Client di autenticazione con smart card

Versione 2.1

Guida dell'amministratore

Agosto 2017 **www.lexmark.com**

Sommario

Cronologia delle modifiche

Agosto 2017

- Aggiunte istruzioni sulla modifica del metodo di accesso
- Aggiunto il supporto per portoghese brasiliano, finlandese, francese, tedesco, italiano, cinese semplificato e spagnolo.

Gennaio 2016

- Rilascio del documento iniziale per i prodotti multifunzione con display touch simile a un tablet.

Panoramica

Utilizzare l'applicazione per proteggere l'accesso alle stampanti richiedendo agli utenti di accedere utilizzando una smart card o un nome utente e una password. È possibile proteggere l'accesso alla schermata iniziale della stampante o a singole applicazioni e funzioni.

L'applicazione fornisce inoltre opzioni di autenticazione Kerberos e un ticket Kerberos che può essere utilizzato per proteggere altre applicazioni.

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

Elenco di controllo per la conformità alla distribuzione

Accertarsi che:

- ☐ Nella stampante siano installati almeno 512 MB di RAM
- ☐ Nella stampante siano installati un lettore di smart card e il relativo driver.

Sia disponibile quanto segue per configurare l'applicazione:

- ☐ Certificato dell'Autorità di certificazione (file .cer)
- ☐ Account LDAP (Lightweight Directory Access Protocol) e Active Directory®

  _____
- ☐ Area di autenticazione Kerberos, dominio e controller di dominio

  _____
- ☐ File Kerberos (per più domini)

Configurazione delle impostazioni della stampante

È necessario disporre dei diritti di amministrazione per configurare le impostazioni della stampante.

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.
   - Dalla schermata iniziale della stampante, toccare **Impostazioni** > **Rete/Porte** > **Panoramica sulla rete**.
2. Aprire un browser web e immettere l'indirizzo IP della stampante.

Impostazione del timeout dello schermo

Per impedire l'accesso non autorizzato, è possibile limitare la quantità di tempo in cui un utente può rimanere connesso alla stampante senza eseguire alcuna attività.

1. In Embedded Web Server, fare clic su **Impostazioni** > **Periferica** > **Preferenze**.
2. Nel campo Timeout schermo, specificare l'intervallo di tempo prima che lo schermo diventi inattivo e che l'utente venga disconnesso. Si consiglia di impostare il valore su 30 secondi.
3. Fare clic su **Salva**.

Installazione manuale di certificati

Nota: Per scaricare il certificato CA automaticamente, vedere "Installazione automatica di certificati" a pagina 7.

Prima di configurare le impostazioni Kerberos o del controller di dominio, installare il certificato CA utilizzato per la convalida del controller di dominio. Se si desidera utilizzare la convalida della catena per il certificato del controller di dominio, installare l'intera catena di certificati. Ogni certificato deve trovarsi in un file PEM (.cer) separato.

1. In Embedded Web Server, fare clic su **Impostazioni** > **Protezione** > **Gestione certificati**.
2. Nella sezione Gestisci certificati CA, fare clic su **Carica CA**, quindi selezionare il file PEM (.cer).

   Certificato di esempio:

   ```
   -----BEGIN CERTIFICATE-----
   MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBtlr4gHG85zANBgkqhkiG9w0BAQUFADBs
   …
   l3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
   -----END CERTIFICATE-----
   ```

3. Fare clic su **Salva**.

Installazione automatica di certificati

1. In Embedded Web Server, fare clic su **Impostazioni** > **Protezione** > **Gestione certificati** > **Configura aggiorn. aut. certif**.
2. Se viene richiesta l'aggiunta a un dominio Active Directory, fare clic su **Aggiungi al dominio**, quindi immettere le informazioni sul dominio.

   Nota: Assicurarsi che il dominio Active Directory corrisponda all'area autenticazione Kerberos o al dominio utilizzato nelle impostazioni della smart card. Per ulteriori informazioni, vedere "Configurazione delle impostazioni della smart card" a pagina 11.
3. Selezionare **Abilita aggiornamento automatico**.

