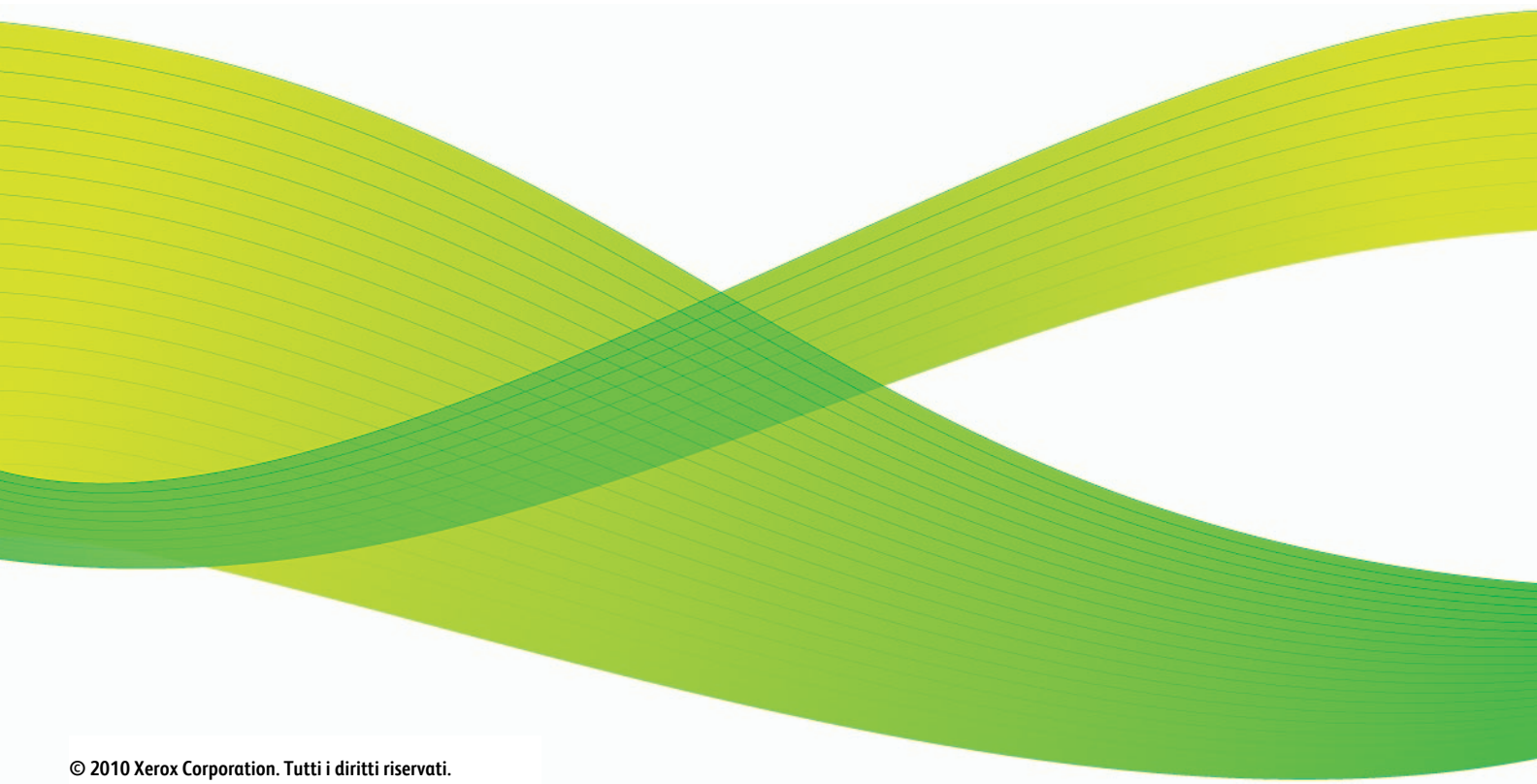
Version 1.6, October 2010

# Xerox Secure Access Unified ID System®

## Guida all'installazione



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

# Indice generale

# 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 a causa delle implicazioni 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

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

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

# 2 Elenco di controllo per l'installazione

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<br>(*) 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: Preparazione della rete e del database | * | * |
| 3. Capitolo 4, Installazione del server di Secure Access: Eseguire la 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 | * | * |
| 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 dell'installazione

In questo capitolo:



Questa guida illustra come installare il software del server Xerox Secure Access Unified ID System™ ed eseguire la configurazione fisica dei dispositivi di autenticazione. Prima di configurare i dispositivi di autenticazione è necessario installare il server.

