il numero consentito di accessi non riusciti.

Aumento del periodo di blocco e del numero consentito di accessi non riusciti

- 1 A seconda del modello della stampante, in Embedded Web Server, effettuare una delle seguenti operazioni:
 - Fare clic su **Impostazioni** > **Protezione** > **Impostazioni di protezione varie** > **Restrizioni di accesso**.
 - Fare clic su **Configurazione** > **Protezione**.
- 2 Aumentare il periodo di blocco e il numero consentito di accessi non riusciti o l'intervallo di tempo per la disconnessione automatica.
- 3 Fare clic su **Inoltra**.

Impossibile registrare una stampante client

Provare una o più delle seguenti soluzioni:

Verificare che la stampante principale o di backup sia in linea

Per ulteriori informazioni, vedere ["Accesso alla pagina di stato dell'applicazione" a pagina 17](#).

Verificare che la stampante principale e quella di backup siano configurate correttamente

Per ulteriori informazioni, vedere "[Configurazione dell'autenticazione utente basata sulla stampante](#)" a [pagina 9](#).

Accertarsi di non registrare più di 23 stampanti client

Per ulteriori informazioni, vedere "[Gestione degli account utente e delle stampanti client](#)" a [pagina 17](#).

Contattare il rappresentante Lexmark

Impossibile convalidare la scheda

Provare una o più delle seguenti soluzioni:

Impostazione del metodo di accesso su Accesso con scheda e manuale

- 1** Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2** Dalla sezione Schermata di accesso, impostare Metodo di accesso su **Scheda o Accesso manuale**.
- 3** Fare clic su **Applica**.

Contattare il rappresentante Lexmark

Impossibile trovare informazioni sull'area di autenticazione

Provare una o più delle seguenti soluzioni:

Alcuni metodi di accesso per l'accesso manuale o la registrazione della scheda, ad esempio gli account locali o LDAP, non richiedono la selezione dell'area di autenticazione. I metodi di accesso che richiedono la selezione dell'area di autenticazione sono Kerberos, Active Directory e LDAP+GSSAPI.

Disattivare la selezione dell'area di autenticazione

- 1** Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2** Nella sezione Impostazioni avanzate, deselezionare **Utilizza area di autenticazione selezionata**.
- 3** Fare clic su **Applica**.

Modificare il metodo di accesso

- 1** Da Embedded Web Server, accedere alla pagina di configurazione dell'applicazione.
- 2** Nella sezione Autenticazione utente, impostare Controllo accesso registrazione scheda e Controllo accesso manuale su **App 1 o Soluzione 1**.
- 3** Fare clic su **Applica**.

Contattare il rappresentante Lexmark

Impossibile connettersi al server LDAP

Provare una o più delle seguenti soluzioni:

Verificare che le impostazioni LDAP siano configurate correttamente

Per ulteriori informazioni, vedere ["Configurazione delle impostazioni LDAP" a pagina 15](#).

Contattare il rappresentante Lexmark

Domande frequenti

Perché non è possibile aggiungere o eliminare una stampante client quando una stampante di backup funziona come stampante principale?

Una stampante client può essere eliminata o aggiunta solo quando la stampante principale è in linea.

È possibile rimuovere una stampante client e riassegnarla alla sua nuova stampante principale anche se la stampante principale è offline?

Sì. Effettuare le seguenti operazioni:

- 1 Da Embedded Web Server della stampante client, installare l'applicazione.
- 2 Impostare il ruolo come stampante client e configurarla assegnandola alle nuove stampanti principali e di backup. Per ulteriori informazioni, vedere ["Impostazione del ruolo della stampante" a pagina 10](#).

Che cosa succede se l'applicazione della stampante viene accidentalmente disinstallata?

- 1 Da Embedded Web Server, installare l'applicazione.
- 2 Impostare un ruolo per la stampante. Per ulteriori informazioni, vedere ["Impostazione del ruolo della stampante" a pagina 10](#).

Nota: Assicurarsi di impostare la stampante principale, quindi la stampante di backup, infine consecutivamente le stampanti client.