   Nota: Se si desidera installare il certificato CA senza attendere il tempo di esecuzione pianificato, selezionare **Trasporta adesso**.
4. Fare clic su **Salva**.

Configurazione delle impostazioni TCP/IP

1. In Embedded Web Server, fare clic su **Impostazioni** > **Rete/Porte** > **TCP/IP**.
2. Effettuare una delle seguenti operazioni:
   - Se si utilizza un indirizzo IP statico, immettere l'indirizzo del server DNS. Se è disponibile un server DNS di backup, immettere l'indirizzo di tale server.
   - Se la stampante si trova in un dominio diverso, immettere gli altri domini nel campo Ordine ricerca dominio. Utilizzare le virgole per separare più domini.

   Nota: Utilizzare il nome di dominio assegnato alle workstation degli utenti.
3. Fare clic su **Salva**.

Impostazione di data e ora

Quando si utilizza l'autenticazione Kerberos, accertarsi che la differenza tra l'ora della stampante e l'ora del controller di domino non sia superiore a cinque minuti. È possibile aggiornare manualmente le impostazioni di data e ora o utilizzare il protocollo NTP (Network Time Protocol) per sincronizzare automaticamente l'ora della stampante con quella del controller di dominio.

1. In Embedded Web Server, fare clic su **Impostazioni** > **Periferica** > **Preferenze** > **Data e ora**.

Configurazione manuale

Nota: La configurazione manuale della data e dell'ora disabilita il protocollo NTP.

a. Nella sezione di configurazione, nel campo Imposta data e ora manualmente, immettere la data e l'ora appropriate.

b. Selezionare il formato della data, dell'ora e il fuso orario.

   Nota: Se si seleziona **(UTC+utente) Personalizzato**, specificare i valori di scarto per l'ora UTC (GMT) e l'ora legale.

Configurazione di NTP

a Nella sezione Network Time Protocol, selezionare **Abilita NTP**, quindi digitare l'indirizzo IP o il nome host del server NTP.

b Se il server NTP richiede l'autenticazione, nel menu Attiva autenticazione, selezionare **Tasto MD5**.

c A seconda del modello di stampante, immettere l'ID della chiave e la password o selezionare il file contenente le credenziali di autenticazione NTP.

2 Fare clic su **Salva**.

Protezione dell'accesso alla stampante

Protezione dell'accesso alla schermata iniziale

Prima di accedere alla schermata iniziale della stampante, gli utenti devono autenticarsi.

Nota: Prima di iniziare, verificare che l'applicazione Personalizzazione schermo sia attivata sulla stampante. Per ulteriori informazioni, consultare la *Guida per l'amministratore per Personalizzazione schermo*.

1 In Embedded Web Server, fare clic su **Impostazioni** > **Protezione** > **Metodi di accesso**.

2 Dalla sezione Pubblica, fare clic su **Gestisci autorizzazioni**.

3 Espandere **App**, deselezionare **Presentazione**, **Modifica sfondo** e **Screen saver**, quindi fare clic su **Salva**.

4 Nella sezione Metodi di accesso aggiuntivi, fare clic su **Gestisci autorizzazioni** accanto a Smart card.

5 Selezionare un gruppo di cui si desidera gestire le autorizzazioni.

Nota: Il gruppo Tutti gli utenti viene creato per impostazione predefinita. Quando si specificano gruppi di Active Directory esistenti nel campo Elenco autorizzazione gruppi, vengono visualizzati più nomi di gruppi. Per ulteriori informazioni, vedere "Configurazione delle impostazioni avanzate" a pagina 12.

6 Espandere **Applicazioni**, quindi selezionare **Presentazione**, **Modifica sfondo** e **Screen saver**.

7 Fare clic su **Salva**.

Protezione dell'accesso a singole applicazioni e funzioni

Prima di accedere a un'applicazione o a una funzione della stampante, gli utenti devono autenticarsi.

1 In Embedded Web Server, fare clic su **Impostazioni** > **Protezione** > **Metodi di accesso**.

2 Dalla sezione Pubblica, fare clic su **Gestisci autorizzazioni**.

3 Espandere una o più categorie, deselezionare le applicazioni o le funzioni che si desidera proteggere, quindi fare clic su **Salva**.