Una volta installato correttamente il server Secure Access, consultare la Guida all'amministrazione di Secure Access per istruzioni complete sull'installazione del dispositivo e sulla configurazione del software.

Questo capitolo fornisce informazioni su:

- i componenti che costituiscono il server Secure Access
- i requisiti di sistema

# Componenti di Secure Access

Il prodotto Xerox Secure Access Unified ID System™ (d'ora in avanti definito semplicemente "Secure Access") è una soluzione hardware e software composta da:

- Software del server Secure Access che gestisce il database utenti e contiene servizi che comunicano con gli MFP (stampanti multifunzione) e i dispositivi di autenticazione di Secure Access.
- Un dispositivo di autenticazione di Secure Access, che comprende un lettore di schede e controlla l'accesso agli MFP Xerox.

  oppure
- Un lettore di schede USB di Secure Access

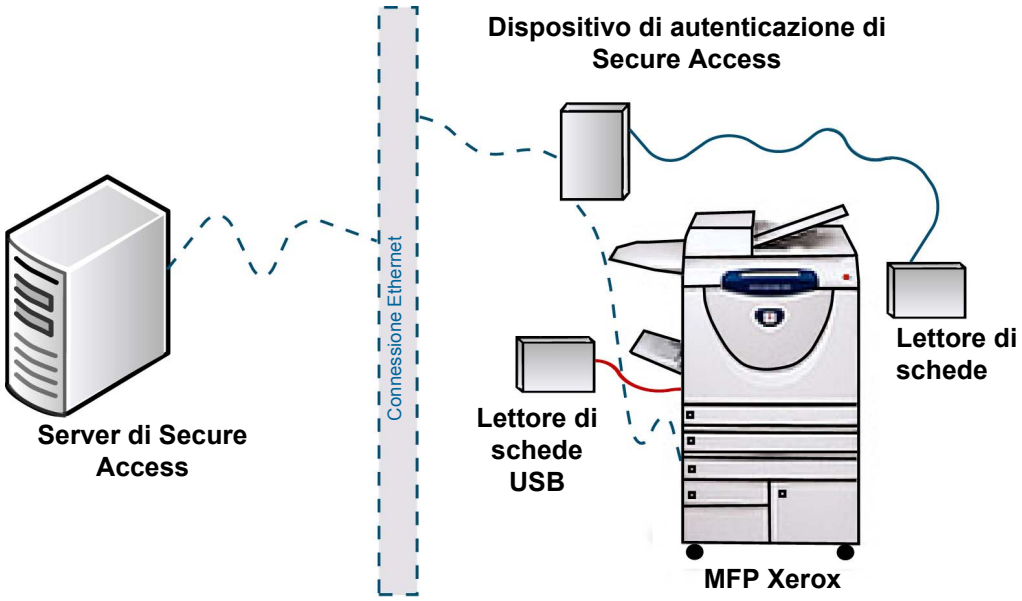



**Figura 3-1:** Componenti di Secure Access

L'installazione di ciascun server Secure Access richiede almeno tre servizi:

- 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)

Inoltre, occorre installare Secure Access Manager, uno strumento amministrativo utilizzato per attivare la comunicazione tra i vari componenti di Secure Access.

## 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. Vedere Requisiti del server di Secure Access a pagina 18 per informazioni sui database supportati.

## 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.

## 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.

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

Per tratenere i lavori di stampa 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.

È inoltre possibile aggiungere il servizio personalizzato Release My Documents (Accetta i miei documenti) all'MFP. Si tratta di un servizio che consente agli utenti di accedere alla coda di stampa protetta direttamente dal pannello comandi dell'MFP. Per istruzioni di configurazione, vedere Guida all'amministrazione di Xerox Secure Access.