- 3 Configurare la stampante in base al ruolo.

Note:

- Se l'applicazione viene reinstallata su una stampante principale, assegnarla alla sua stampante di backup.
- Se l'applicazione viene reinstallata su una stampante di backup, assegnarla alla sua stampante principale.
- Se l'applicazione viene reinstallata su una stampante client, assegnarla alla sua stampante principale e di backup.
- Per ulteriori informazioni, vedere ["Riassegnazione dei ruoli per la stampante" a pagina 18](#).

Perché non viene visualizzato il pulsante Copia o Fax sulla schermata di blocco anche se è stata attivata la funzione di copia o fax senza effettuare l'accesso?

Impostare il controllo di accesso delle funzioni di copia o fax su **Nessuna protezione**. Per ulteriori informazioni, vedere "[Configurazione della schermata di accesso](#)" a pagina 9.

Cosa accade se si hanno gli stessi controlli di accesso per Controllo accesso manuale e Controllo accesso sessione?

Per accedere alle funzioni della stampante dalla schermata iniziale, è necessario immettere le credenziali quando si accede manualmente.

È possibile avere diversi controlli di accesso per Controllo accesso manuale e Convalida scheda?

Sì, ad eccezione del caso in cui si utilizzi l'autenticazione tramite Servizio identità. In tal caso, impostare Controllo accesso manuale e Convalida scheda su **Servizio identità**.

Perché la funzione Accesso amministratore non funziona con gli account di rete?

La funzione **Accesso amministratore** è applicabile solo a modelli di protezione per Account interni, PIN e Password.

Avvertenze

Nota sull'edizione

Dicembre 2020

Le informazioni incluse nel seguente paragrafo non si applicano a tutti quei Paesi in cui tali disposizioni non risultano conformi alle leggi locali: LA PRESENTE DOCUMENTAZIONE VIENE FORNITA DA LEXMARK INTERNATIONAL, INC. COSÌ COM'È, SENZA ALCUNA GARANZIA IMPLICITA O ESPLICITA, INCLUSE LE GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ O IDONEITÀ A SCOPI SPECIFICI. In alcuni paesi non è consentita la rinuncia di responsabilità esplicita o implicita in determinate transazioni, pertanto la presente dichiarazione potrebbe non essere valida.

La presente pubblicazione potrebbe includere inesattezze di carattere tecnico o errori tipografici. Le presenti informazioni sono soggette a modifiche periodiche che vengono incluse nelle edizioni successive. Miglioramenti o modifiche ai prodotti o ai programmi descritti nel presente documento possono essere apportati in qualsiasi momento.

I riferimenti a prodotti, programmi o servizi contenuti in questa pubblicazione non sottintendono alcuna intenzione del produttore di renderli disponibili in tutti i Paesi in cui opera. Qualsiasi riferimento a un prodotto, programma o servizio non implica alcun uso esclusivo di tale prodotto, programma o servizio. Ogni prodotto, programma o servizio funzionalmente equivalente che non violi diritti di proprietà intellettuale può essere utilizzato in sostituzione. La valutazione e la verifica del funzionamento insieme ad altri prodotti, programmi o servizi, tranne quelli espressamente progettati dal produttore, sono di responsabilità dell'utente.

Per il supporto tecnico Lexmark, visitare il sito Web <http://support.lexmark.com>.

Per informazioni sui criteri relativi alla privacy di Lexmark che regolano l'uso di questo prodotto, visitare il sito Web www.lexmark.com/privacy.

Per informazioni sui materiali di consumo e sui download, visitare il sito Web www.lexmark.com.

© 2014 Lexmark International, Inc.

Tutti i diritti riservati.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Marchi

Lexmark e il logo Lexmark sono marchi di Lexmark International, Inc., registrati negli Stati Uniti e/o in altri Paesi.

Gli altri marchi appartengono ai rispettivi proprietari.

