Version 1.6, October 2010

Xerox Secure Access Unified ID System™

Guida all'amministrazione

Traduzione:
Xerox
CTC European Operations
Bessemer Road
Welwyn Garden City
Hertfordshire
AL7 1BU
Regno Unito

Indice generale

5 Appendici

Note sulla sicurezza 1

Leggere attentamente queste note per assicurarsi di utilizzare la macchina in modo sicuro e in conformità alle leggi vigenti.

La macchina è stata progettata e collaudata per soddisfare severi requisiti di sicurezza. Tali requisiti comprendono l'approvazione di enti di certificazione per la sicurezza e la conformità agli standard di protezione ambientali in vigore.

Prima di utilizzare la macchina, leggere attentamente le seguenti istruzioni e farvi riferimento per garantire un funzionamento sempre sicuro del sistema.

AVVERTENZA: qualsiasi alterazione non autorizzata, compresi l'aggiunta di nuove funzioni o il collegamento di dispositivi esterni, può invalidare la certificazione del prodotto. Per ulteriori informazioni, rivolgersi al fornitore autorizzato di zona

Alimentatore elettrico

L'alimentatore fornito con la macchina deve essere utilizzato con il tipo di alimentazione indicato sull'etichetta dati. Se non si è certi che l'alimentazione elettrica utilizzata soddisfa tali requisiti, rivolgersi alla locale società erogatrice di energia elettrica per informazioni.

AVVERTENZA - Informazioni sulla sicurezza elettrica

- Utilizzare esclusivamente l'alimentatore fornito con il sistema.
- Non collocare il sistema in luoghi di passaggio o in cui il cavo di alimentazione e il relativo alimentatore potrebbero essere calpestati.
- Non collocare oggetti sul cavo dell'alimentatore.
- Qualora si verifichi una qualsiasi delle seguenti condizioni, spegnere immediatamente la macchina e scollegare il cavo di alimentazione dalla presa elettrica. Contattare un fornitore di assistenza autorizzato locale per risolvere il problema.
  - La macchina emette odori anomali.
  - Il cavo di alimentazione è danneggiato o consunto.
  - È scattato l'interruttore automatico del quadro elettrico, il fusibile o altro dispositivo di sicurezza.
  - La macchina è stata esposta all'acqua.
  - Una qualunque parte della macchina è danneggiata.

Dispositivo di scollegamento

Il cavo di alimentazione dell'alimentatore agisce da dispositivo di scollegamento per il sistema. Per interrompere completamente l'alimentazione alla macchina, scollegare il cavo di alimentazione dalla presa elettrica.

Informazioni sulle norme vigenti

Emissioni di radiofrequenze

Stati Uniti, Canada

Nota: il sistema è stato collaudato e giudicato conforme ai limiti di un dispositivo digitale di Classe B, Parte 15 delle Normative FCC. Tali limiti sono intesi a fornire una ragionevole protezione da interferenze dannose in un'installazione di tipo residenziale. Il sistema genera, utilizza e può irradiare energia di radiofrequenza e, se non installato e utilizzato in accordo alle istruzioni, può provocare interferenze dannose alle radiocomunicazioni. Tuttavia, non esiste alcuna garanzia che, in una specifica installazione, non si verificheranno interferenze. Qualora il sistema causi interferenze dannose alla ricezione radio o televisiva, determinate dall'accensione o dallo spegnimento della macchina, si consiglia che l'utente corregga tali interferenze adottando una o più delle seguenti misure:

- Cambiare l'orientamento dell'antenna ricevente o spostarla.
- Aumentare la distanza tra il sistema e il dispositivo ricevente.
- Collegare il sistema a una presa su un circuito diverso da quello al quale è collegato il dispositivo di ricezione.
- Rivolgersi al rivenditore o a un tecnico radio/TV qualificato.

Il sistema richiede l'utilizzo di cavi di interfaccia schermati per garantire la conformità alle normative FCC negli Stati Uniti

Canada

Questo dispositivo digitale di classe "B" è conforme alla normativa canadese ICES-003.

Cet appareil Numérique de la classe "B" est conforme à la norme NMB-003 du Canada.

Europa

CE	Il marchio CE apposto a questo prodotto costituisce la dichiarazione di conformità da parte di XEROX alle seguenti direttive applicabili dell'Unione europea alle date indicate:
12 dicembre 2006:	Direttiva del Consiglio 2006/95/CE e relativi emendamenti, per il ravvicinamento della legislazione degli stati membri in relazione alle apparecchiature a bassa tensione.
15 dicembre 2004:	Direttiva del Consiglio 2004/108/CE e relativi emendamenti, per il ravvicinamento della legislazione degli stati membri in relazione alla compatibilità elettromagnetica.
9 marzo 1999:	Direttiva del Consiglio 99/5/CE in materia di apparecchiature radio e apparecchiature terminali di telecomunicazione e il mutuo riconoscimento della loro conformità.

Per una dichiarazione completa di conformità e la definizione delle direttive pertinenti e degli standard di riferimento, rivolgersi al fornitore XEROX di zona.

AVVERTENZE:

- Per consentire l'uso di questa macchina in prossimità di strumentazione industriale, scientifica e medica (ISM - Industrial, Scientific and Medical), può rendersi necessario limitare le radiazioni esterne generate dalla strumentazione ISM o prendere speciali precauzioni.
- Il sistema richiede l'utilizzo di cavi di interfaccia schermati per garantire la conformità alla Direttiva del Consiglio 89/336/CEE.

"Informazioni sulle norme vigenti per RFID"

I lettori forniti con il prodotto generano radiofrequenza da 13,56 MHz utilizzando un sistema a circuito d'induzione come dispositivo di identificazione a radiofrequenza (RFID). Questo dispositivo RFID è conforme ai requisiti specificati in FCC Part 15, in Industry Canada RSS-210, alla Direttiva del Consiglio 99/5/CE e a tutte le leggi e a tutti i regolamenti locali applicabili.

Il funzionamento di questo dispositivo è soggetto alle due condizioni seguenti: (1) questo dispositivo non può causare interferenze dannose e (2) questo dispositivo deve accettare qualsiasi interferenza, comprese quelle che potrebbero causare un funzionamento indesiderato.

Eventuali modifiche o cambiamenti apportati al sistema non espressamente approvati da Xerox Corporation possono invalidare la facoltà di utilizzare la macchina.

Riciclaggio e smaltimento del prodotto

Se è necessario smaltire autonomamente la macchina, si tenga presente che contiene piombo, mercurio e altri materiali il cui smaltimento, in alcuni paesi, potrebbe essere soggetto a normative specifiche per ragioni ambientali. La presenza di piombo e mercurio è pienamente conforme alle normative internazionali in vigore al momento della messa in commercio del prodotto.

Unione Europea

Informazioni sullo smaltimento per utenti commerciali

L'applicazione di questo simbolo sul sistema conferma la necessità di smaltire la macchina in conformità alle procedure nazionali in vigore.

In accordo con la legislazione europea, lo smaltimento di prodotti elettrici ed elettronici a fine vita va eseguito nel rispetto delle normative vigenti.

Prima di provvedere allo smaltimento del sistema, contattare il fornitore Xerox locale per informazioni sulle procedure di ritiro dei prodotti a fine vita.

Nord America (Stati Uniti, Canada)

Xerox ha messo in atto un programma di ritiro, riutilizzo e riciclaggio dei prodotti a livello mondiale. Contattare il fornitore Xerox (1-800-ASK-XEROX) per stabilire se questo prodotto Xerox fa parte del programma. Per ulteriori informazioni sui programmi ambientali Xerox, visitare il sito http://www.xerox.com/environment

Se è necessario smaltire autonomamente la macchina, si tenga presente che potrebbe contenere piombo, mercurio, perclorato e altri materiali il cui smaltimento, in alcuni paesi, potrebbe essere soggetto a normative specifiche per ragioni ambientali. La presenza di questi materiali è pienamente conforme alle normative internazionali in vigore al momento della messa in commercio del prodotto. Per informazioni su riciclaggio e smaltimento, contattare le autorità competenti del proprio paese. Negli Stati Uniti, è possibile anche consultare il sito Web di Electronic Industries Alliance http://www.eiae.org

Sostanze con perclorato: questo prodotto può contenere uno o più dispositivi contenenti perclorato, come le pile. Può essere necessaria una procedura speciale. Vedere in proposito http://www.dtsc.ca.gov/hazardouswaste/perchlorate

Informazioni sullo smaltimento per utenti privati

La presenza di questo simbolo sulla macchina indica che non è possibile smaltire il sistema tramite i normali canali di smaltimento dei rifiuti domestici.

Ai sensi della legislazione europea, gli apparecchi elettrici ed elettronici devono essere smaltiti diversamente dai rifiuti domestici.

I privati che risiedono nei Paesi Membri dell'Unione Europea hanno la facoltà di inviare gratuitamente gli apparecchi elettrici ed elettronici a speciali aree di raccolta. Per ulteriori informazioni, contattare l'ente che gestisce le operazioni di smaltimento di tali prodotti nel proprio paese.

In alcuni Stati Membri, in concomitanza con l'acquisto di un nuovo dispositivo, il rivenditore locale ha l'obbligo di ritirare gratuitamente il dispositivo sostituito. Rivolgersi al fornitore per informazioni.

Altri paesi

Per maggiori informazioni sulle modalità di smaltimento, contattare l'ente locale per lo smaltimento dei rifiuti.

Informazioni di contatto per la salute e la sicurezza sul lavoro

Informazioni di contatto

Per ulteriori informazioni in merito a salute e sicurezza sul lavoro in riferimento a questo prodotto, chiamare i seguenti numeri:

Stati Uniti: 1 800 828 6571

Canada: 1 800 828 6571

Europa: +44 1707 353 434

http://www.xerox.com/environment safety information US (informazioni sulla sicurezza del prodotto per gli Stati Uniti)

http://www.xerox.com/environment_europe safety information EU (informazioni sulla sicurezza del prodotto per l'UE)

Elenco di controllo per l'installazione

2

La Guida all'amministrazione e la Guida all'installazione di Xerox Secure Access contengono istruzioni dettagliate per l'installazione e la configurazione del server di Secure Access e dei sistemi MFP.
In questo capitolo viene fornita una tabella che descrive a grandi linee l'ordine di installazione in base al tipo di configurazione hardware di Secure Access a partire dalla Guida all'installazione.

Passaggi **(*) indica un passaggio obbligatorio**	**Xerox Secure Access con lettore di schede USB**	**Xerox Secure Access con dispositivo di autenticazione e lettore di schede**
Guida all'installazione		
1. Leggere il capitolo 3, Descrizione generale dell'installazione	*	*
2. Capitolo 4, Installazione del server di Secure Access, sezione 1, Preparazione della rete e del database	*	*
3. Capitolo 4, Installazione del server di Secure Access, sezione 2, Esecuzione della procedura di installazione guidata	*	*
4. Capitolo 5, Configurazione dell'hardware: passaggio 1, Configurazione dell'indirizzo IP del dispositivo di autenticazione	Saltare	*
5. Capitolo 5, Configurazione dell'hardware: passaggio 2, Montaggio del dispositivo di autenticazione di Secure Access	Saltare	*
6. Capitolo 5, Configurazione dell'hardware: passaggio 3. Collegamento dell'hardware	Saltare	*
7. Capitolo 5, Configurazione dell'hardware: passaggio 4. Installazione/collegamento del lettore di schede USB di Secure Access	*	Saltare
Guida all'amministrazione		
8. Leggere il capitolo 3, Descrizione generale di Secure Access	*	*
9. Capitolo 4, Flusso di lavoro di configurazione, passaggio 1, Configurazione del dispositivo Xerox MFP in modo che accetti l'autenticazione di rete attraverso il meccanismo Xerox Secure Access	*	*
10. Capitolo 4, Aggiunta dei dispositivi MFP al database di Secure Access	*	*

Passaggi **(*) indica un passaggio obbligatorio**	**Xerox Secure Access con lettore di schede USB**	**Xerox Secure Access con dispositivo di autenticazione e lettore di schede**
11. Capitolo 4, Associazione dell'MFP a un dispositivo di autenticazione di Secure Access	Saltare	*
12. Capitolo 4, Configurazione della stampa Follow-You (opzionale)	*	*
13. Capitolo 4, Impostazione dei parametri di autenticazione	*	*
14. Capitolo 4, Importazione e sincronizzazione degli account utente	*	*
15. Capitolo 4, Configurazione del servizio personalizzato Release My Documents (Rilascia i miei documenti)	*	*

3 Descrizione generale di Secure Access

In questo capitolo:

Dopo avere installato il server Xerox Secure Access Unified ID System™ ed eseguito la configurazione fisica dei dispositivi di autenticazione o del lettore di scheda USB Secure Access, utilizzare questa guida per aggiungere dispositivi MFP (Multi-function Printer, stampante multifunzione) al database di Secure Access e abilitare la comunicazione tra il server e i dispositivi di autenticazione. Utilizzare questa guida per eseguire le attività di configurazione avanzate per tutti i componenti e le funzioni di Secure Access.