## Configurazione multiserver

Un'installazione in cui tutti i servizi sono installati sullo stesso server viene definita installazione "locale". Alcuni installazioni possono però richiedere più di un server per distribuire il carico di gestione. Un'installazione in cui i servizi sono distribuiti su due o più server viene definita installazione "remota".

Sia che venga usata un'installazione singola o una multipla, il DRE e il DCE devono sempre essere sullo stesso server.

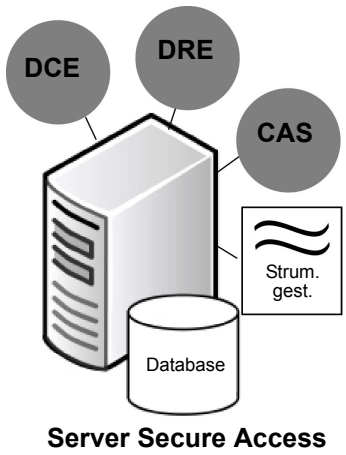



**Figura 3-2:** Esempio di installazione locale

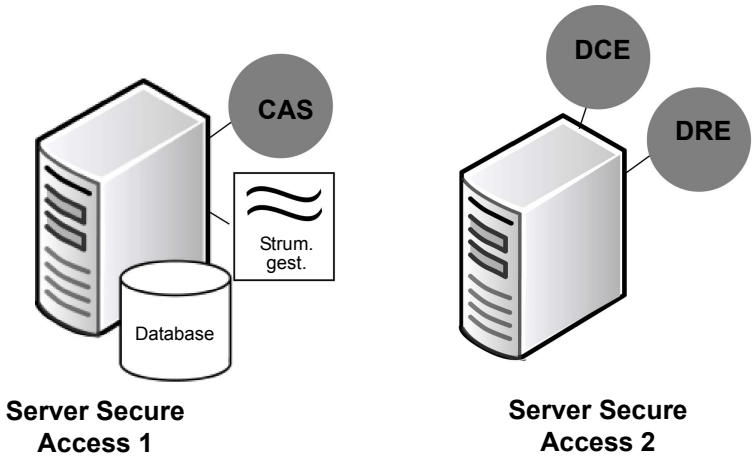



**Figura 3-3:** Esempio di installazione remota

Inoltre, se Secure Access deve gestire numerosi MFP, è possibile installare più server di stampa DRE per bilanciare il carico di comunicazione.

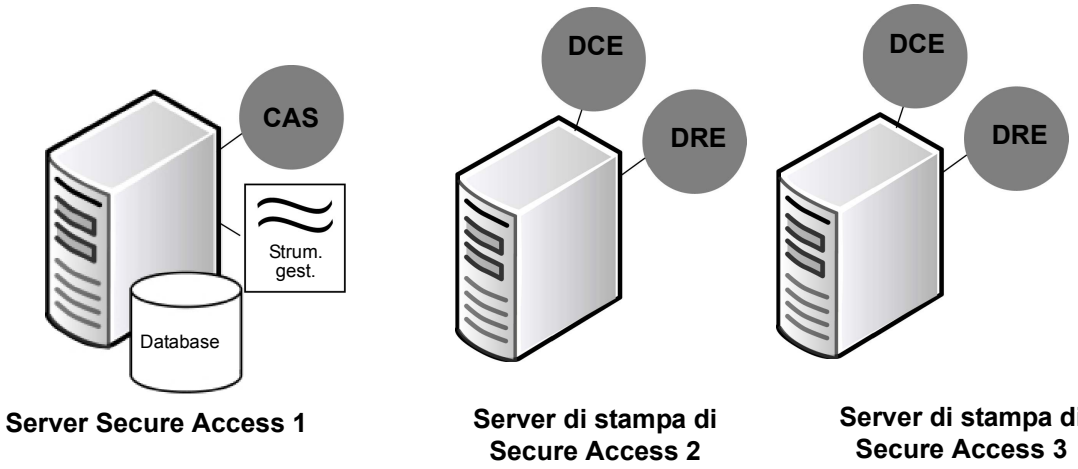



**Figura 3-4:** Installazione di più server di stampa

Vedere Esecuzione della procedura di installazione guidata a pagina 23 per maggiori dettagli sull'installazione e la configurazione di più server. La procedura di installazione guidata consente di selezionare solo i componenti che si desidera installare su ciascuna macchina. I servizi DRE e DCE possono essere installati su server multipli, ma sempre entrambi sullo stesso server.