Indice

A

abilitazione di un segnale
acustico dopo aver effettuato
l'accesso 15
accesso
 manuale 20
 pagina di stato 17
 PIN 20
accesso a Embedded Web
Server 5
accesso alla pagina di
configurazione 8
accesso manuale 20
accesso manuale alla
stampante 20
accesso tramite PIN 20
account utente
 eliminazione 17
account utente interni
 aggiunta 5
 raggruppamento 5
aggiunta
 stampanti client 17
 utenti 20
aggiunta di un account utente
interno 5
assegnazione della stampante di
backup 18
autenticazione amministratore
 configurazione 8
autenticazione utente basata
sulla stampante
 configurazione 9
autenticazione utente tramite
LDAP
 configurazione 14
autenticazione utente tramite
PIN
 configurazione 13
autenticazione utente tramite
Servizio identità
 configurazione 12
autenticazione utente tramite
servizio Web
 configurazione 11

C

configurazione
 metodo di accesso 9
 schermata di accesso 9
configurazione dei controlli di
accesso 6
configurazione
dell'autenticazione
amministratore 8
configurazione
dell'autenticazione utente basata
sulla stampante 9
configurazione
dell'autenticazione utente tramite
il servizio Web 11
configurazione
dell'autenticazione utente tramite
LDAP 14
configurazione
dell'autenticazione utente tramite
PIN 13
configurazione
dell'autenticazione utente tramite
Servizio identità 12
configurazione delle aree di
autenticazione
 metodi di accesso 15
configurazione delle impostazioni
del servizio Web 11
configurazione delle impostazioni
di Servizio identità 13
configurazione delle impostazioni
LDAP 15
configurazione delle impostazioni
PIN 14
configurazione di una nuova
stampante principale 18
controlli accesso
 configurazione 6
creazione di un modello di
protezione 6

D

domande frequenti 25

E

eliminazione
 account utente 17
 stampanti client 17
Embedded Web Server
 accesso 5
errore dell'applicazione 21
errore di autenticazione 22
esportazione di un file di
configurazione 16

F

file di configurazione
 esportazione o importazione 16

G

gruppi di impostazioni per un
account utente interno 5

I

importazione di un file di
configurazione 16
impossibile connettersi al server
LDAP 24
impossibile convalidare la
scheda 23
impossibile registrare una
stampante client 22
impossibile trovare informazioni
sull'area di autenticazione 23
impostazione
 stampanti 10
impostazione delle preferenze
dell'applicazione 15
Impostazioni LDAP
 configurazione 15
Impostazioni PIN
 configurazione 14
Impostazioni Servizio identità
 configurazione 13
impostazioni servizio Web
 configurazione 11

L

l'utente è bloccato 22

M

- messaggi di registrazione
 - impostazione 15
- metodo di accesso
 - configurazione 9
- migrazione
 - stampanti client 18
- modello di protezione
 - creazione 6

N

- nuova stampante principale
 - configurazione 18

P

- pagina di configurazione per l'applicazione
 - accesso 8
- pagina di stato
 - accesso 17
- panoramica 4
- PIN
 - registrazione 20
- preferenze dell'applicazione
 - impostazione 15
- profilo di accesso
 - utilizzo 15

R

- registrazione di un PIN 20
- registrazione utenti 20
- riassegnazione dei ruoli stampante 18
- risoluzione dei problemi
 - errore dell'applicazione 21
 - errore di autenticazione 22
 - impossibile connettersi al server LDAP 24
 - impossibile convalidare la scheda 23
 - impossibile registrare una stampante client 22
 - impossibile trovare informazioni sull'area di autenticazione 23
 - l'utente è bloccato 22
- ruoli stampante
 - riassegnazione 18

S

- schermata di accesso
 - configurazione 9
- stampante di backup
 - assegnazione 18
 - impostazione 10
- stampante principale
 - impostazione 10
- stampanti
 - impostazione 10
- stampanti client
 - aggiunta 17
 - eliminazione 17
 - impostazione 10
 - migrazione 18

U

- uso della funzione di copia senza effettuare l'accesso 9
- uso della funzione di fax senza effettuare l'accesso 9
- uso di un profilo di accesso 15
- utenti
 - aggiunta 20
 - registrazione 20

V

- visualizzazione delle aree di autenticazione per gli account utente 15