Questo capitolo fornisce informazioni su:

- i componenti hardware e software che compongono Xerox Secure Access
- l'accesso a Secure Access Manager per amministrare il sistema

Che cos'è Secure Access?

Secure Access Unified ID System consente di controllare l'accesso alle funzioni di stampa, fax, copia e scansione sulle stampanti multifunzione (MFP) Xerox. Per poter utilizzare un dispositivo gestito da Secure Access, un utente deve far scorrere la propria scheda sul lettore di schede o avvicinarla a quest'ultimo. Il pannello comandi dell'MFP si attiva solo se le informazioni dell'account utente sono state autenticate dal server di Secure Access.

Utilizzando un protocollo proprietario (Convenience Authentication Protocol), il dispositivo di autenticazione di Secure Access si connette al server tramite una connessione di rete Ethernet per verificare le informazioni dell'utente lette da una scheda o da una scheda di prossimità. Se si utilizza un lettore di schede USB, la comunicazione avviene direttamente dall'MFP al server di Secure Access. Se il server di Secure Access autorizza l'utente, il pannello del dispositivo MFP si sblocca ed è pronto per l'uso. Se l'utente non viene autorizzato, l'MFP resta bloccato e l'utente non è in grado di eseguire alcuna attività sul dispositivo.

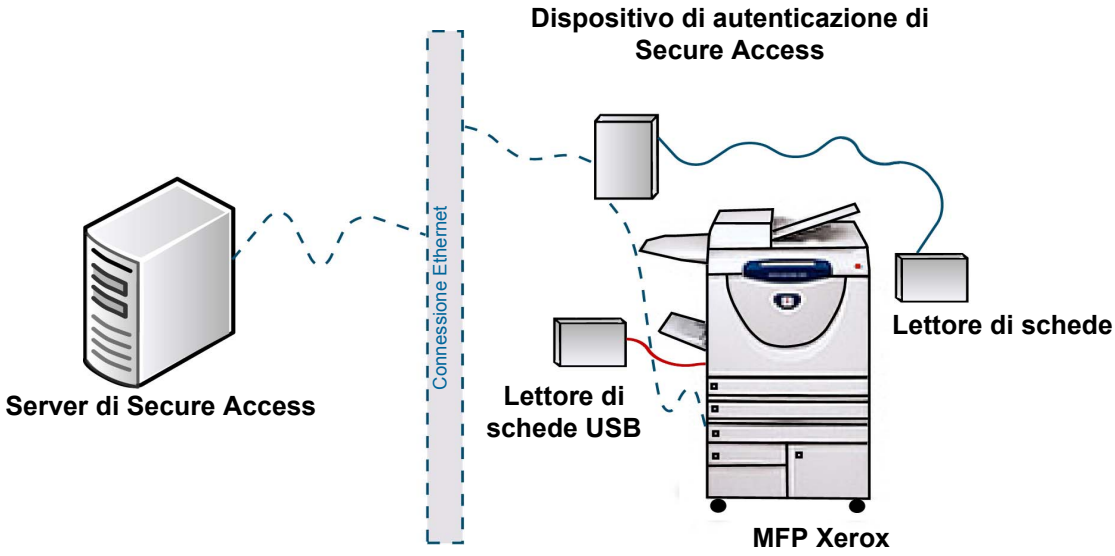


Figura 3-1: Componenti della soluzione Secure Access

Se l'utente desidera scansire documenti, il server di Secure Access fornisce l'ID utente di rete all'MFP compatibile; il dispositivo MFP utilizza l'ID per implementare la funzionalità Single Sign-on ed eseguire l'autenticazione automatica per la scansione.

Componenti di Secure Access

La soluzione richiede due componenti principali:

1. Il dispositivo di autenticazione di **Secure Access**, che comprende un terminale di autenticazione e un lettore di schede esterno. Gli utenti non accedono al terminale di autenticazione.

   Il lettore di schede è collegato al dispositivo di autenticazione solo attraverso un cavo seriale mentre non è collegato direttamente all'MFP. Vedere la *Guida all'installazione* per le istruzioni di installazione e montaggio.

Figura 3-2: Dispositivo di autenticazione di Secure Access

Oppure

1. **Lettore di schede USB del server di Secure Access**, che è collegato al dispositivo MFP. Vedere la Guida all'installazione per le istruzioni di installazione e montaggio.
2. **Server di Secure Access**, che comprende i seguenti componenti:
   - CAS (Core Authentication Server - Server di autenticazione principale)
   - DCE (Device Control Engine - Motore di controllo del dispositivo)
   - DRE (Document Routing Engine - Motore di instradamento documenti)
   - Manager Secure Access (Strumenti amministrativi)

   Nota: è possibile installare questi componenti in un unico server oppure distribuirli su più server. Alcune installazioni possono richiedere anche più di un DCE o DRE. Per maggiori dettagli, vedere la *Guida all'installazione*.

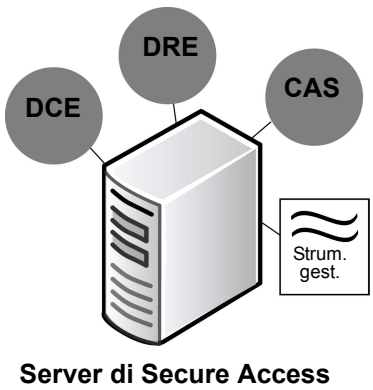


Figura 3-3: Componenti server di Secure Access

I componenti del server principale utilizzano porte dedicate per la comunicazione. Ogni componente attende la connessione su una specifica porta per ricevere dati o richieste provenienti da altri componenti. Per un elenco completo delle assegnazioni di porta per componente, vedere Assegnazioni porta a pagina 45.

CAS (Core Authentication Server - Server di autenticazione principale)

Sul CAS risiede il database che contiene i dati di tutti gli utenti e dispositivi MFP.

Ogni installazione di Secure Access richiede la presenza di un database preinstallato. Il CAS utilizza l'istanza del database per creare un database di account contenente le informazioni su tutti gli utenti e i dispositivi. Per informazioni sui database supportati, vedere Requisiti di sistema nella Guida all'installazione.

DCE (Device Control Engine - Motore di controllo del dispositivo)

Il DCE gestisce tutte le comunicazioni con i dispositivi MFP. Quando un utente desidera utilizzare la funzionalità di copia, scansione o fax su un MFP, deve prima attivare il lettore di schede. La lettura di una scheda o scheda di prossimità dà inizio a una richiesta di accesso.

Il dispositivo di autenticazione inoltra la richiesta di accesso al DCE, il quale contatta il CAS per verificare i dati dell'account utente associato alla scheda. Questo processo viene descritto nelle figure 4 e 5.

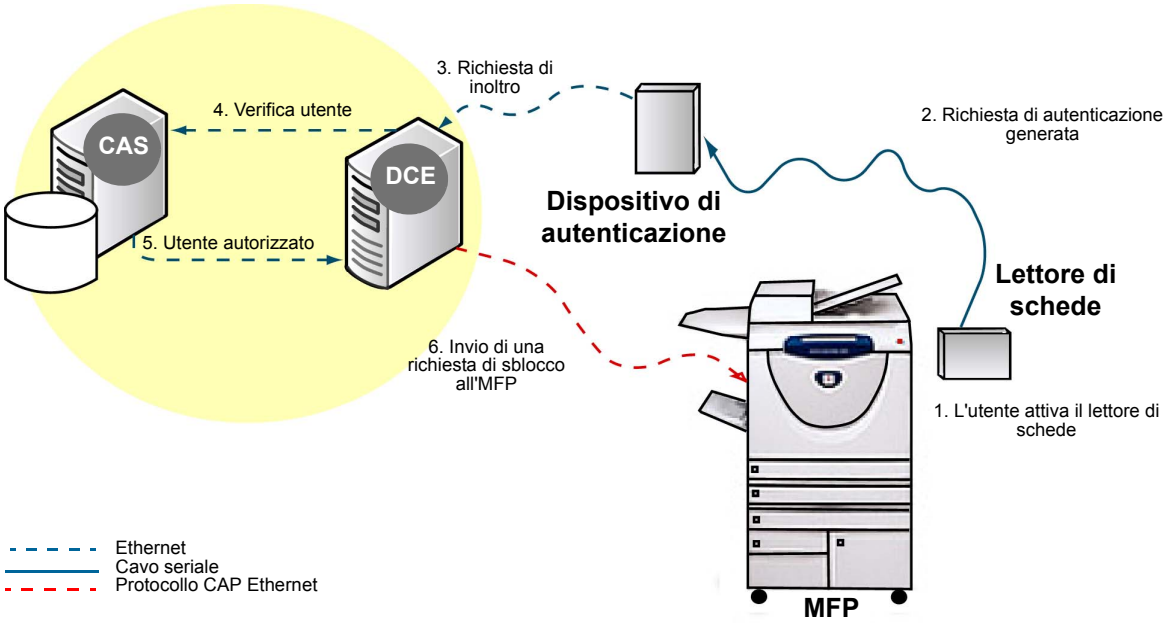


Figura 3-4: Flusso di lavoro di autenticazione utente

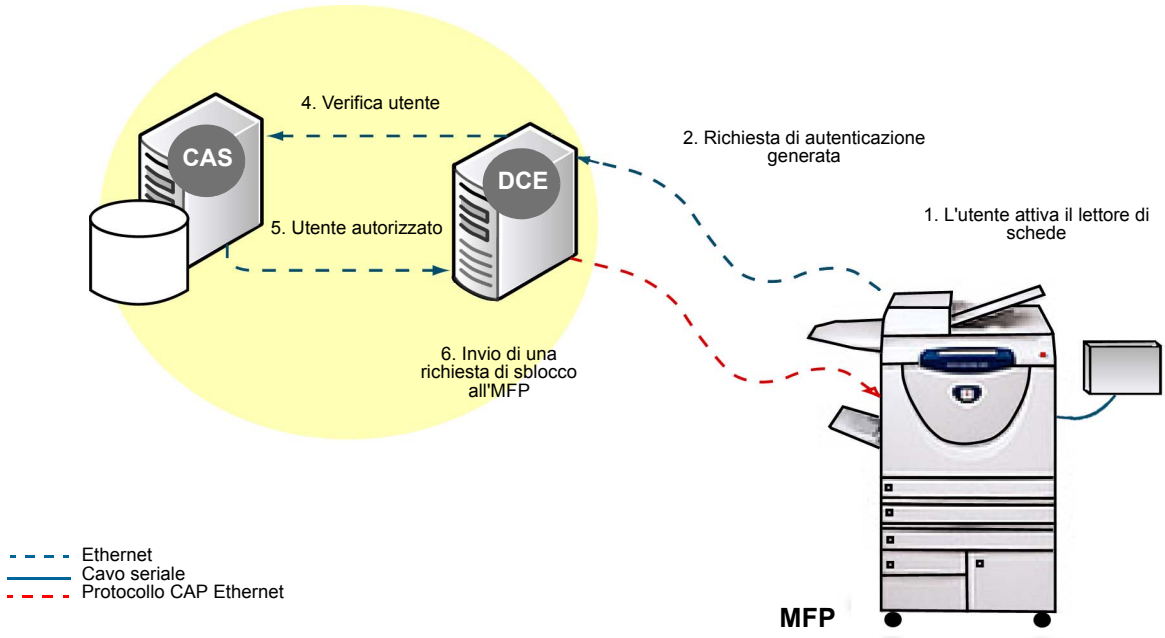


Figura 3-5: Flusso di lavoro di autenticazione utente con lettore di schede USB

DRE (Document Routing Engine - Motore di instradamento documenti)

Il DRE è il server di stampa. La funzione principale del server è quella di abilitare il flusso di documenti dalle workstation degli utenti ai dispositivi MFP. Di seguito viene descritto un tipico flusso di lavoro DRE:

1. Un utente genera una richiesta di stampa a un MFP che viene registrata nel database di Secure Access Manager.
2. Se l'utente inoltra il lavoro di stampa a una coda che utilizza una porta di Secure Access Manager, il DRE trattiene il lavoro sul server di stampa.
3. Quando l'utente esegue l'accesso all'MFP, il DRE cerca i lavori per quella stampante (e/o gruppo di pull) e rilascia quelli che sono stati inviati dall'utente che ha eseguito l'accesso.