# Requisiti del server di Secure Access

Prima di installare Secure Access, accertarsi che i server che si intende utilizzare soddisfino i requisiti operativi minimi illustrati di seguito.

La tabella sottostante illustra solo i requisiti operativi minimi. Per ottimizzare le prestazioni in ambienti ad alto volume di stampe sono necessari più spazio su disco e memoria e un processore più veloce.

| Componente | Requisiti minimi |
|---|---|
| Hardware | • Procssore: Pentium III, Athlon o superiore<br>• Memoria di sistema: 512 MB minimo<br>• Spazio su disco per l'applicazione: 100 MB<br>• Spazio su disco per l'applicazione: 20 MB<br>• Risoluzione video: 1024 x 768 |
| Sistema operativo per CAS/DCE/DRE | Uno tra:<br>• Windows Server 2003 (32 bit)<br>• Windows XP Professional (32 bit soltanto)[1]<br>• Windows Server 2008 (32 e 64 bit), 2008 R2 (64 bit)<br>Nota: Prima di installare il software del server Secure Access, è necessario che siano installati tutti gli aggiornamenti critici per il sistema operativo in uso. |
| Database | • Microsoft SQL Server 2005 Express[2]<br>• Microsoft SQL Server 2005 Express (64 bit)<br>Nota: Secure Access non può essere installato su un server che gestisce un'applicazione MSDB quale FreeFlow™ SMARTsend™ poiché questi database entrano in conflitto con il database del server SQL. |

[1] Se si intende installare il servizio CAS su un server Windows XP Professional che non è connesso a un dominio, attenersi alle istruzioni riportate a pagina 15 per configurare le impostazioni di autenticazione utente.

[2] Per eseguire SQL Server 2005 Express su Windows Server 2008 o 2008 R" è necessarrio Windows Service Pack 2 (SP2) o una versione successiva.

## Impostazioni di autenticazione utente in Windows XP Professional

Se si intende installare il servizio CAS di Secure Access su una piattaforma Microsoft Windows XP Professional e il computer non è connesso a un domino, occorre cambiare le impostazioni di protezione di Windows XP per consentire l'accesso agli account utente denominati.

Per impostazione predefinita, in Windows XP Professional gli accessi di rete che utilizzano gli account locali sono associati automaticamente all'account Guest. Modificare questa impostazione se si preferisce che gli utenti eseguano l'autenticazione con le proprie credenziali.

Completare questi passaggi prima di eseguire l'installazione guidata di Secure Access.

1. Aprire la finestra Impostazioni protezione locale sul computer su cui si intende installare il servizio CAS.
2. Nel riquadro di spostamento sinistro, fare doppio clic su **Criteri locali**, quindi fare doppio clic su **Opzioni di protezione**.
3. Nel riquadro a destra, scorrere verso il basso fino a **Accesso di rete: modello di condivisione e sicurezza per account locali**.
4. Fare doppio clic su questa voce e scegliere **Classico: l'utente locale esegue l'autenticazione con le proprie credenziali**.
5. Fare clic su **Applica** e poi su **OK** per chiudere la finestra.
6. Chiudere le Impostazioni di sicurezza locale.

# Requisiti del componente hardware di Secure Access

Assicurarsi di disporre dell'hardware fornito:

**Configurazione 1**

- Alimentatore
- Cavo di alimentazione
- Chiave di bypass (chiave metallica utilizzata per ripristinare le impostazioni predefinite del dispositivo) Vedere Ripristino di un dispositivo di identificazione nelle appendici della Guida all'amministrazione.
- Cavo di rete Ethernet 10/100 Base-T
- Lettore di schede

oppure

**Configurazione 2**

- Lettore di schede USB di Secure Access.