4 Nella sezione Metodi di accesso aggiuntivi, fare clic su **Gestisci autorizzazioni** accanto a Smart card.

5 Selezionare un gruppo di cui si desidera gestire le autorizzazioni.

Nota: Il gruppo Tutti gli utenti viene creato per impostazione predefinita. Quando si specificano gruppi di Active Directory esistenti nel campo Elenco autorizzazione gruppi, vengono visualizzati più nomi di gruppi. Per ulteriori informazioni, vedere "Configurazione delle impostazioni avanzate" a pagina 12.

6 Espandere una o più categorie, quindi selezionare le applicazioni o le funzioni alle quali si desidera che gli utenti autenticati abbiano accesso.

7 Fare clic su **Salva**.

Visualizzazione delle applicazioni o funzioni protette nella schermata Home

Per impostazione predefinita, le applicazioni o funzioni protette sono nascoste nella schermata Home della stampante.

1 Da Embedded Web Server, fare clic su **Impostazioni** > **Sicurezza** > **Varie**.

2 Nel menu Funzioni protette, selezionare **Mostra**.

3 Fare clic su **Salva**.

Configurazione dell'applicazione

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

Configurazione delle impostazioni della schermata di accesso

Utilizzare le impostazioni della schermata di accesso per configurare la modalità di accesso degli utenti alla stampante.

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

   App > **Client Autenticazione con smart card** > **Configura**

2. Nella sezione Schermata di accesso, selezionare il tipo di accesso.
3. Nel menu Modalità di convalida utente, selezionare il metodo per la convalida dei certificati utente.
   - **Active Directory**: il certificato utente sulla smart card viene convalidato utilizzando l'autenticazione Kerberos. Questa impostazione potrebbe richiedere l'esecuzione di ricerche LDAP.
   - **Active Directory con accesso guest**: gli utenti che dispongono di smart card ma che non sono presenti in Active Directory possono accedere ad alcune delle funzioni della stampante. È necessario un server OCSP (Online Certificate Status Protocol) opportunamente configurato. Se l'autenticazione di Active Directory non riesce, l'applicazione invia una query al server OCSP.
   - **Solo PIN**: gli utenti possono accedere solo alle applicazioni o alle funzioni che non richiedono l'autenticazione Kerberos.
4. Nel menu Convalida smart Card, selezionare il metodo di autenticazione degli utenti dopo aver toccato una smart card.
5. Se necessario, consentire agli utenti di modificare il metodo di accesso.
6. Fare clic su **Applica**.

Configurazione delle impostazioni di accesso manuale

Per l'accesso manuale, la stampante utilizza il dominio predefinito specificato nel file di configurazione Kerberos. Se si utilizza un dominio diverso, specificare il nome di dominio nelle impostazioni di acceso manuale.

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

   App > **Client Autenticazione con smart card** > **Configura**

2. Nella sezione Impostazioni accesso manuale, immettere uno o più domini nel campo Domini di accesso manuale.
3. Fare clic su **Applica**.

Configurazione delle impostazioni della smart card

Nota: Verificare che la connessione di rete tra la stampante e il server di autenticazione sia configurata correttamente. Per ulteriori informazioni, contattare l'amministratore di sistema.

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

   App > **Client Autenticazione con smart card** > **Configura**

2. Nella sezione Impostazione smart card, nel menu Informazioni Kerberos, selezionare una delle seguenti opzioni:
   - **Utilizza file di impostazione Kerberos dispositivo**: è necessario installare manualmente un file di configurazione Kerberos nella stampante. Attenersi alla seguente procedura:
     a. In Embedded Web Server, fare clic su **Impostazioni** > **Protezione** > **Metodi di accesso**.
     b. Nella sezione Account di rete fare clic su **Aggiungi metodo di accesso** > **Kerberos**.
     c. Nella sezione Importa file Kerberos, selezionare il file krb5.conf appropriato.
     d. Se la rete non utilizza la ricerca DNS inversa, nella sezione Impostazioni varie, selezionare **Disattiva ricerche IP inverse**.
     e. Fare clic su **Salva e verifica**.
   - **Utilizza impostazione Kerberos semplice**: viene creato automaticamente un file Kerberos nella stampante. Specificare le seguenti impostazioni:
     - **Area di autenticazione**: l'area di autenticazione deve essere immessa in caratteri maiuscoli.
     - **Controller di dominio**: utilizzare le virgole per separare più valori. I controller di dominio verranno convalidati nell'ordine elencato.
     - **Dominio**: il dominio da associare all'area di autenticazione Kerberos specificata nel campo Area di autenticazione. Utilizzare le virgole per separare più domini.