   Nota: se il servizio personalizzato Release My Documents (Rilascia i miei documenti) è installato, gli utenti possono accedere alla schermata Release My Documents per vedere la coda di stampa protetta e rilasciare uno o più documenti. Vedere Configurazione del servizio personalizzato Release My Documents (Rilascia i miei documenti) a pagina 40.

Se nel dispositivo non è installata una porta Secure Access, il lavoro viene stampato senza convalida.

Per stampare i lavori trattenuti in una coda protetta, è possibile configurare la stampa Follow-You. Per attivare questa funzionalità, è necessario configurare l'MFP affinché utilizzi una porta di Secure Access e non una porta standard. Il monitor porta si integra con le funzioni e il sistema secondario di stampa Windows come parte del servizio di spooling. Il monitor porta riceve i lavori di stampa e li trattiene in una coda virtuale protetta in attesa che un utente autorizzato li rilasci per un particolare MFP.

Quando la stampa Follow-You è abilitata, l'utente deve prima eseguire l'autenticazione sull'MFP prescelto; come descritto in Figure 3-4: Flusso di lavoro di autenticazione utente a pagina 16. Se l'autenticazione riesce e il servizio personalizzato Release My Documents è installato, l'utente può accedere al pannello frontale dell'MFP per visualizzare la coda di stampa. L'utente può rilasciare uno o tutti i lavori (se configurati).

Esecuzione di modifiche ai componenti del server

Se si apportano modifiche di configurazione ai componenti principali (CAS, DRE, DCE) del server di Secure Access all'interno di Secure Access Manager (ad esempio l'aggiunta di nuovi dispositivi di Secure Access), è necessario attendere almeno trenta secondi prima che tali modifiche diventino effettive.

Il ritardo dell'aggiornamento dei componenti del server dipende dalla funzione di polling di CAS. Ciò significa che il ritardo potrebbe essere maggiore nel caso in cui CAS non fosse disponibile durante il polling dopo le modifiche al server. CAS invia i nuovi dati ai componenti interessati una volta che la connessione viene ripristinata.

Supporto per il lettore di dati e il flusso di lavoro utente

Le funzionalità di MFP sono bloccate finché un utente non fornisce dati di autenticazione validi. A tal fine, l'utente deve far scorrere la propria scheda di prossimità o smart card sul lettore di prossimità oppure scorrere la scheda in un lettore di banda magnetica.

Una volta che il CAS ha convalidato i dati dell'utente, l'MFP viene sbloccato ed è pronto per essere utilizzato. Quando l'utente ha finito di usare il dispositivo, preme il pulsante **Clear All (Cancella tutto)** o **Access (Accesso)** sulla tastiera dell'MFP per uscire e bloccare il dispositivo.

Secure Access supporta numerosi tipi di lettori esterni: lettore di banda magnetica, EM Marin, lettore di schede di prossimità HID, Hitag, Indala, Legic e Mifare. Tutti i lettori vengono preconfigurati dal produttore e non richiedono ulteriore configurazione.

Lettore di banda magnetica

Secure Access supporta lettori di banda magnetica esterni. Gli utenti possono immettere i dati per la convalida facendo scorrere una scheda magnetica codificata attraverso un lettore di schede. Il lettore è in grado di leggere qualsiasi scheda magnetica standard sulla Traccia 2 e accetta dati con codifica standard e personalizzata. I dati della traccia 1 sono disponibili con i lettori di banda magnetica USB.

Utilizzo di un lettore di banda magnetica

Illustrare agli utenti la seguente procedura che consente di utilizzare un lettore magnetico a strisciamento:

1. Inserire la scheda nel binario con la banda magnetica rivolta lontano dal terminale. Premere con decisione la scheda contro la guida.
2. Far scorrere la scheda lungo il binario ed estrarla.

   Nota: non strisciare la scheda tenendola inclinata, altrimenti il terminale non riesce a leggere i dati.

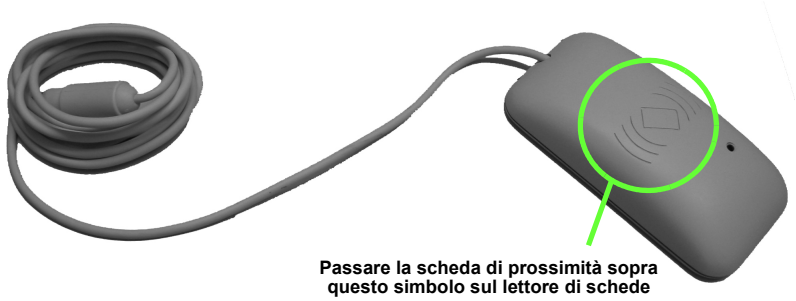
   Se il terminale non è in grado di leggere la scheda, il LED emette una luce rossa fissa. Inserire nuovamente la scheda nel binario e farla scorrere attraverso il lettore.

Smart Card (schede intelligenti) senza contatto e schede di prossimità

Secure Access supporta smart card senza contatto Legic e Mifare: lettore di banda magnetica, EM Marin, lettore di schede di prossimità HID, Hitag, Indala, Legic e Mifare. Gli utenti possono immettere i dati di convalida passando la scheda di prossimità a una distanza massima di 2,5 centimetri dal lettore esterno.

Utilizzo di una scheda di prossimità o smart card

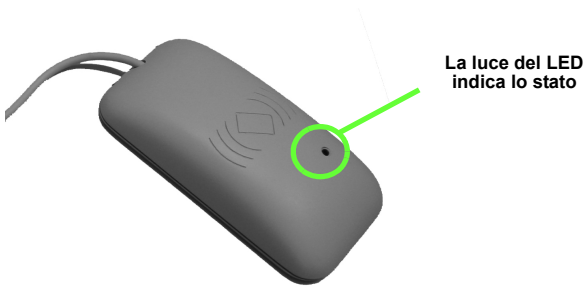
Per immettere i dati utilizzando una scheda di prossimità o una smart card, passare la scheda a una distanza massima di 2,5 centimetri dal simbolo di prossimità situato nella parte alta del lettore di schede. Per individuare il lettore di prossimità sul lettore di dati, cercare questo simbolo:



Se la lettura effettuata non è valida, il LED diventa rosso e lampeggia.

Segnali e modalità del lettore di schede

Secure Access visualizza i messaggi attraverso un LED sul modulo del lettore di schede.



Il comportamento del LED è identico per entrambi i lettori di schede, tranne per le differenze segnalate. Possono essere visualizzati i seguenti segnali:

Stato del LED	Significato
Rosso fisso	Il sottosistema di autenticazione è inattivo; è pronto ma non ci sono sessioni attive.
Verde fisso	Il dispositivo di autenticazione è in modalità Pronto e una sessione è attiva. Questo stato si verifica anche se si utilizza un lettore di schede USB mentre il dispositivo MFP si avvia e il controller di rete non è stato inizializzato.
Verde lampeggiante lento	Dati ricevuti dal lettore di schede, in attesa di autenticazione per sessione attiva o input utente (es. autoregistrazione della scheda o Release All Jobs prompt (richiesta di rilascio di tutti i lavori)).
Rosso lampeggiante lento	Il sottosistema di autenticazione non è collegato al server.
Rosso lampeggiante veloce	Scheda non valida, accesso negato.

Il sottosistema di autenticazione ha due modalità di funzionamento: Modalità Inattivo o Modalità Pronto.

Un sottosistema di autenticazione pronto per l'utilizzo è in modalità Inattivo. Quando un utente fa scorrere una scheda con banda magnetica, il dispositivo passa alla modalità Pronto. Il dispositivo ritorna alla modalità Inattivo quando un utente completa una transazione o dopo un periodo di inattività in modalità Pronto, configurabile in base all'impostazione dell'MFP.

> Nota: il sottosistema di autenticazione ritorna alla modalità Inattivo se viene attivato il timer della modalità sospensione dell'MFP.

Quando il dispositivo è in modalità Inattivo, il LED sul lettore di schede è rosso fisso.

In modalità Pronto, il LED sul lettore di schede è verde fisso e l'utente può iniziare a utilizzare il dispositivo gestito per eseguire una transazione.

Amministrazione Secure Access

Tutte le operazioni di amministrazione vengono gestite attraverso Secure Access Manager. Per impostazione predefinita, il programma di installazione posiziona Secure Access Manager nel menu Start.

Cercarlo in **Start** > **Programmi** > **Xerox Secure Access** > **Secure Access Manager**.

Nota: è necessario disporre dei privilegi di Amministratore sul server di Secure Access per avviare Secure Access Manager.

Prima di avviare Secure Access Manager, selezionare il CAS con cui lavorare. Il CAS esegue la convalida utilizzando un singolo database di autenticazione, per cui è necessario digitare il nome corretto del database o sceglierlo dall'elenco.

L'interfaccia di Secure Access Manager è suddivisa in cinque aree. Quando si sceglie un'attività dagli strumenti, viene aggiornato il contenuto del riquadro destro e sono visualizzate le impostazioni disponibili.

Supporto lingue

Al momento dell'installazione di Secure Access, nella procedura guidata è stata visualizzata la richiesta di impostare la lingua da utilizzare per i componenti presenti nel pacchetto. Questa impostazione si applica solo all'interfaccia di Secure Access Manager.

La lingua visualizzata sul pannello comandi dell'MFP è determinata dalle impostazioni del dispositivo. Il server di Secure Access verifica l'impostazione della lingua del dispositivo MFP ogni volta che un utente fa scorrere la propria scheda nel lettore. Se sull'MFP è impostata una lingua diversa da inglese, francese, tedesco, italiano o spagnolo, le richieste di Secure Access vengono visualizzate in inglese.

Configurazione e gestione

4

In questo capitolo:

Per configurazione si intende la configurazione software necessaria per stabilire la comunicazione tra gli MFP, i dispositivi di autenticazione e il server. Si raccomanda di seguire il flusso di lavoro descritto a pagina 24 per ottenere risultati ottimali.

In questo capitolo vengono fornite informazioni per:

- eseguire una configurazione iniziale completa
- aggiungere i dispositivi MFP al database di Secure Access
- associare un dispositivo di autenticazione di Secure Access al dispositivo MFP se non si utilizza un lettore di scheda USB
- abilitare l'autenticazione e configurare ulteriori opzioni di autenticazione
- importare e sincronizzare gli account utente con Sincronizzazione di Active Directory
- monitorare gli eventi di autenticazione

Flusso di lavoro di configurazione

Eseguire i passaggi nell'ordine in cui vengono presentati. In caso contrario, l'installazione risulterà incompleta.

Prima di iniziare, verificare di aver installato correttamente il server di Secure Access. Seguire le istruzioni fornite nella Guida all'installazione di Xerox Secure Access Unified ID System™. Installare il CAS e almeno un DCE e un DRE.

1. **Configurazione del dispositivo Xerox MFP in modo che accetti l'autenticazione di rete attraverso il meccanismo Xerox Secure Access**

   A tale scopo, utilizzare CentreWare Internet Services, a cui è possibile connettersi tramite un browser Internet. Per informazioni su come installare e configurare Xerox Secure Access sul dispositivo, vedere il CD di amministrazione del sistema MFP.

2. **Aggiunta dei dispositivi MFP al database di Secure Access**

   Creare una voce per ciascun dispositivo MFP presente in Secure Access Manager. Assegnare ciascun MFP a un particolare server di stampa DRE (se necessario).

3. **Configurazione della stampa Follow-You**

   Nota: questo passaggio è facoltativo e va eseguito solo se è necessario utilizzare la stampa Follow-You nel sito.

   Per configurare la stampa Follow-You, creare dei gruppi di pull che raggruppano i dispositivi con caratteristiche simili. Quando un utente invia un documento a un MFP parte di un gruppo di pull, l'utente può eseguire l'autenticazione su un qualsiasi MFP del gruppo che provvederà ad estrarre il lavoro dalla coda e a stamparlo.

4. **Impostazione dei parametri di autenticazione**

   Configurare i parametri che saranno utilizzati da Secure Access per autenticare le richieste di accesso degli utenti, compresa l'abilitazione di richieste secondarie e la configurazione dei dati della scheda.