## Lettori schede supportati

Secure Access supporta i seguenti lettori schede:

- ABA Magstripe
- Mifare (compresi i lettori HID iCLASS)
- Legic
- HID 125 kHz
- Indala
- EM Marin
- Hitag

# Installazione del server di Secure Access

4

In questo capitolo:



Questa sezione fornisce istruzioni sull'utilizzo dell'installazione guidata del server di Secure Access. Assicurarsi di seguire attentamente le istruzioni e che i server soddisfino i requisiti operativi minimi delineati in Requisiti del server di Secure Access a pagina 18.

In questo capitolo vengono fornite informazioni per:

- preparare la rete e il database prima di eseguire l'installazione
- utilizzare la procedura guidata di installazione per selezionare i componenti da installare per il server di Secure Access

# Preparazione della rete e del database

Sebbene la procedura di installazione di Secure Access sia molto semplice, prima di lanciare la procedura eseguire le operazioni sottoelencate:

1. Pianificare i ruoli del sistema.
2. Abilitare Xerox Secure Access sull'MFP utilizzando il software CentreWare Internet Services.

   Nota:

   - Utilizzando un browser Web, accedere a CentreWare Internet Services sull'MFP. Accedere alla pagina per abilitare Xerox Secure Access. Questa impostazione richiederà l'abilitazione di SSL e la creazione di un certificato. Per ulteriori informazioni, consultare il CD di amministrazione del sistema MFP.
   - Per i lettori di schede USB, l'MFP potrebbe richiedere un aggiornamento software. A tale scopo, rivolgersi al rappresentante Xerox o andare alla pagina di supporto per il modello di MFP in uso spostandosi a "Supporto e Driver" su www.xerox.com
3. Stabilire la destinazione di installazione per ciascun componente di Secure Access.

   Nota: prima di implementare Secure Access sulla rete, assicurarsi di avere privilegi di Amministratore su tutte le macchine da installare e configurare.
4. Verificare che la propria configurazione di rete sia predisposta per la comunicazione tra i componenti di Secure Access.
5. Utilizzando gli aggiornamenti di Windows, assicurarsi che siano stati installati tutti i necessari aggiornamenti principali al sistema operativo.
6. Installare Microsoft .NET Framework 2.0.

   Nota: fare riferimento al sito Web di Microsoft per un elenco completo dei prerequisiti di installazione per SQL Server 2005 o 2008 Express Edition.
7. Installare e configurare il database.

   Nota: se si utilizza SQL Server 2005 o 2008 Express, è necessario configuare il database per poter usare Windows Authentication Mode. Secure Access non supporta autenticazioni miste.

# Esecuzione della procedura di installazione guidata

Durante l'installazione di Secure Access, la procedura guidata di installazione consente di selezionare le funzioni da installare per ciascun server. Qualora si stiano distribuendo i componenti su più server, è necessario eseguire la procedura guidata su ciascun dispositivo server, selezionando solo i componenti richiesti. Qualora si stia eseguendo l'installazione su un solo server, è sufficiente eseguire la procedura guidata una sola volta.

Non dimenticare che ciascuna implementazione richiede almeno un componente CAS, DCE, DRE e Secure Access Manager.

1. Prima di eseguire l'installazione, assicurarsi che i passaggi della Sezione 1, "Preparazione della rete e del database," siano stati completati.
2. Chiudere tutte le applicazioni del server prima di eseguire l'installazione di Secure Access.
3. Avviare la procedura guidata di installazione di Secure Access.
   - Se si esegue l'installazione dal CD di Secure Access, selezionare **32-bit Setup.exe** per iniziare l'installazione su un server a 32 bt o selezionare **64-bit Setup.exe** per iniziare l'installazione su un server a 64 bit.

   oppure

   - Se si sta eseguendo l'installazione da un'origine elettronica, scaricare il file ZIP e eseguire il file **Setup.exe** per server a 32 o 64 bit.