       Nota: Il dominio distingue maiuscole e minuscole.
     - **Timeout**: immettere un valore compreso tra 3 e 30 secondi.

3. Nel menu Convalida controller di dominio, selezionare il metodo di convalida del certificato del controller di dominio.

   Nota: Prima di configurare questa impostazione, assicurarsi che siano installati nella stampante i certificati appropriati. Per ulteriori informazioni, vedere "Installazione manuale di certificati" a pagina 6.
   - **Utilizza convalida certificato dispositivo**: viene utilizzato il certificato CA installato nella stampante.
   - **Utilizza convalida catena di dispositivi**: viene utilizzata l'intera catena di certificati installata nella stampante.
   - **Utilizza convalida OCSP**: viene utilizzato il server OCSP. È necessario che sia installata nella stampante l'intera catena di certificati. Nella sezione OCSP (Online Certificate Status Protocol), configurare le seguenti impostazioni:
     - **URL del risponditore**: l'indirizzo IP o il nome host del risponditore o ripetitore OCSP e numero della porta utilizzata. Utilizzare le virgole per separare più valori.
       Ad esempio, **`http://x:y`**, dove ***x*** è l'indirizzo IP o il nome host e ***y*** è il numero della porta.
     - **Certificato risponditore**: viene utilizzato il certificato X.509.
     - **Timeout risponditore**: immettere un valore compreso tra 5 e 30 secondi.
     - **Consenti stato sconosciuto**: gli utenti possono accedere anche se lo stato di uno o più certificati è sconosciuto.

4. Fare clic su **Applica**.

Configurazione delle impostazioni avanzate

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

   App > **Client Autenticazione con smart card** > **Configura**

2. Nella sezione Impostazioni avanzate, selezionare un ID della sessione.

   Nota: Alcune applicazioni, ad esempio Processi di stampa in attesa protetti ed E-mail sicura, protetta, richiedono l'immissione di un valore per l'ID utente della sessione.

3. Nel menu messaggio E-mail da indirizzo, selezionare da dove la stampante recupera l'indirizzo e-mail dell'utente.

4. Se necessario, selezionare **Attendi informazioni utente** per recuperare tutte le informazioni sull'utente prima che all'utente sia consentito accedere alla schermata iniziale o all'applicazione protetta.

   Se le seguenti impostazioni sono impostate su Ricerca LDAP, selezionare questa opzione.

   - ID utente sessione
   - E-mail da indirizzo

   Se le seguenti impostazioni non sono vuote, selezionare questa opzione.

   - Altri attributi utente
   - Elenco autorizzazione gruppi

   Nota: Se si utilizza l'accesso manuale per E-mail sicura, selezionare questa opzione per memorizzare l'indirizzo e-mail dell'utente nella sessione di accesso. Per consentire agli utenti con accesso manuale di inviare e-mail a se stessi, abilitare l'opzione "Invia copia a utente corrente" nelle impostazioni e-mail della stampante.

5. Se necessario, selezionare **Usa SSL per le informazioni utente** per recuperare le informazioni sull'utente dal controller di dominio utilizzando una connessione SSL.

6. Se necessario, nel campo Altri attributi utente, immettere gli altri attributi LDAP da aggiungere alla sessione. Utilizzare le virgole per separare più valori.

7. In Elenco autorizzazione gruppi, immettere i gruppi di Active Directory che possono accedere alle applicazioni o funzioni. Utilizzare le virgole per separare più valori.

   Nota: I gruppi devono trovarsi nel server LDAP.