5. **Importazione e sincronizzazione degli account utente**

   Configurare i parametri di sincronizzazione di Active Directory, quindi importare gli account utente esistenti nel database di Secure Access.

6. **Installare il servizio personalizzato Release My Documents (Rilascia i miei documenti)**

   Per consentire agli utenti di visualizzare o rilasciare uno o più documenti dalla coda di stampa direttamente dal pannello comandi dell'MFP, installare il servizio personalizzato Release My Documents.

7. **Configurazione dell'autoregistrazione della scheda**

   Per consentire agli utenti di registrare autonomamente le proprie schede.

Aggiunta dei dispositivi MFP al database di Secure Access

Ogni MFP deve essere registrato nel database di Secure Access. È necessario assegnare un nome univoco a ogni dispositivo MFP e disporre dell'indirizzo IP di rete di ognuno.

Questo passaggio è suddiviso in due ulteriori passaggi per facilità: Immissione dei parametri del dispositivo e Associazione del dispositivo MFP a un dispositivo di autenticazione Secure Access.

Immissione dei parametri del dispositivo

1. In Secure Access Manager fare clic su **Devices (Dispositivi)**.
2. Da Settings (Impostazioni), fare clic su **Add...(Aggiungi)** nell'elenco di dispositivi.
3. Nella finestra di dialogo Physical Device Summary (Riepilogo dispositivi fisici) che viene visualizzata, digitare le informazioni richieste, descritte nella tabella in basso.

   Nota: i campi Manufacturer (Produttore) e Model (Modello) vengono compilati automaticamente la prima volta che il dispositivo contatta il DRE. Alla successiva riapertura di questa finestra, l'informazione sarà già presente.

Impostazione	Descrizione
Name (Nome)	Digitare un nome univoco per questo MFP. Questo nome verrà utilizzato per identificare il dispositivo in Secure Access Manager.
Hostname/IP address (Nome host/Indirizzo IP)	Digitare l'indirizzo IP o il nome host. Si raccomanda di risolvere il nome host qualora non si conosca l'indirizzo IP.
Descrizione	Immettere una descrizione che aiuterà gli altri amministratori a identificare il dispositivo, solitamente per ubicazione. Ad esempio, "secondo piano, Risorse Umane".
Dispositivo di autenticazione	Selezionare il dispositivo di autenticazione di Secure Access (dall'indirizzo MAC) che controllerà l'accesso a questo MFP. Nota: se si utilizza un lettore di schede USB di Secure Access, non associare un dispositivo di autenticazione e lasciarlo "<USB Reader>" (lettore USB).
Secure Access compatibility (Compatibilità Secure Access)	• **MFP with Secure Access capability** (MFP con funzionalità Secure Access): selezionare l'opzione se MFP utilizza un lettore di schede USB o se si utilizza un dispositivo MFP Xerox che supporta Secure Access. Immettere l'**Admin ID** (ID amministrazione) e la **Password** associati a questo MFP. • **Other type of MFP or printer** (Altro tipo di MFP o stampante): selezionare l'opzione se il dispositivo di autenticazione viene utilizzato per la stampa Follow-You con qualsiasi MFP o stampante che non supporta Secure Access.
Server	Immettere il nome del server in cui è stato installato DCE e che controllerà questo MFP o questa stampante.

Impostazione	Descrizione
Initialize Secure Access device (Initializzazione del dispositivo Secure Access)	Il dispositivo di Secure Access viene inizializzato automaticamente alla prima configurazione. Se si cambia l'MFP, inizializzare il dispositivo Secure Access facendo clic su questo pulsante. Verrà visualizzata una finestra di pop up in cui si conferma che l'inizializzazione è stata eseguita correttamente. Nota: utilizzare questo pulsante anche per installare il servizio personalizzato Release My Documents (Rilascia i miei documenti). Per ulteriori informazioni, vedere Configurazione del servizio personalizzato Release My Documents (Rilascia i miei documenti) a pagina 40.
Behavior (Comportamento)	Se si utilizza Secure Access Port Monitor per consentire la stampa Follow-You, è possibile scegliere tra due opzioni di rilascio disponibili: • **Al terminale di controllo assegnato:** l'utente deve far scorrere la propria scheda sull'MFP per rilasciare i documenti inviati a quel dispositivo. • **Release documents from pull group (Rilascia i documenti dal gruppo di pull):** dopo l'autenticazione, l'utente può seguire le istruzioni sul pannello comandi per selezionare i documenti in coda da uno specifico pull-group. Per ulteriori informazioni, vedere Configurazione della stampa Follow-You a pagina 32. Se si utilizzano i monitor porta di Windows, queste impostazioni non hanno effetto.

4. Fare clic su **OK** per salvare le impostazioni.

   Nota: se Secure Access rileva che il dispositivo è abilitato per i servizi personalizzati, e si sono effettuate modifiche nella finestra di dialogo Devices (Dispositivi), viene visualizzata una finestra popup:

   - Se l'estensione Release My Documents (Rilascia i miei documenti) non è installata nel dispositivo, viene visualizzato il messaggio "Do you want to enable Follow-You printing?" (Attivare la stampa Follow-You?).
   - Se l'estensione Release My Documents non è installata nel dispositivo, viene visualizzato il messaggio "Do you want to enable Follow-You printing?" (Attivare la stampa Follow-You?).

Associazione dell'MFP a un dispositivo di autenticazione di Secure Access

Nota: se si utilizza un lettore di scheda USB di Secure Access, saltare questo passaggio.

La prima volta che si accende un dispositivo di autenticazione collegato alla rete, il DCE registra il dispositivo. In Secure Access Manager, il dispositivo viene visualizzato come dispositivo di autenticazione di Secure Access non assegnato. È necessario associare ogni MFP a un dispositivo di autenticazione di Secure Access Per associare ogni dispositivo di autenticazione all'MFP appropriato, utilizzare la scheda di configurazione (consultare la Guida all'installazione) compilata durante l'installazione dell'hardware.

1. In Secure Access Manager, fare clic su **Devices** (Dispositivi), quindi selezionare l'MFP da configurare.

2. Nella finestra di dialogo Physical Device Summary (Riepilogo dispositivi fisici), fare clic sull'elenco a discesa Hardware Address (Indirizzi hardware).
3. Utilizzando la propria scheda di configurazione come riferimento, individuare l'indirizzo MAC del dispositivo di autenticazione che controllerà l'accesso a questo particolare MFP.
4. Fare clic su **OK** per salvare le modifiche.

Impostazione dei parametri di autenticazione

Prima di importare gli account utente, è necessario configurare il server CAS per la convalida degli account in rapporto ai PIN principali e secondari. I PIN collegano un account utente di Secure Access alle informazioni contenute sulla scheda magnetica.

Il PIN principale è la sequenza numerica che identifica in modo univoco l'utente e corrisponde di solito al numero di scheda. Per immettere il PIN principale, l'utente deve semplicemente far scorrere la propria scheda.

Se si desidera attivare un ulteriore livello di protezione, è possibile abilitare anche PIN secondari. Se questi valori sono abilitati, l'utente deve prima far scorrere la propria scheda e poi immettere una password aggiuntiva sul pannello comandi dell'MFP. L'utente avrà accesso all'MFP solo se i dati della scheda magnetica e la password del PIN secondario vengono autenticati.

1. In Secure Access Manager, selezionare **Configuration** (Configurazione) > **Authentication Device Settings** (Impostazioni dispositivo di autenticazione).
2. Nell'area **Authentication mechanisms** (Meccanismi di autenticazione), selezionare uno o più meccanismi di autenticazione:
   - Selezionare **Secure Access PINs** solo se si desidera collegare un account di stampa Secure Access a dati di accesso.
   - Abilitare **External user ID and password** (ID utente esterno e password) solo se si utilizzano schede magnetiche per verificare le informazioni utente all'esterno di Secure Access.
   - Abilitare **Secure Access PIN with external password** (PIN Secure Access con password esterna) se gli utenti fanno scorrere la scheda per l'identificazione ma immettono anche la password del proprio account utente Secure Access. Secure Access eseguirà un controllo incrociato: cercherà l'account nel database, quindi verificherà l'account rispetto all'autorità esterna selezionata per l'accesso di rete.

   Nota: se si seleziona un meccanismo di autenticazione esterna, il campo **Enable secondary prompt** (Abilita richiesta secondaria) viene abilitato automaticamente. L'autenticazione esterna non può verificarsi se il campo Secondary PIN (PIN secondario) è vuoto.
3. Dall'area **External authorities** (Autorità esterne), selezionare una o più autorità esterne solo se è stato selezionato un metodo di autenticazione corrispondente:
   - Selezionare **Windows** per convalidare gli account rispetto a un dominio di Windows predefinito. Digitare il nome del dominio nel campo **Default domain** (Dominio predefinito).
   - Selezionare **NetWare** per convalidare gli account rispetto a un contesto NetWare predefinito. Immettere il nome nel campo **Default context** (Contesto predefinito).

   Nota: per eseguire la convalida rispetto a un contesto NetWare, è necessario installare il client Novell NetWare per Windows sul CAS.

   - Selezionare **LDAP** per convalidare gli account rispetto a un server LDAP predefinito. Digitare il nome del server LDAP, quindi scegliere un tipo di LDAP dall'elenco. Selezionare Force SSL encryption (Forza codifica SSL) per utilizzare la codifica SSL (Secure Socket Layer).

4. Nell'area **Card setup** (Impostazione scheda), eseguire le operazioni seguenti:
   a. Immettere la posizione dei dati di inizio e fine nei campi. I dati recuperati da queste posizioni verranno utilizzati come PIN principale.
   b. Fare clic su **<None>** (Nessuno) accanto a **HID decoding (Decodifica HID)** se si utilizza un lettore di scheda di prossimità HID. I dispositivi di autenticazione devono essere configurati in modo da restituire le informazioni sulla scheda in un formato standard.

   Per maggiori informazioni su come immettere parametri di decodifica, vedere HID decoding (Decodifica HID). a pagina 30.
   c. Selezionare **Auto-register primary PINs** (Registrazione automatica PIN primari) per permettere agli utenti di registrare una scheda magnetica non riconosciuta da utilizzare in futuro. Per istruzioni, vedere Configurazione dell'autoregistrazione della scheda a pagina 30.
5. Nell'area **Secure Access device prompts**, immettere il testo predefinito che verrà visualizzato sul pannello comandi dell'MFP:
   a. Immettere un **Title** (Titolo) che verrà visualizzato in tutte le richieste.
   b. Immettere il testo di **Login prompt** (Richiesta di accesso) che verrà visualizzato per richiedere all'utente di eseguire la procedura di accesso. Ad esempio "Please swipe your card to login" (Far scorrere la scheda per accedere).
   c. Selezionare **Enable secondary prompt** (Abilita richiesta secondaria) per visualizzare sul pannello comandi dell'MFP Xerox un messaggio che richieda all'utente di immettere un codice PIN (o password) secondario.
   d. Selezionare **Enable release all jobs prompt** (Abilita richiesta di rilascio di tutti i lavori) per visualizzare sul pannello comandi dell'MFP Xerox un messaggio che richieda all'utente se desidera rilasciare tutti i lavori in coda per la stampa.
6. Nell'area **SNMP** immettere i propri valori di **Get** and **Set Community names** (Nomi di comunità Get e Set)

   Nota: se si modificano i nomi predefiniti in Secure Access, è necessario cambiarli anche su tutti i dispositivi fisici in modo che la comunicazione SNMP funzioni. Per informazioni su come cambiare queste impostazioni, consultare la documentazione dell'MFP.
7. Immettere il numero di **JBA Account Identification** (Identificazione di account JBA) se si desidera utilizzare Secure Access con un'applicazione di contabilità JBA esterna.
8. Impostare **Job Expiry** time (Ora di scadenza lavori) per indicare il numero di ore trascorse le quali ogni lavoro ancora presente in coda di stampa verrà rimosso dalla coda. Il valore predefinito è 1 ora.
9. Se sulla rete non si utilizzano i nomi di comunità SNMP predefiniti, ("public" per l'accesso in lettura e "private" per l'accesso in scrittura), specificare i nomi di comunità nei campi corrispondenti della finestra. Notare che tutti i dispositivi devono utilizzare gli stessi nomi di comunità.

   Nota: se non si immettono i nomi di comunità, il server di Secure Access non sarà in grado di rilevare automaticamente i tipi di dispositivo quando si creano nuove porte; sarà tuttavia ancora possibile creare porte specificando manualmente i dettagli della connessione.
10. Fare clic su **OK** per salvare le impostazioni.