   Nota: se si tenta di eseguire il file setup.exe e si riceve un messaggio di errore, potrebbe essere necessario aggiornare la versione del programma di installazione Microsoft. Visitare il sito Web di Microsoft e scaricare e installare la versione più recente del programma di installazione Microsoft per il sistema operativo in uso.
4. Nella schermata di benvenuto, fare clic su **Avanti** per iniziare la procedura di installazione.
5. Leggere il contratto di licenza del software e fare clic su **Accetto**, quindi fare clic su **Avanti**.
6. Scegliere le opzioni da installare nella macchina e fare clic su **Avanti**.

   Per impostazione predefinita, tutti i componenti sono selezionati. Selezionare solo i componenti richiesti su questo specifico server. Ad esempio, se questo server funge da server di stampa, installare solo i componenti DRE e DCE. Eseguire il programma di installazione su un altro server per installare i componenti restanti in base alle esigenze.

   Nota: leggere le descrizioni dei componenti fornite nella sezione Componenti di Secure Access a pagina 14 prima di installare ciascun componente. Tali informazioni aiuteranno a stabilire la modalità di implementazione dei componenti più adatta alle esigenze della propria organizzazione.
7. Scegliere la lingua dell'interfaccia desiderata nella schermata **Select Language** (Seleziona lingua). Questa è la lingua che verrà utilizzata soltanto in Secure Access Manager. La lingua utilizzata nei messaggi visualizzati sul pannello comandi dell'MFP è definita dalle impostazioni dell'MFP.

8. Nella schermata **Instance for SQL Express** (Istanza per SQL Express), immettere il nome dell'istanza di database creata per il database SQL Express. Fare clic su **Avanti**.

   Nota: il nome istanza immesso in questo campo DEVE corrispondere al nome istanza creato per il database di Secure Access quando è stato installato SQL Express. Senza il nome istanza corretto l'installazione non può procedere. Se è stata eseguita un'installazione SQL Express standard e non è stato modificato nessuno dei parametri di default, lasciare questa impostazione come SQLEXPRESS e fare clic su Avanti.

9. Specificare un **nome utente** e una **password** per i servizi nella schermata **User Name for Services** (Nome utente per i servizi).

   Quando si installano i componenti su più macchine è necessario immettere le stesse credenziali utente per ciascuna installazione. Tali credenziali vengono utilizzate per avviare ed eseguire tutti i servizi. Se non vengono immesse le stesse credenziali su tutti i componenti, il CAS non risponderà alle richieste da parte del DCE o del DRE.

   Gli account del dominio devono utilizzare il nome di dominio (ad esempio, dominio\nome utente).

   Sebbene questo account non richieda privilegi amministrativi sul server di Secure Access, l'account deve avere privilegi di Operatore di stampa per consentire al DRE di elaborare le richieste di stampa.

10. Immettere il nome del server di autenticazione di Xerox Secure Access.

    Quando si avvia Secure Access Manager, è necessario identificare il CAS usando il nome immesso qui.

11. Fare clic su **Installa** per avviare la procedura d'installazione. La procedura guidata di installazione copia file, imposta servizi e crea collegamenti a Secure Access Manager.

12. Al termine della procedura, fare clic su **Fine** per uscire dalla procedura guidata di installazione.

13. L'installazione del server di Secure Access è ora completa. Per la configurazione dell'hardware di Secure Access, vedere il capitolo 5.

# Aggiornamento di Secure Access

Sia che si esegua un aggiornamento a fasi o che si aggiornino tutti i componenti durante un tempo di inattività programmato, di seguito sono riportate le istruzioni alla procedura di installazione guidata degli aggiornamenti di Secure Access.

Nota: si consiglia di eseguire il back up del proprio database prima di eseguire gli aggiornamenti.

Durante l'aggiornamento di Secure Access l'installazione guidata individua i componenti di Secure Access già installati nella macchina (ad esempio, il database). Questi componenti saranno selezionati automaticamente nell'installazione guidata. È possibile mantenere le impostazioni predefinite o selezionare ulteriori componenti da installare.