8. Se il DNS non è abilitato sulla rete, caricare un file host.

   Immettere le associazioni nel file di testo nel formato ***xy***, dove ***x*** è l'indirizzo IP e ***y*** è il nome host. È possibile assegnare più nomi host a un indirizzo IP. Ad esempio, **`255.255.255.255 NomeHost1 NomeHost2 NomeHost3`**.

   Non è possibile assegnare più indirizzi IP a un nome host. Per assegnare indirizzi IP a gruppi di nomi host, immettere ogni indirizzo IP e i relativi nomi host associati in una riga separata del file di testo.

   Ad esempio:

   ```
   123.123.123.123 NomeHost1 NomeHost2
   456.456.456.456 NomeHost3
   ```

9. Fare clic su **Applica**.

Importazione o esportazione di un file di configurazione

Nota: L'importazione dei file di configurazione sovrascrive le configurazioni esistenti dell'applicazione.

1. In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:
   App > **Client Autenticazione con smart card** > **Configura**
2. Fare clic su **Importa** o **Esporta**.

Risoluzione dei problemi

Errore dell'applicazione

Provare una o più delle seguenti soluzioni:

Controllare il registro di diagnostica

1. Aprire un browser Web e digitare ***IP*/se**, dove ***IP*** è l'indirizzo IP della stampante.
2. Fare clic su **Embedded Solutions**, quindi effettuare le seguenti operazioni:
   a. Eliminare il file di registro.
   b. Impostare il livello di registrazione su **Sì**.
   c. Generare il file di registro.
3. Analizzare il registro, quindi risolvere il problema.

   Nota: Dopo aver risolto il problema, impostare il livello di registrazione su **No**.

Contattare il rappresentante Lexmark

Problemi di accesso

Impossibile rilevare il lettore di schede o la smart card

Provare una o più delle seguenti soluzioni:

Accertarsi che il lettore di schede sia collegato correttamente alla stampante

Verificare che il lettore di schede e la smart card siano compatibili

Assicurarsi che il lettore di smart card sia supportato

Per un elenco dei lettori di smart card supportati, vedere il file *Leggimi*.

Accertarsi che il driver del lettore di schede sia installato nella stampante

Contattare il rappresentante Lexmark

L'utente è bloccato

Provare una o più delle seguenti soluzioni:

Aumentare il numero consentito di accessi non riusciti e il periodo di blocco

Nota: questa soluzione è applicabile solo ad alcuni modelli di stampante.

1. In Embedded Web Server, fare clic su **Impostazioni** > **Protezione** > **Restrizioni di accesso**.
2. Aumentare il numero consentito di accessi non riusciti e il periodo di blocco.
3. Fare clic su **Salva**.

   Nota: Le nuove impostazioni diventano effettive una volta trascorso il periodo di blocco.

Reimpostare o sostituire la smart card

Impossibile convalidare il PIN

Provare una o più delle seguenti soluzioni:

Verificare che il PIN immesso sia corretto

Contattare l'amministratore del sistema

Impossibile accedere manualmente

Provare una o più delle seguenti soluzioni:

Verificare che il dominio specificato nella configurazione Kerberos sia corretta

Specificare i domini nelle impostazioni di accesso manuale

Per ulteriori informazioni, vedere "Configurazione delle impostazioni di accesso manuale" a pagina 10.

Contattare l'amministratore del sistema

L'utente viene disconnesso immediatamente dopo la connessione

Aumentare il valore di timeout dello schermo

Per ulteriori informazioni, vedere "Impostazione del timeout dello schermo" a pagina 6.

La schermata iniziale della stampante non si blocca

Provare una o più delle seguenti soluzioni:

Accertarsi che Personalizzazione schermo sia attivata

Per ulteriori informazioni, consultare la *Guida per l'amministratore per Personalizzazione schermo*.

Proteggere l'accesso alla schermata iniziale

Per ulteriori informazioni, vedere "Protezione dell'accesso alla schermata iniziale" a pagina 8.

Problemi di autenticazione

Autenticazione Kerberos non riuscita

Provare una o più delle seguenti soluzioni:

Controllare il registro di diagnostica

1. Aprire un browser Web e digitare ***IP*/se**, dove ***IP*** è l'indirizzo IP della stampante.
2. Fare clic su **Embedded Solutions**, quindi effettuare le seguenti operazioni:
   a. Eliminare il file di registro.
   b. Impostare il livello di registrazione su **Sì**.
   c. Generare il file di registro.
3. Analizzare il registro, quindi risolvere il problema.