HID decoding (Decodifica HID).

Per configurare la codifica HID, eseguire le operazioni seguenti:

1. In Secure Access Manager, selezionare **Configuration** (Configurazione) > **Authentication Device Settings (**Impostazioni dispositivo di autenticazione).
2. Fare clic su **<None>** (Nessuno) accanto a **HID decoding** (Decodifica HID) nell'area Card Setup (Impostazione scheda).
3. Nell'area **HID decoding** (Decodifica HID), eseguire le operazioni seguenti:
   - Se si conosce il tipo di codifica, immettere le informazioni di codifica della scheda HID riportate di seguito. Se non si conosce il tipo di codifica, contattare il fornitore HID per stabilire quale tipo di codifica è utilizzato dalle schede di prossimità.
   - Nel caso in cui non sia necessario estrarre le informazioni di codice della struttura, contrassegnare solo **ID code** (codice ID). Se è necessario estrarre sia il codice di struttura che il codice ID, contrassegnare entrambe le opzioni.

   a. Nel campo **Facility Start** (Inizio struttura), immettere la posizione nel bitstream raw (basato su 0, da sinistra a destra, inclusivo) dove inizia il codice di struttura.
   b. Nel campo **Facility End** (Fine struttura), immettere la posizione nel bitstream raw (basato su 0, da sinistra a destra, inclusivo) dove termina il codice di struttura.
   c. Nel campo **Facility Width** (Larghezza struttura), immettere il numero di cifre decimali per la parte di struttura del valore che il dispositivo di autenticazione emetterà. Se necessario, all'inizio del numero verranno aggiunti degli zero. Se il proprio sito o il formato di scheda HID non utilizza un codice di struttura oppure se non si richiede che venga restituito come parte del valore di scheda, impostare Facility Width su 0 per disabilitare l'estrazione del numero di struttura.
   d. Nel campo **ID Start** (Inizio ID), immettere la posizione nel bitstream raw (basato su 0, da sinistra a destra, inclusivo) dove inizia il codice ID.
   e. Nel campo **ID End** (Fine ID), immettere la posizione nel bitstream raw (basato su 0, da sinistra a destra, inclusivo) dove termina il codice ID.
   f. Nel campo **ID Width** (Larghezza ID), immettere il numero di cifre decimali per la parte di codice ID del valore che il dispositivo di autenticazione emetterà. Se necessario, all'inizio del numero verranno aggiunti degli zero. Per ogni lettura di scheda, il dispositivo di autenticazione restituirà un singolo valore di autenticazione, cioè il codice struttura decodificato seguito dall'ID decodificato.
   g. Fare clic su **OK** per salvare le impostazioni.

Configurazione dell'autoregistrazione della scheda

Se si desidera che gli utenti registrino autonomamente le proprie schede magnetiche, è necessario abilitare questa opzione in Secure Access.

1. In Secure Access Manager, selezionare **Configuration** (Configurazione) > **Authentication Device Settings** (Impostazioni dispositivo di autenticazione).
2. Selezionare **Auto-register primary PINs** (Registrazione automatica PIN primari) nell'area Card **Setup** (Impostazione scheda).
3. Fare clic su **OK** per salvare le modifiche.

Quando un utente fa scorrere una scheda non registrata, il sistema visualizza un messaggio per richiedere di effettuare l'accesso all'MFP con credenziali valide (ID utente e password). Le credenziali dell'utente devono essere già presenti in CAS affinché l'autoregistrazione abbia successo.

Una volta registrata la la scheda, ogni volta che l'utente la farà scorrere, le relative informazioni di account verranno associate automaticamente alla scheda e l'utente potrà accedere senza immettere manualmente le proprie credenziali. Potrà essere richiesto al''utente un PIN secondario, se configurato.

Nota: se l'opzione **Secure Access PIN with external password** (PIN Secure Access con password esterna) è selezionata al momento della configurazione dell'autoregistrazione, il PIN Secur Access verrà sostituito dai dati sulla scheda magnetica una volta che la scheda è stata autenticata e registrata. Il PIN Secur Access non costituirà più una credenziale valida per l'accesso.

Configurazione della stampa Follow-You

La stampa Follow-You permette a un utente di inviare un lavoro di stampa a un MFP ma di eseguire l'autenticazione su un MFP diverso, e quindi di visualizzare un elenco di lavori trattenuti in una coda protetta. L'utente può quindi "richiamare" il lavoro di stampa sull'MFP presso cui ha eseguito l'autenticazione, anche se questo non è il dispositivo originale selezionato per la stampa.

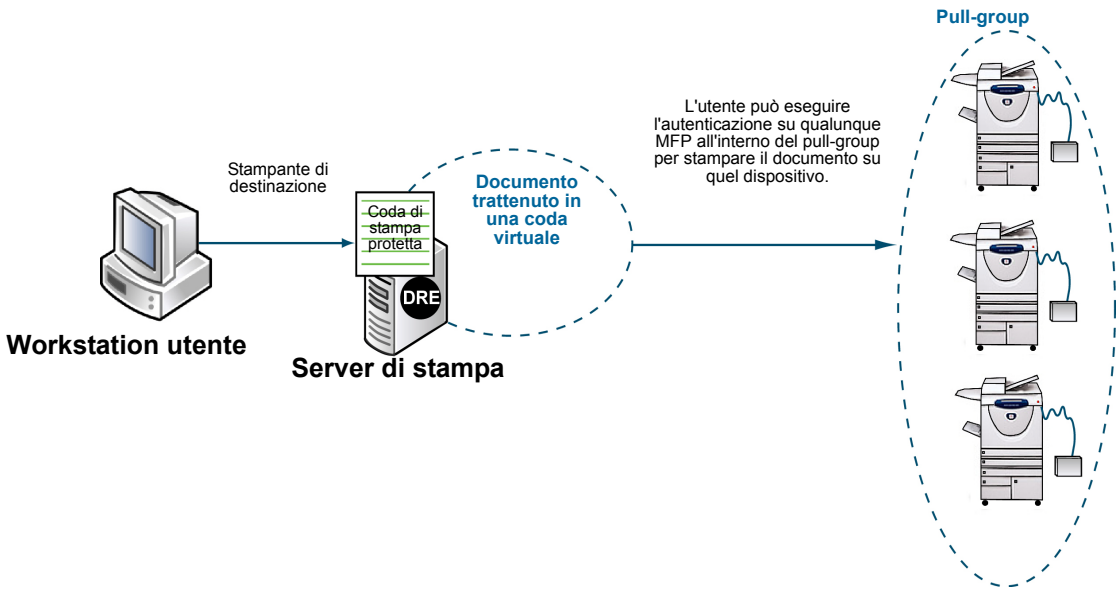


Figura 4-1: Flusso di lavoro per la stampa Follow-You

Per configurare la stampa Follow-You, è necessario eseguire due passaggi:

1. Utilizzare Secure Access Port Monitor per abilitare la configurazione tra il server di stampa e tutti gli MFP controllati. È possibile convertire le porte Windows esistenti in porte Secure Access. Il monitor porta intercetta tutti i documenti inviati ai dispositivi all'interno di un pull-group e li trattiene nella coda protetta fino al rilascio da parte dell'utente autorizzato. Per istruzioni, vedere Conversione delle porte per utilizzare Secure Access Port Monitor a pagina 32.
2. Creare i pull-group all'interno di Secure Access Manager. Vedere Creazione di gruppi di pull a pagina 34.

Per consentire all'utente di vedere i lavori in attesa nella coda protetta direttamente sul pannello comandi dell'MFP, aggiornare l'MFP in modo da includere il servizio personalizzato Release My Documents (Rilascia i miei documenti). Per istruzioni, vedere Configurazione del servizio personalizzato Release My Documents (Rilascia i miei documenti) a pagina 40.

Conversione delle porte per utilizzare Secure Access Port Monitor

Secure Access utilizza porte speciali per abilitare la stampa Follow-You. Ogni dispositivo che fa parte di un pull-group deve utilizzare Secure Access Port Monitor. Se si dispone di dispositivi già configurati per l'utilizzo di porte Windows, è possibile convertire facilmente le porte.

1. Accertarsi che i dispositivi da convertire siano accesi, connessi alla rete e configurati per la stampa.

2. Utilizzando **Risorse del computer**, spostarsi al percorso di installazione di Secure Access.
3. Aprire la cartella **Tools** e fare doppio clic su **SAPrinterConversionWizard.exe**.
4. Sulla schermata di benvenuto della procedura guidata Printer Conversion (Conversione stampante), fare clic su Next (Avanti).
5. Selezionare il **percorso del server di stampa**.

   Se il server di stampa (DRE) risiede sulla macchina locale, selezionare **Local machine** (Macchina locale), altrimenti selezionare **Remote server** (Server remoto).
6. Selezionare **Convert printers to use the Secure Access Port Monitor** (Converti stampanti per l'utilizzo di Secure Access Port Monitor), quindi fare clic su **Next** (Avanti).
7. Selezionare o deselezionare le stampanti nell'elenco **Convert Printers** (Converti stampanti), quindi fare clic su **Next** (Avanti).
8. Fare clic su **Finish** (Fine) per completare la conversione.

Creazione di una coda di stampa con una porta di Secure Access

Conformemente all'hardware della stampante, può essere necessaria più di una porta che utilizza Secure Access Port Monitor su un server di stampa. È possibile configurare una nuova definizione di stampante che utilizza Secure Access Port Monitor.

1. Utilizzando l'interfaccia standard di Windows, aprire la procedura **Installazione guidata stampante** di Windows.
2. Seguire le istruzioni visualizzate per aggiungere una stampante locale e creare una nuova porta.
3. Quando richiesto, selezionare **Porta Secure Access** come tipo di porta da creare e fare clic su Avanti. Viene visualizzata la procedura Aggiunta guidata porta stampante e viene richiesto di verificare che la stampante sia accesa, collegata alla rete e configurata in modo appropriato.
4. Fare clic su **Avanti** e selezionare **Physical printer** (Stampante fisica) come **Device Type** (Tipo di dispositivo) dall'elenco a discesa.
5. Specificare un **nome di stampante** o **indirizzo IP**.
6. La procedura guidata fornisce un **nome porta** basato sul nome della stampante o sull'indirizzo IP. Modificare questo nome manualmente, se desiderato.
7. Fare clic su **Avanti** per continuare con le opzioni di configurazione porta. Viene visualizzata la schermata di configurazione porta. Vengono visualizzate automaticamente le **informazioni del dispositivo rilevato** se la procedura guidata può ottenere questi dati dalla stampante.
8. Specificare se utilizzare le impostazioni standard o personalizzate per questa porta.

   Se si seleziona l'opzione **Use custom settings** (Utilizza impostazioni personalizzate):
   a. Se si seleziona comunicazione **Raw port** (Porta Raw), individuare il numero di **Porta** TCP e specificare se Port Monitor deve mantenere la connessione aperta.
   b. Se si seleziona **LPR**, specificare il nome della **Coda** di stampa sul dispositivo fisico (ad esempio, PORT1).
   c. Se si seleziona **Specific device** (Dispositivo specifico), selezionare il **Manufacturer** (Produttore) e il **Model** (Modello) appropriati dagli elenchi a discesa. Il dispositivo utilizza i parametri di comunicazione predefiniti relativi a queste selezioni.

9. Fare clic su **Avanti** e specificare il **nome del dispositivo fisico**. Questo è il nome del dispositivo visualizzato all'interno di Secure Access.
10. Rivedere i dettagli di questa nuova porta e della registrazione del dispositivo, quindi fare clic su **Fine** per chiudere Aggiunta guidata porta stampante di Secure Access oppure fare clic su **Indietro** per modificare qualche impostazione. Chiudendo la procedura guidata di aggiunta porte della stampante di Secure Access si ritorna a Installazione guidata stampante di Windows.
11. Completare i passaggi rimanenti di questa procedura. Quando richiesto, selezionare **Sì** per stampare una pagina di prova.
12. Verificare i dettagli della stampante Windows e fare clic su **Fine** per uscire dalla procedura oppure su **Indietro** per modificare qualche impostazione, se necessario.

Creazione di gruppi di pull

I gruppi di pull creati dovrebbero riflettere le esigenze della propria società. Ad esempio, è possibile raggruppare dispositivi compatibili per collocazione fisica, per reparto, per produttore e così via. È possibile creare gruppi di pull che includono una selezione di dispositivi collegati a un singolo server di stampa.