Per eseguire l'aggiornamento di Secure Access, eseguire le operazioni seguenti:

1. Chiudere tutte le applicazioni del server prima di eseguire l'installazione di Secure Access.
2. Avviare la procedura guidata di installazione di Secure Access.
   - Se si esegue l'installazione dal CD di Secure Access, selezionare **32-bit Setup.exe** per iniziare l'installazione su un server a 32 bt o selezionare **64-bit Setup.exe** per iniziare l'installazione su un server a 64 bit.

   oppure

   - Se si sta eseguendo l'installazione da un'origine elettronica, scaricare il file ZIP e eseguire il file **Setup.exe** per server a 32 o 64 bit.

   Nota: se si tenta di eseguire il file setup.exe e si riceve un messaggio di errore, potrebbe essere necessario aggiornare la versione del programma di installazione Microsoft. Visitare il sito Web di Microsoft e scaricare e installare la versione più recente del programma di installazione Microsoft per il sistema operativo in uso.
3. Nella schermata di benvenuto, fare clic su **Avanti** per iniziare la procedura di installazione.
4. Leggere il contratto di licenza del software e fare clic su **Accetto**, quindi fare clic su **Avanti**.
5. Scegliere le opzioni da installare nella macchina e fare clic su **Avanti**.

   Per impostazione predefinita, tutti i componenti sono selezionati. Selezionare solo i componenti richiesti su questo specifico server. Ad esempio, se questo server funge da server di stampa, installare solo i componenti DRE e DCE. Eseguire il programma di installazione su un altro server per installare i componenti restanti in base alle esigenze.
6. Immettere il nome del server di autenticazione di Xerox Secure Access.
7. Fare clic su **Finish** (Fine) per uscire dall'installazione guidata.

L'installazione degli aggiornamenti del server di Secure Access è ora completa. Per la configurazione dell'hardware di Secure Access, vedere il capitolo 5.

# 5 Configurazione dell'hardware di Secure Access

In questo capitolo:



Questo capitolo fornisce le istruzioni per eseguire la configurazione hardware di Secure Access. Prima di configurare l'hardware di Secure Access è necessario aver installato il software Secure Access Server. Seguire le istruzioni fornite nel Capitolo 4 per installare il server di Secure Access.

**Se si utilizza un lettore di schede USB per Secure Access, passare alla pagina 33.**.

1. Impostare l'indirizzo IP di ciascun dispositivo di autenticazione.
2. Montare il dispositivo di autenticazione di Secure Access sopra o accanto all'MFP.
3. Collegare i cavi di alimentazione, seriale, di espansione e del lettore di schede.

# Configurazione dell'indirizzo IP del dispositivo di autenticazione

**ATTENZIONE:** Se non si utilizza un server DHCP per assegnare gli indirizzi IP, NON COLLEGARE IL DISPOSITIVO DI AUTENTICAZIONE ALLA RETE finché non è stato impostato manualmente l'indirizzo IP. Vedere Assegnazione manuale dell'indirizzo IP a pagina 29.

Per impostazione predefinita, i dispositivi di autenticazione di Secure Access sono configurati per la comunicazione DHCP. È necessario assegnare un indirizzo IP a ciascun dispositivo di autenticazione e configurare l'indirizzo IP server del componente DCE. Esistono due metodi per assegnare l'indirizzo IP:

- È possibile utilizzare un server DHCP per assegnare gli indirizzi. Consultare Configurazione del server DHCP per individuare i dispositivi di autenticazione a pagina 28.
- Se non si utilizza un server DHCP, o se si preferisce non impostare l'opzione 230 sul proprio server DHCP, è necessario utilizzare l'applicazione Authentication Device Web Admin per impostare gli indirizzi manualmente. Consultare Assegnazione manuale dell'indirizzo IP a pagina 29.

## Configurazione del server DHCP per individuare i dispositivi di autenticazione

Le istruzioni seguenti sono specifiche per un server DHCP Windows. Se il server DHCP viene eseguito su una piattaforma diversa (ad esempio server DHCP UNIX, Linux, OS X server, OpenVMS, AS/400), configurare il server DHCP in modo che passi l'indirizzo server DCE al valore 230.