   Nota: Dopo aver analizzato il registro, impostare il livello di registrazione su **No**.

Accertarsi che il file di configurazione sia installato nella stampante

- Se si utilizza l'impostazione Kerberos semplice per creare il file di configurazione Kerberos, effettuare le seguenti operazioni:
  1. In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:
     App > **Client Autenticazione con smart card** > **Configura**
  2. Nella sezione Impostazione Kerberos semplice, verificare che i valori relativi ad area di autenticazione, controller di dominio e timeout siano corretti.
- Se si utilizza il file di impostazione Kerberos del dispositivo, effettuare le seguenti operazioni:
  1. In Embedded Web Server, fare clic su **Impostazioni** > **Protezione** > **Metodi di accesso**.
  2. Nella sezione Account di rete, fare clic su **Kerberos** > **Visualizza file**.
  3. Se il file di configurazione Kerberos non è installato, nella sezione Importa file Kerberos, selezionare il file krb5.conf appropriato.
  4. Fare clic su **Salva e verifica**.

Verificare che il contenuto e il formato del file di configurazione siano corretti

- Se si utilizza l'impostazione Kerberos semplice, modificare i dettagli di tale impostazione.
- Se si utilizza il file di impostazione Kerberos del dispositivo, modificare e reinstallare il file.

Assicurarsi che l'area di autenticazione Kerberos sia in caratteri maiuscoli

- Se si utilizza l'impostazione Kerberos semplice, effettuare le seguenti operazioni:
  1. In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:
     App > **Client Autenticazione con smart card** > **Configura**
  2. Nella sezione Impostazione Kerberos semplice, assicurarsi che l'area di autenticazione sia corretta e che sia digitata in caratteri maiuscoli.
  3. Fare clic su **Applica**.

- Se si utilizza il file di impostazione Kerberos del dispositivo, effettuare le seguenti operazioni:
  1. In Embedded Web Server, fare clic su **Impostazioni** > **Protezione** > **Metodi di accesso**.
  2. Nella sezione Account di rete, fare clic su **Kerberos** > **Visualizza file**.
  3. Assicurarsi che le aree di autenticazione nel file di configurazione siano digitate in caratteri maiuscoli.

Specificare il dominio del sistema operativo Microsoft® Windows®

- Se si utilizza l'impostazione Kerberos semplice, effettuare le seguenti operazioni:
  1. In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:
     App > **Client Autenticazione con smart card** > **Configura**
  2. Nella sezione Impostazione Kerberos semplice, aggiungere il dominio Windows nel campo Dominio.

     Ad esempio, se il valore del campo Dominio è **`NomeDominio,.NomeDominio`** e il dominio Windows è **`x.y.z`**, modificare il valore del campo Dominio in **`NomeDominio,.NomeDominio,x.y.z`**.

     Nota: Il dominio distingue maiuscole e minuscole.
  3. Fare clic su **Applica**.
- Se si utilizza il file di impostazione Kerberos del dispositivo, aggiungere una voce nella sezione **`domain_realm`** del file. Immettere l'area di autenticazione del dominio Windows in lettere maiuscole, quindi reinstallare il file nella stampante.

Contattare il rappresentante Lexmark

Impossibile generare o leggere le informazioni del certificato dalla smart card

Provare una o più delle seguenti soluzioni:

Verificare che le informazioni del certificato sulla smart card siano corrette

Contattare il rappresentante Lexmark

Impossibile convalidare il controller di dominio

Provare una o più delle seguenti soluzioni:

Verificare che l'area di autenticazione, il controller di dominio e il dominio nel file di configurazione Kerberos siano corretti

- Se si utilizza l'impostazione Kerberos semplice, effettuare le seguenti operazioni:
  1. In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:
     App > **Client Autenticazione con smart card** > **Configura**
  2. Nella sezione Impostazione Kerberos semplice, verificare che l'area di autenticazione, il controller di dominio e il dominio siano corretti.