Il driver del dispositivo selezionato per il gruppo di pull deve essere compatibile con tutti i dispositivi associati a quel gruppo. Se si desidera che un lavoro di stampa generato per un MFP venga stampato con un MFP diverso, è fondamentale che la seconda stampante comprenda tutti i comandi di stampa inclusi nel flusso di dati proveniente dal driver.

1. In Secure Access Manager, fare clic su uno o più dispositivi MFP esistenti da assegnare allo stesso gruppo di pull.
2. Nella finestra di dialogo Physical Device Summary (Riepilogo dispositivo fisico), selezionare **Release documents from pull group** (Rilascia i documenti dal gruppo di pull). Digitare il nome del pull-group (si può utilizzare qualsiasi nome si desideri), quindi fare clic su **OK** per applicare la modifica.

   Nota: è necessario digitare il nome del pull-group soltanto la prima volta che viene utilizzato. In seguito, il nome apparirà automaticamente nell'elenco.
3. Ripetere i passaggi 1 e 2 per selezionare i dispositivi e creare altri gruppi di pull.

Importazione e sincronizzazione degli account utente

Per abilitare l'autenticazione, è necessario creare account utente che corrispondano agli attributi utilizzati sulla scheda magnetica. Quando un utente fa scorrere la propria scheda, il dispositivo di autenticazione inoltra la richiesta di accesso al DCE, il quale inoltra i dettagli della scheda al CAS. Se il CAS individua l'account utente con gli attributi che corrispondono a quelli trovati sulla scheda, l'MFP viene sbloccato e l'utente può eseguire l'operazione richiesta: trasmissione di fax, scansione, copia o rilascio di lavori di stampa.

In Secure Access sono disponibili tre metodi per importare gli account utente:

- Utilizzo di Active Directory per importare (e, in via facoltativa, sincronizzare) gli account.
- Importazione degli account utente da un file CSV.
- Creazione manuale di account all'interno di Secure Access Manager.

Utilizzo della sincronizzazione di Active Directory per importare utenti esistenti

Se si dispone di un server Active Directory, è possibile selezionare le informazioni di account che si desidera importare e sincronizzare. La sincronizzazione ridurrà al minimo le spese di gestione e permetterà di aggiornare automaticamente gli account.

La procedura descritta di seguito abilita l'esecuzione in background di un'attività. In Secure Access Manager, fare clic sullo strumento Users (Utenti) per osservare i risultati dell'attività; l'elenco di utenti verrà compilato automaticamente quando l'attività sarà completata.

> Nota: i servizi vanno avviati da un account di dominio con accesso ad Active Directory del contatto. Eseguire l'accesso come amministratore di dominio. Se i servizi vengono avviati usando un account di amministratore locale, la sincronizzazione di Active Directory avrà esito negativo.

È importante selezionare le opzioni nell'ordine corretto nella finestra di dialogo relativa alla sincronizzazione di Active Directory, seguire quindi con attenzione la procedura riportata di seguito.

1. In Secure Access Manager, fare clic su **Configuration** (Configurazione) > **Active Directory Synchronization** (Sincronizzazione di Active Directory).
2. Nell'area **Containers** (Contenitori), fare clic su **Add** (Aggiungi). Un controller di dominio è un server che fornisce accesso ad Active Directory per i computer membri. Digitare il nome del controller nel campo.
3. Nell'area **Containers** (Contenitori), fare clic su **Add** (Aggiungi). Un contenitore è una cartella presente nella struttura di Active Directory che contiene utenti, gruppi o computer.

> **ATTENZIONE:** Verificare che i contenitori OU scelti comprendano solo dati di account utente. Se gli OU contengono altri dati (come le informazioni di sistema o di contatto), si otterranno risultati imprevisti. Può essere necessario creare contenitori OU specifici da utilizzare solo per le operazioni di importazione e sincronizzazione.

4. Regolare l'**intervallo di sincronizzazione** per modificare la frequenza con cui Secure Access sincronizza il database con l'istanza di Active Directory specificata. Il valore dell'intervallo di sincronizzazione deve essere almeno di 15 minuti.
5. Selezionare o deselezionare le opzioni relative agli **aggiornamenti di Active Directory da applicare** — **Adds** (Aggiunte), **Deletes** (Cancellazioni) o **Changes** (Modifiche) — per specificare quali account di Active Directory saranno ricevuti da Secure Access e applicati al database degli account durante le successive sincronizzazioni.

   È possibile scegliere di importare utenti aggiunti o modificati oppure rimuovere account non attivi dal database di Secure Access. Lasciare queste impostazioni con i valori predefiniti per fare in modo che gli account vengano aggiornati e mantenuti sincronizzati con il server di Active Directory.
6. Gli attributi di **Assign Values from Active Directory** (Assegna valori da Active Directory) consentono di risparmiare tempo e fatica poiché assegnano attributi specifici a tutti gli utenti di un contenitore selezionato. Si tenga presente che è necessario immettere il nome dell'attributo di Active Directory, non l'etichetta del campo. Sebbene i singoli account utente possano essere aggiornati successivamente, si raccomanda di scegliere questi attributi prima di eseguire l'importazione, in modo da velocizzare la creazione degli account.

   Gli attributi **Primary PIN** (PIN principale) e **Secondary PIN** (PIN secondario) associano i PIN presenti nel server di Active Directory ai campi omonimi di Secure Access. Selezionare il PIN secondario se si desidera importare questi campi. Un PIN secondario è come una password che aggiunge un ulteriore livello di protezione e che l'utente deve inserire dal pannello comandi dell'MFP, se Enable secondary prompt è selezionato in **Configuration** (Configurazione) > **User Authentication Device Settings** (Impostazioni dispositivo di autenticazione). Digitare il nome dell'attributo per i campi PIN1 (di solito il numero della scheda) e PIN2 utilizzato sul server di Active Directory.

   Gli attributi **Primary PIN** (PIN principale) e **Secondary PIN** (PIN secondario) possono anche essere associati a indirizzi email.
7. Fare clic su **Import** (Importa) per iniziare immediatamente l'attività di importazione per la prima volta. L'importazione viene eseguita in background e può impiegare qualche minuto, conformemente alle dimensioni dell'istanza Active Directory che si sta importando.
8. Fare clic su **OK** per chiudere la finestra di dialogo. L'attività procede anche se la finestra è chiusa.
9. Dopo qualche minuto, aggiornare Secure Access Manager e verificare l'elenco di utenti per accertarsi che l'importazione degli account sia stata eseguita correttamente. Aprire anche le proprietà di un account utente e verificare che le impostazioni siano corrette.

Aggiunta di utenti tramite importazione di un file di testo

Utilizzare l'utilità **SAcmd.exe** per aggiungere, cancellare, modificare e interrogare gli account utente usando un file di testo.

Nota: questo metodo si limita a importare i dati senza sincronizzarli.

Per impostazione predefinita, Secure Access installa questa utilità nella seguente directory del server di autenticazione: **Programmi** > **Xerox** >**Secure Access** >**Tools**.

L'utilità riga di comando accetta comandi nel seguente formato:

```
SACmd  -s(Server) (Azione) (ID_Ogg.)| [(Opzioni)]
Esempio: -sTestServer adduser1 "John Smith" johns@here.com pin1 pin2
```

Eseguire il comando con un file batch:

```
SACmd  -s(Server) -f(FileBatch)
```

Comando batch SACmd

Accetta un file CSV come file batch, un file per server. Il funzionamento batch consente tutte le azioni di comando tranne il comando di interrogazione.

Nota: copiare il file csv nella cartella **Secure Access** > **Tools**.

```
[Secure Access\percorso file \Tools]\SACmd –s(Server) –f NomeFileBatch.csv
```

Formato file CSV: `(Azione), (ID_Ogg.)|Tutti,  [(Dettagli)]`

I parametri tra parentesi tonde ( ) sono obbligatori mentre quelli tra parentesi quadre [ ] sono facoltativi. Utilizzare la tabella seguente per specificare i parametri del comando.

Parametro	Variabili
Server	Specificare il nome o l'indirizzo IP del CAS.
Azione	Specificare l'azione da eseguire sull'account scegliendo tra: • add - Aggiungi utente • delete- Cancella utente • query - Interroga il database. • modify - Modifica un attributo oggetto
ID_Ogg.	Applica l'azione solo all'ID oggetto specificato. Racchiudere tra virgolette doppie gli ID oggetto che contengono uno spazio, ad esempio John Doe.
Opzioni per il comando Action (azione)	Specificare valori aggiuntivi. Racchiudere tra virgolette doppie i valori vuoti o i valori che comprendono spazi. Specificare le quantità con un punto come separatore decimale. Per l'azione modify, inserire “!” per i campi che non si desidera modificare. (user_ID): ID utente (user_ID): ID utente (email): e-mail utente

Comando Add

Add (Aggiungi) permette di aggiungere account utente. Impostare come valori tutti i campi fino all'ultimo richiesto.

Per aggiungere un utente:

```
add(ID_utente) [(nome_utente) (e-mail) (PINPrincipale) (PINSecondario)]
```

Esempio:

```
SACmd -SMyServer add JohnD "John Doe" "johnd@here.com" 123 Password
```

Comando Delete

Delete (Cancella) permette di cancellare account utente.

Per cancellare un utente:

```
delete (ID_utente)
```

Esempio:

```
SACmd -SMyServer delete JohnD
```

Comando Modify

Modify (Modifica) consente all'utente di modificare le impostazioni del database utenti. Impostare come valori tutti i campi fino all'ultimo richiesto.

Per modificare un utente:

```
modify (ID_utente) [(nome_utente) (e-mail) (PINPrincipale)
(PINSecondario)]
```

Esempio: aggiornare l'indirizzo e-mail dell'utente johnd e mantenere le altre informazioni:

```
SACmd -SMyServer modify johnd! johnd@newplace.com
```

Creazione manuale di account

È possibile utilizzare Secure Access Manager per aggiungere singoli account utente quando necessario.

1. Selezionare gli utenti, quindi fare clic sul pannello delle impostazioni e selezionare **Add user** (Aggiungi utente) dal menu.
2. Nella finestra di dialogo User Properties (Proprietà utente), immettere le informazioni richieste, descritte nella tabella seguente.

Campo	Descrizione
User ID (ID utente)	ID che ha eseguito l'accesso al database per controllare l'account.
Full Name (Nome completo)	Il nome completo dell'utente. Immettere un nome che permetta di identificare facilmente l'utente all'interno di Accounts Manager o Department Manager. Questo nome appare anche negli estratti conto e nei rapporti.
Email address (Indirizzo e-mail)	L'indirizzo e-mail viene fornito all'MFP, per attività come la scansione su e-mail.
Primary PIN (PIN principale)	Il PIN principale è di solito il numero della scheda.
Secondary PIN (PIN secondario)	Il PIN secondario funge da password e l'utente deve inserirlo sul pannello comandi dell'MFP, dopo aver fatto scorrere la scheda per l'autenticazione.
Confirm Secondary PIN (Verifica PIN secondario)	Digitare nuovamente il PIN secondario per la verifica della password.

Monitoraggio degli eventi di autenticazione

Secure Access registra ogni evento di autenticazione nel database di Secure Access. È possibile generare un log di autenticazione per qualsiasi data e visualizzare la cronologia di eventi come:

- Autenticazioni non riuscite
- Inizio sessione (autenticazione riuscita)

Ogni evento registrato contiene le seguenti informazioni:

- Source IP Address (Indirizzo IP di origine)
- Primary PIN (PIN principale)
- Validation Result (Risultato convalida)
- Server type (Tipo di server)
- Username (Nome utente)
- Indirizzo e-mail
- Server Name (Nome server)

In Secure Access Manager, fare clic su **Authentication log** (Log di autenticazione), poi fare clic con il pulsante destro del mouse su **View log by date** (Visualizza log per data). Selezionare la data, poi fare clic su **OK**.

Configurazione del servizio personalizzato Release My Documents (Rilascia i miei documenti)

Il servizio personalizzato Release My Documents (Rilascia i miei documenti) aggiorna l'MFP e aggiunge l'opzione Release My Documents alla schermata Custom Services (Servizi personalizzati) del pannello comandi. Questa schermata (mostrata di seguito) contiene i lavori di stampa in coda per l'utente. È possibile selezionare uno o più lavori e rilasciarli o eliminarli direttamente dal pannello comandi dell'MFP.