- Se si utilizza il file di impostazione Kerberos del dispositivo, effettuare le seguenti operazioni:
  1. In Embedded Web Server, fare clic su **Impostazioni** > **Protezione** > **Metodi di accesso**.
  2. Nella sezione Account di rete, fare clic su **Kerberos** > **Visualizza file**.
  3. Verificare che l'area di autenticazione, il controller di dominio e il dominio siano corretti.

Aumentare il valore di timeout del controller di dominio

- Se si utilizza l'impostazione Kerberos semplice, effettuare le seguenti operazioni:
  1. In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:
     App > **Client Autenticazione con smart card** > **Configura**
  2. Nella sezione Installazione Kerberos semplice, immettere un valore compreso tra 3 e 30 secondi nel campo Timeout.
  3. Fare clic su **Applica**.
- Se si utilizza il file di impostazione Kerberos del dispositivo, immettere un valore compreso tra 3 e 30 secondi. Al termine, reinstallare il file nella stampante. Per ulteriori informazioni sulla configurazione delle impostazioni della smart card, vedere "Configurazione delle impostazioni della smart card" a pagina 11.

Assicurarsi che il controller di dominio sia disponibile

Utilizzare le virgole per separare più valori. I controller di dominio verranno convalidati nell'ordine elencato.

Assicurarsi che la porta 88 non sia bloccata tra la stampante e il controller di dominio

Impossibile convalidare il certificato del controller di dominio

Provare una o più delle seguenti soluzioni:

Verificare che i certificati installati nella stampante siano corretti

Per ulteriori informazioni, vedere "Installazione manuale di certificati" a pagina 6.

Assicurarsi che il metodo di convalida del controller di dominio sia configurato correttamente

1. In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:
   App > **Client Autenticazione con smart card** > **Configura**
2. Nella sezione Impostazione smart card, nel menu Convalida controller di dominio, selezionare il metodo di convalida appropriato.
3. Fare clic su **Applica**.

Impossibile trovare l'area di autenticazione nel file di configurazione Kerberos

Aggiungere o cambiare l'area di autenticazione

- Se si utilizza l'impostazione Kerberos semplice, effettuare le seguenti operazioni:
  1. In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:
     App > **Client Autenticazione con smart card** > **Configura**
  2. Nella sezione Impostazione Kerberos semplice, nel campo Area di autenticazione, aggiungere o cambiare l'area di autenticazione. L'area di autenticazione deve essere immessa in caratteri maiuscoli.

     Nota: L'impostazione Kerberos semplice non supporta più voci di area di autenticazione Kerberos. Se sono necessarie più aree di autenticazione, installare un file di configurazione Kerberos contenente le aree di autenticazione necessarie.
  3. Fare clic su **Applica**.
- Se si utilizza il file di impostazione Kerberos del dispositivo, aggiungere o cambiare l'area di autenticazione nel file. L'area di autenticazione deve essere immessa in caratteri maiuscoli. Al termine, reinstallare il file nella stampante.

Orologi del controller di dominio e della periferica non sincronizzati

Accertarsi che la differenza tra l'ora della stampante e l'ora del controller di domino non sia superiore a cinque minuti

Per ulteriori informazioni, vedere "Impostazione di data e ora" a pagina 7.

Impossibile convalidare la catena di certificati del controller di dominio

Provare una o più delle seguenti soluzioni:

Accertarsi che tutti i certificati necessari per la convalida della catena siano installati nella stampante e che le informazioni siano corrette

Per ulteriori informazioni, vedere "Installazione manuale di certificati" a pagina 6.

Accertarsi che la catena di certificati vada dal controller di dominio all'Autorità di certificazione radice

Assicurarsi che tutti i certificati non siano scaduti

1. In Embedded Web Server, fare clic su **Impostazioni** > **Protezione** > **Gestione certificati**.
2. Assicurarsi che le date dei campi Valido da e Valido fino non siano scadute.

Consentire agli utenti di accedere anche se lo stato di uno o più certificati è sconosciuto

1. In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:
   App > **Client Autenticazione con smart card** > **Configura**
2. Nella sezione OCSP (Online Certificate Status Protocol), selezionare **Consenti stato sconosciuto**.