> Nota: è inoltre possibile configurare la stampa Follow-You per attivare questa funzionalità. Per istruzioni, vedere Configurazione della stampa Follow-You a pagina 32.

Se il servizio personalizzato Release My Documents non è installato, la schermata Release My Documents non è disponibile sul pannello dell'MFP e l'utente non è in grado di selezionare i singoli lavori per rilasciarli. L'utente vede, invece, una richiesta di conferma del rilascio di tutti i lavori in attesa sul server di stampa immediatamente dopo l'autenticazione.

Quando un utente esegue l'autenticazione, viene inviata una notifica a DCE per l'utente. DCE contatta il server di stampa DRE per ottenere l'elenco di tutti i documenti in coda per l'utente. La schermata Release My Documents sul pannello comandi dell'MFP viene riempita.

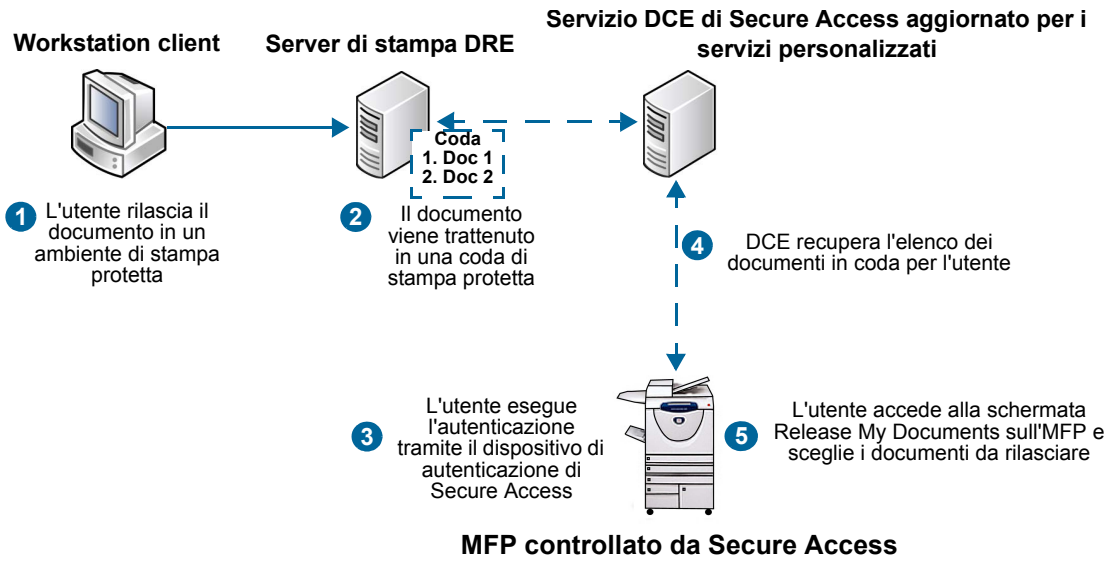


Figura 4-2: Architettura Release My Documents

Aggiunta del servizio personalizzato Release My Documents all'MFP

Se si aggiungono nuovi dispositivi a Secure Access Manager, si riceve una richiesta di installare il servizio personalizzato Release My Documents quando si sceglie OK dopo avere effettuato modifiche nella finestra Device (Dispositivo). Per istruzioni, vedere Immissione dei parametri del dispositivo a pagina 25.

> Nota: l'aggiunta del servizio personalizzato è opzionale. Se non si aggiunge il servizio, si riceve la richiesta di rilasciare i documenti durante il processo di autenticazione.

Per aggiungere il servizio personalizzato a un dispositivo già configurato in Secure Access Manager, procedere come segue:

1. In Secure Access Manager, fare clic su **Devices (Dispositivi)**.
2. Nell'elenco di dispositivi, fare clic su quello da aggiornare.
3. Nella finestra di dialogo Physical Device Summary (Riepilogo dispositivi), fare clic sul pulsante **Initialize Secure Access device** (Inizializza dispositivo Secure Access).
4. Quando si visualizza la richiesta "Do you want to enable Follow-You printing?" (Abilitare la stampa Follow-You), fare clic su **Yes** (Sì).

   Viene eseguito un file eseguibile in background per aggiornare il servizio DCE e includere la schermata Release My Documents (Rilascia i miei documenti) in Custom Services (Servizi personalizzati) sul pannello comandi dell'MFP.

Per stabilire se l'installazione è riuscita, eseguire l'autenticazione all'MFP, quindi premere **All Services** (Tutti i servizi). Si vedrà un pulsante denominato "**Release my documents**" (Rilascia i miei documenti). A seconda del modello di MFP, può essere necessario premere il pulsante **Custom Services** (Servizi personalizzati) per vedere la funzione e accedere ad essa.

Se l'installazione non riesce, il pulsante è denominato "**Servicex**', dove 'x' rappresenta un numero (es., Service4 o Service5). Per risolvere il problema, vedere Risoluzione dei problemi di installazione del servizio personalizzato Release My Documents (Rilascia i miei documenti) a pagina 50.

Flusso di lavoro utente finale per Release My Documents (Rilascia i miei documenti)

Nel grafico seguente è rappresentato il flusso di lavoro utente finale. Dopo avere inviato il lavoro di stampa, l'utente passa a un MFP controllato, effettua l'autenticazione tramite un dispositivo di autenticazione di Secure Access, quindi sceglie **Custom Services** (Servizi personalizzati) > **Release My Documents** (Rilascia i miei documenti) sul pannello comandi per accedere alle funzioni di rilascio dei documenti protetti.

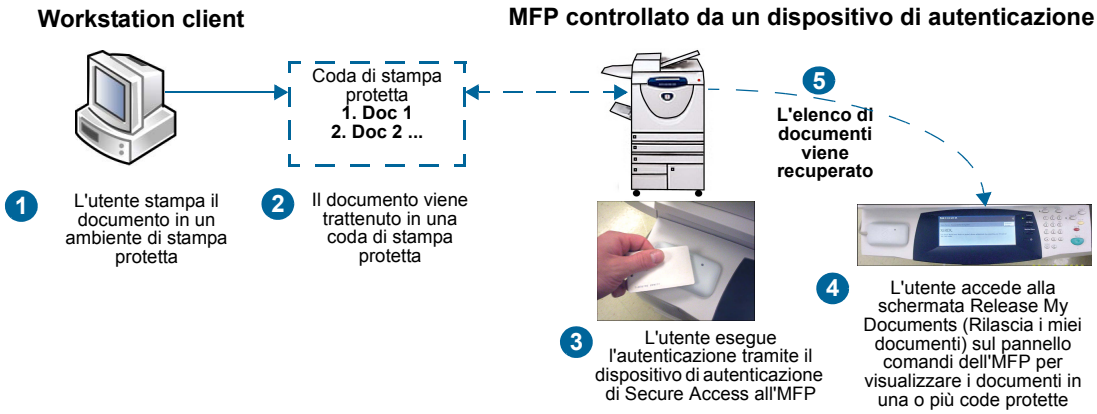


Figura 4-3: Flusso di lavoro utente finale con l'estensione Release My Documents (Rilascia i miei documenti) installata

Appendici

A

In questo capitolo:

Permessi di accesso a sincronizzazione directory

SAModifyDeletedContainerSecurity.exe modifica le autorizzazioni di accesso amministrative del contenitore degli oggetti eliminati in Windows Active Directory, in modo che Secure Access possa accedere agli oggetti durante la sincronizzazione della directory.

Per impostazione predefinita, solo gli amministratori di Active Directory dispongono del permesso di accesso. L'account Windows che esegue i servizi di Secure Access dovrà disporre di questo tipo di accesso se si desidera sincronizzare gli account eliminati tra Active Directory e Secure Access.

L'account che esegue questo comando deve essere configurato come amministratore nel dominio di Active Directory.

Vedere Utilizzo della sincronizzazione di Active Directory per importare utenti esistenti a pagina 35 per ulteriori informazioni sulla configurazione delle opzioni di sincronizzazione di Active Directory.

Per impostazione predefinita, Secure Access installa questa utilità nella seguente directory del server di autenticazione: **Programmi > Xerox > Secure Access > Tools**.

L'utilità riga di comando accetta comandi nel seguente formato:

```
SAModifyDeletedContainerSecurity.exe (-s server) [-p | {-r} -a nomeaccount]
```

I parametri tra parentesi tonde ( ) sono obbligatori mentre quelli tra parentesi quadre [ ] sono facoltativi.

Parametro	Descrizione
-s server	Il nome del server del controller di dominio di Active Directory.
-p	Visualizza i permessi attuali sul contenitore.
-r	Rimuove i permessi di accesso per il nome di account specificato.
- a nomeaccount	L'account a cui concedere l'accesso al contenitore. I permessi di accesso verranno rimossi se viene utilizzata l'opzione -r per specificarli.

Ripristino di un dispositivo di autenticazione

Utilizzare la chiave bypass per ripristinare le impostazioni predefinite sul dispositivo di autenticazione. Questa chiave viene fornita con il dispositivo e va conservata in un luogo sicuro.

1. Verificare che il dispositivo di autenticazione sia acceso.
2. Inserire la chiave bypass nell'apposito alloggiamento.
3. Ruotare la chiave di un quarto di giro verso di SÉ.
4. Ruotare la chiave indietro riportandola alla posizione iniziale.
5. Estrarre la chiave.

   Nota: se non si riporta la chiave in posizione originale prima di estrarla, il dispositivo emette un segnale acustico ogni 10 secondi.

Assegnazioni porta

Secure Access utilizza le seguenti porte per la comunicazione:

Componente	Porta
CAS	TCP 2910
DRE	TCP 2938
DCE	TCP 1824, TCP 2939, UDP 2613
Dispositivo di autenticazione di Secure Access	TCP 1234

Queste porte vengono aperte automaticamente quando si installa Secure Access. Se è necessario intervenire sulle impostazioni di Windows Firewall, è possibile aggiungere le porte all'elenco degli elementi attendibili nei computer in cui è stato installato un componente del server di Secure Access.

Soluzione dei problemi

Prima di chiamare l'assistenza, verificare questi indizi di guasto e seguire le istruzioni proposte per correggere il problema.

	Indizio	Istruzioni
1	La spia sul lettore è spenta?	**Dispositivo di autenticazione**: se la spia del lettore di schede è spenta significa che al lettore non arriva alimentazione elettrica. Dispositivo di autenticazione: verificare che il cavo del lettore sia collegato e che il connettore sia ben inserito nel connettore mini-DIN sull'unità di controllo. Se il cavo è collegato in modo corretto e la spia continua a non accendersi, passare al punto successivo. **Lettore USB:** verificare che sull'MFP sia in esecuzione il software di livello appropriato. Controllare che la spina del lettore sia inserita correttamente nell'MFP. Se il LED non si accende anche dopo aver verificato la connessione, oppure dopo un'interruzione di corrente, accendere l'MFP e provare con un lettore sostitutivo.
2	L'unità di controllo è alimentata?	**Dispositivo di autenticazione**: controllare la parte posteriore (lato del connettore) dell'unità di controllo. Se l'alimentazione è presente, la spia gialla vicino alla presa contrassegnata "Ethernet" è accesa. Verificare che il cavo dell'alimentazione sia inserito correttamente nell'alimentatore e nella presa a muro. Verificare che la presa a muro funzioni correttamente.
3	La spia del lettore è rossa e lampeggia lentamente?	**Dispositivo di autenticazione**: una luce rossa che lampeggia lentamente significa che il lettore è collegato correttamente all'unità di controllo ma che quest'ultima non è riuscita a collegarsi al server. Verificare che il cavo Ethernet sia inserito nella presa "Ethernet" dell'unità di controllo e che l'altra estremità sia inserita nella presa Ethernet a muro. **Lettore USB**: il modulo del lettore dell'MFP non è in grado di comunicare con il server. Assicurarsi che ci sia connettività di rete all'MFP e che il dispositivo sia stato inizializzato correttamente in Secure Access Manager.
4	La spia del collegamento Ethernet è spenta?	**Dispositivo di autenticazione**: se la spia verde accanto alla presa "Ethernet" è spenta, non è presente il collegamento Ethernet. Verificare che il cavo patch Ethernet sia in buone condizioni provando a collegare un cavo diverso e verificare che la presa Ethernet a muro sia attiva.
5	La spia del collegamento Ethernet è verde fissa?	**Dispositivo di autenticazione**: se la spia verde di fianco alla presa "Ethernet" è accesa e non lampeggia, significa che è presente il collegamento Ethernet ma non è in corso alcuna attività. Verificare che la presa Ethernet a muro sia collegata all'hub o all'interruttore corretto.