3 Fare clic su **Applica**.

Contattare il rappresentante Lexmark

Impossibile connettersi al risponditore OCSP

Provare una o più delle seguenti soluzioni:

Accertarsi che l'URL del risponditore OCSP sia corretto

1 In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:

App > **Client Autenticazione con smart card** > **Configura**

2 Nella sezione OCSP (Online Certificate Status Protocol), verificare che l'URL del risponditore sia corretto.

3 Fare clic su **Applica**.

Aumentare il valore di timeout del risponditore

1 In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:

App > **Client Autenticazione con smart card** > **Configura**

2 Nella sezione OCSP (Online Certificate Status Protocol), immettere un valore compreso tra 5 e 30 nel campo Timeout risponditore.

3 Fare clic su **Applica**.

Impossibile convalidare il certificato del controller di dominio rispetto al risponditore OCSP

Provare una o più delle seguenti soluzioni:

Accertarsi che l'URL del risponditore OCSP e il certificato del risponditore siano configurati correttamente

1 In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:

App > **Client Autenticazione con smart card** > **Configura**

2 Nella sezione OCSP (Online Certificate Status Protocol), nel campo URL del risponditore, specificare le seguenti impostazioni:

- Indirizzo IP o nome host del risponditore o ripetitore OCSP
- Numero della porta utilizzata

Ad esempio, **`http://x:y`**, dove ***x*** è l'indirizzo IP e ***y*** è il numero della porta.

3 Nel campo Certificato risponditore, selezionare il certificato appropriato.

4 Fare clic su **Applica**.

Verificare che il controller di dominio restituisca il certificato corretto

Assicurarsi che il risponditore OCSP convalidi il certificato del controller di dominio corretto

Impossibile accedere a singole applicazioni e funzioni della stampante

Provare una o più delle seguenti soluzioni:

Consentire l'accesso sicuro alle applicazioni o funzioni

Per ulteriori informazioni, vedere "Protezione dell'accesso a singole applicazioni e funzioni" a pagina 8.

Se l'utente appartiene a un gruppo Active Directory, accertarsi che il gruppo è autorizzato ad accedere alle applicazioni e funzioni

Problemi LDAP

Errore ricerche LDAP

Provare una o più delle seguenti soluzioni:

Assicurarsi che le impostazioni di server e firewall siano configurate per consentire la comunicazione tra la stampante e il server LDAP sulla porta 389 e 636

Se non si utilizza la ricerca DNS inversa sulla rete, disattivare tale opzione in Impostazioni Kerberos

1. Da Embedded Web Server, fare clic su **Impostazioni** > **Protezione**.
2. Nella sezione Account utente, fare clic su **Kerberos**.
3. Nella sezione Impostazioni varie, selezionare **Disattiva ricerche IP inverse**.
4. Fare clic su **Salva e verifica**.

Se il server LDAP richiede SSL, abilitare SSL per le ricerche LDAP

1. In Embedded Web Server, accedere alla pagina di configurazione dell'applicazione:
   App > **Client Autenticazione con smart card** > **Configura**
2. Nella sezione Impostazioni avanzate, selezionare **Usa SSL per le informazioni utente**.
3. Fare clic su **Applica**.

Restringere la base di ricerca LDAP all'ambito minimo possibile che includa tutti gli utenti necessari

Accertarsi che tutti gli attributi LDAP siano corretti

Errore licenza

Contattare il rappresentante Lexmark

Avvertenze

Nota all'edizione

Agosto 2017

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 COMMERCIABILITÀ 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 vìoli 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 di Lexmark, visitare il sito Web all'indirizzo **http://support.lexmark.com**.

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

Marchi

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

Microsoft, Windows e Active Directory sono marchi o marchi registrati del gruppo di società Microsoft negli Stati Uniti e in altri Paesi.

Tutti gli altri marchi appartengono ai rispettivi proprietari.

GNU Lesser General Public License

Vedere la GNU Lesser General Public License online all'indirizzo **http://www.gnu.org/licenses/lgpl.html**.

Additional copyrights

This product includes software developed by:

Indice

O

P

R

S

T

U

V