	Indizio	Istruzioni
6	Il dispositivo è visualizzato nell'elenco sul server di Secure Access?	**Dispositivo di autenticazione**: controllare l'elenco a discesa dei dispositivi di autenticazione sulla console di Secure Access e verificare che contenga l'indirizzo MAC del dispositivo all'origine del problema. Se l'indirizzo MAC del dispositivo (come indicato sull'etichetta del numero di serie dell'unità di controllo) non è in elenco, significa che il dispositivo non è riuscito a contattare il server. **Lettore USB:** non viene elencato alcun dispositivo di autenticazione se si utilizza un lettore USB.
7	Il dispositivo ha ricevuto un indirizzo IP?	**Dispositivo di autenticazione**: se si utilizza DHCP per configurare i dispositivi, controllare il server DHCP per verificare che sia stato assegnato un indirizzo IP (utilizzare l'indirizzo MAC per verificare) al dispositivo. Se non ha ricevuto un indirizzo IP, il dispositivo non è in grado di comunicare con il server DHCP oppure è stato configurato utilizzando la configurazione IP manuale.
8	Il dispositivo ha ricevuto un indirizzo server da DHCP?	**Dispositivo di autenticazione**: se si utilizza DHCP per configurare i dispositivi, controllare che il server DHCP imposti su 230 l'indirizzo IP del server. Verificare che il valore corrisponda all'indirizzo IP del server. Si tenga presente che il server di Secure Access non dovrebbe essere configurato tramite DHCP. Se il valore 230 non è stato impostato oppure è stato impostato in modo errato, il dispositivo non sarà in grado di contattare il server.
9	L'indirizzo IP è stato impostato manualmente?	**Dispositivo di autenticazione**: se l'indirizzo IP è stato impostato manualmente, individuare l'indirizzo nel registro e utilizzarlo per collegarsi al dispositivo tramite un Web browser. Se è impossibile collegarsi alla pagina Web con l'indirizzo IP del dispositivo, il dispositivo non è collegato in modo corretto, non è in grado di comunicare oppure l'indirizzo di rete è stato registrato in modo errato. Per eliminare la prima possibilità, collegare il dispositivo direttamente al PC utilizzando un cavo incrociato e tentare nuovamente la connessione. Una volta stabilito il collegamento, verificare che le impostazioni di rete e l'indirizzo IP del server siano corretti.

	Indizio	Istruzioni
10	Il dispositivo non è raggiungibile al relativo indirizzo IP?	**Dispositivo di autenticazione**: se non è possibile connettersi al dispositivo utilizzando l'indirizzo IP con un cavo Ethernet normale connesso alla porta Downlink, ripristinare le impostazioni predefinite per il dispositivo. A tal fine, scollegare l'alimentazione dall'unità di controllo, inserire la chiave, girarla sulla posizione "on" e collegare nuovamente l'alimentazione. Dopo 30 secondi, sospendere l'alimentazione, estrarre la chiave e collegare nuovamente l'alimentazione. Dovrebbe essere ora possibile collegare il dispositivo all'indirizzo IP predefinito 192.168.2.1. A tale scopo, assicurarsi che le impostazioni di rete del PC siano corrette. Se a questo punto è possibile collegarsi alla pagina Web del dispositivo, configurare manualmente le impostazioni di rete oppure tentare la configurazione DHCP collegando il dispositivo alla rete. Se la pagina Web è ancora irraggiungibile, l'unità di controllo potrebbe essere difettosa.
11	La spia del lettore diventa rossa e lampeggia velocemente quando si fa scorrere una scheda?	La spia rossa che lampeggia velocemente indica una lettura di scheda non valida; il server di Secure Access ha rilevato che l'ID della scheda non corrisponde a un utente valido della rete. Provare il lettore con un'altra scheda utente, il cui funzionamento è stato accertato sugli altri lettori. Se le schede non vengono lette correttamente su alcun lettore, la causa potrebbe essere dovuta alla configurazione del server; contattare il centro di assistenza tecnica per verificare la configurazione del server.
12	La spia del lettore rimane rossa quando si fa scorrere una scheda?	Se la spia del lettore non cambia durante la lettura di una scheda, significa che il lettore non ha rilevato la scheda. La scheda magnetica potrebbe essere stata codificata con uno standard diverso oppure inserita alla rovescia o per il verso errato; una scheda di prossimità o una smart card senza contatto potrebbero non essere state avvicinate abbastanza al lettore oppure essere di un tipo non corretto. Verificare che la scheda sia stata fatta scorrere correttamente. Se la stessa scheda funziona su altri lettori dello stesso sito, potrebbe trattarsi di un guasto al modulo del lettore. Se la scheda non funziona su altri lettori, controllarla con il rivenditore e verificare che sia riportata nell'elenco delle schede compatibili con il lettore.
13	La spia del lettore diventa verde quando si fa scorrere una scheda?	La spia rossa significa che è in corso una sessione di Secure Access. Ciò significa che la scheda è stata letta in modo corretto e corrisponde a un utente valido di Secure Access. Se la luce diventa verde, ma l'MFP è disattivato, il dispositivo di Secure Access potrebbe essere associato a un MFP errato. Controllare la configurazione del dispositivo nella console di Secure Access per verificare che il dispositivo di Secure Access sia associato all'MFP corretto.

	Indizio	Istruzioni
14	Il pannello comandi dell'MFP è sempre sbloccato?	Il pannello comandi dell'MFP può essere bloccato solo su dispositivi che supportano Xerox Secure Access. Verificare che il modello che si tenta di utilizzare sia supportato e che abbia installata la corretta versione di firmware.
15	Che cosa significano i messaggi di errore "Failed to enable Follow-You printing" (Impossibile abilitare la stampa Follow-You) e "Failed to enable Follow-You printing: no site specified" (Impossibile abilitare la stampa Follow-You: nessun sito specificato)?	Questi messaggi appaiono se il servizio personalizzato Release My Documents (Rilascia i miei documenti) non viene installato correttamente. Vedere Risoluzione dei problemi di installazione del servizio personalizzato Release My Documents (Rilascia i miei documenti) a pagina 50.
16	I messaggi del dispositivo (titoli e prompt di accesso) non vengono visualizzati sul pannello comandi dell'MFP	Aprire il dispositivo in Secure Access Manager. Fare clic sul pulsante **Initialize SecureAccess device** (Inizializza il dispositivo SecureAccess). Sul pannello comandi dell'MFP dovrebbero essere visualizzati i messaggi corretti.
17	La spia del lettore è verde fissa dopo il riavvio dell'MFP?	**Lettore USB:** verificare che nell'MFP sia in esecuzione il software di livello appropriato.

Risoluzione dei problemi di installazione del servizio personalizzato Release My Documents (Rilascia i miei documenti)

Se il pulsante 'Release my documents' (Rilascia i miei documenti) non è visualizzato nella schermata Custom Services (Servizi personalizzati) sull'MFP, può essere necessario eseguire il file di installazione con parametri specifici. Se DNS non consente all'MFP di risolvere il nome host del server in cui è in esecuzione DCE, lo strumento non sarà in grado di registrare i dispositivi correttamente. Per i parametri specifici da utilizzare per l'installazione, consultare la tabella seguente.

Il file eseguibile dell'estensione Release My Documents (Rilascia i miei documenti) si trova nella cartella Tools (Strumenti) della macchina che ospita CAS (Core Authentication Server - Server di autenticazione principale). Assicurarsi di disporre di autorizzazioni di amministratore sul server che ospita il servizio CAS e DCE per installare i file richiesti.

1. Aprire un prompt dei comandi e modificare il percorso alla cartella Tools. Ad esempio:
   c:\Programmi\Xerox\SecureAccess\Tools\
2. Eseguire il file eseguibile con i parametri delineati nella tabella seguente:
   saxeroxeipregistration.exe

   Nota: è possibile eseguire il comando con parametri che consentono di sovrascrivere l'installazione non riuscita, senza dover prima annullare la registrazione dell'estensione.

Parametro	Risultato
-i	Identifica l'indirizzo IP dell'MFP che riceverà l'estensione Release My Documents (Rilascia i miei documenti)
-r	Registra il server DCE specificato sul dispositivo MFP specificato
-d	Annulla la registrazione dell'estensione Release My Documents (Rilascia i miei documenti) dal dispositivo MFP specificato
-v	Visualizza le informazioni registrate. Eseguire questo comando per confermare l'installazione dell'estensione.
-u	Nome utente per l'autorizzazione ad aggiornare il dispositivo
-p	Password per l'autorizzazione ad aggiornare il dispositivo
-c	Enumera i dispositivi dal server CAS specificato e registra l'estensione su tutti gli MFP Xerox trovati nell'elenco dei dispositivi
/?	Visualizza un elenco di parametri per questa estensione

Esempio:

```
saxeroxeipregistration.exe -i 192.168.97.180 -r 192.168.97.137
```

Indirizzo IP dell'MFP **Indirizzo IP DCE**

Risultato: registra l'aggiornamento con il server DCE specificato e installa l'estensione Release My Documents (Rilascia i miei documenti) in un singolo MFP.

Accesso alla schermata Release My Documents (Rilascia i miei documenti)

Se è installata l'estensione Release My Documents (vedere Guida all'installazione), gli utenti possono accedere alla schermata Release My Documents (Rilascia i miei documenti) e visualizzare i lavori di stampa da una o più code protette e rilasciare o eliminare i lavori.

1. Dopo l'autenticazione, premere **All Services** (Tutti i servizi).
2. Premere **Custom Services** (Servizi personalizzati).
3. Premere **Release My Documents** (Rilascia i miei documenti).
4. Tutti i documenti trattenuti per l'utente nel server di stampa locale sono visualizzati nella schermata. I pulsanti sono descritti nella tabella seguente.

Pulsante	Funzione
Stampa	Selezionare uno o più documenti nell'elenco, quindi premere **Print** (Stampa) per stampare i documenti ed eliminare i lavori dall'elenco. Se il numero di copie è impostato su più di 1, fare clic su **OK** per confermare la richiesta.
Print & Save (Stampa e salva)	Selezionare uno o più documenti nell'elenco, quindi premere **Print & Save** (Stampa e salva) per stampare i documenti senza eliminare i lavori dall'elenco. Se il numero di copie è impostato su più di 1, fare clic su **OK** per confermare la richiesta.
Comando Delete	Selezionare uno o più documenti nell'elenco, quindi premere **Delete** (Elimina) per eliminare i lavori dalla coda senza stamparli.
Select All (Seleziona tutto)	Seleziona tutti i lavori inclusi nell'elenco.
Refresh (Aggiorna)	Contatta il server DCE per stabilire se ci sono lavori in sospeso da aggiungere all'elenco per l'utente corrente. I documenti eventualmente trovati vengono aggiunti in fondo all'elenco.
Details (Dettagli)	Selezionare un documento incluso nell'elenco, quindi premere **Details** (Dettagli) per visualizzare i dettagli quali nome lavoro, data e ora di invio, nome della stampante cui è stato inviato il lavoro in origine e workstation client da cui è stato originato il lavoro.
Exit (Esci)	Riporta alla schermata Custom Services (Servizi personalizzati).

Impostazione del numero di copie per un lavoro di stampa

Dopo l'autenticazione, gli utenti possono utilizzare il tastierino numerico dell'MFP per immettere il numero di copie da stampare. Se il numero di copie è impostato su più di 1, quando si premono i pulsanti **Print** (Stampa) o **Print & Save** (Stampa e salva) viene visualizzata una finestra di conferma. Per stampare il numero di copie corrente, premere **OK**. Per modificare il numero, premere **Cancel** (Annulla), quindi digitare il numero di copie corretto utilizzando il tastierino numerico sul pannello comandi dell'MFP. Premere **Print** (Stampa) o **Print & Save** (Stampa e salva) per rilasciare il lavoro.

Se il lavoro di stampa originale è stato stampato in due copie utilizzando questa funzione, selezionando 2 si ottengono 4 copie dell'originale.

Termine di una sessione utente

Nella schermata Release My Documents (Rilascia i miei documenti), premere prima **Exit** (Esci) per ritornare alla schermata Custom Services (Servizi personalizzati). Premere **Close** (Chiudi) per ritornare alla schermata principale sul pannello comandi. Per chiudere completamente la sessione attiva, premere il pulsante **Clear All** (Cancella tutto) accanto alla tastiera del pannello e scegliere **Log out** nella finestra di dialogo di conferma.