Nota: per ulteriori informazioni tecniche sull'utilizzo di DHCP per assegnare gli indirizzi IP ai dispositivi di autenticazione di Secure Access, vedere Setting the Secure Access Authentication Device IP Address White Paper (Impostazione dell'indirizzo IP del dispositivo di autenticazione di Secure Access) che si trova in www.xerox.com.

1. In Strumenti di amministrazione di Windows, aprire la console di gestione delle finestre DCHP.
2. Selezionare il nodo principale del server DHCP.
3. Dal menu **Azione**, selezionare **Definisci opzioni predefinite**.
4. Dall'elenco a discesa **Classe opzione**, selezionare **Opzioni DHCP standard**.
5. Nella sezione **Nome opzione**, fare clic su **Aggiungi**.
   a. Nel campo **Nome**, digitare: Xerox Secure Access

   Nota: il campo **Nome** è necessario per l'identificazione.

   b. Dall'elenco a discesa **Tipo di dati**, selezionare Stringa.
   c. Nel campo **Codice**, digitare 230.
   d. Nel campo **Descrizione**, digitare: Secure Access
6. Fare clic su **OK**.
7. Nella sezione **Valore stringa**, immettere EQ;A;<indirizzo IP server DCE> nel campo **Stringa**, dove <indirizzo IP server DCE> è l'indirizzo IP del server DCE.
8. Espandere il nodo **Ambito** e selezionare **Opzioni ambito**.

9. Dal menu **Azione**, selezionare **Configura opzioni**.
10. Selezionare **230**.
11. Fare clic su **OK** per salvare le modifiche.

## Assegnazione manuale dell'indirizzo IP

Seguire queste istruzioni soltanto se non si utilizza un server DHCP per impostare l'indirizzo IP del dispositivo di autenticazione OPPURE se si utilizza un server DHCP ma si preferisce utilizzare indirizzi IP statici anziché l'opzione 230.

La prima volta che viene acceso, il dispositivo di autenticazione cerca un server DHCP per ottenere un indirizzo IP. Se non rileva alcun server DHCP, il dispositivo passa alla comunicazione statica e utilizza l'indirizzo IP statico 192.168.2.1. È possibile utilizzare un cavo Ethernet per connettere un sistema (ad esempio un portatile) a ciascun dispositivo di autenticazione e utilizzare un'applicazione di amministrazione Web per cambiare l'indirizzo IP e immettere l'indirizzo IP del server DCE.

Prima di iniziare, stampare la scheda di configurazione a pagina 32. Utilizzare questa scheda per annotare gli indirizzi IP assegnati a ciascun dispositivo di autenticazione.

### Configurazione del portatile:

Prima di poter accedere all'applicazione di gestione Web, il sistema che gestisce l'applicazione deve riconoscere l'indirizzo IP statico.

1. Sul sistema (portatile) che gestirà l'applicazione di gestione Web, selezionare **Connessioni di rete** > **Connessione alla rete locale** > **Proprietà**.
2. Fare doppio clic su **Proprietà Internet** (TCP/IP) e fare clic su **Avanzate**.
3. Nella sezione Indirizzi IP, fare clic su **Aggiungi**.
4. Immettere quanto segue:
   Indirizzo IP: 192.168.2.x (dove x è un IP non assegnato)
   Subnet mask: 255.255.255.0
5. Fare clic su **Aggiungi** per salvare le modifiche.

### Utilizzo dell'applicazione di gestione Web per impostare gli indirizzi IP:

Eseguire la seguente procedura su ciascun dispositivo di autenticazione.

1. Utilizzare un cavo Ethernet standard per collegare un portatile alla porta Downlink sul dispositivo di autenticazione di Secure Access.
2. Per accendere il dispositivo di autenticazione, collegare un'estremità del cavo di alimentazione CA al dispositivo, quindi collegare l'altra estremità a una presa disponibile.
3. Avviare un browser Web e digitare 192.168.2.1 nel campo Indirizzo.
   Questo è l'indirizzo IP assegnato per default al dispositivo di autenticazione di Secure Access.
   Nota: per il francese, selezionare il collegamento fornito.
4. Fare clic sul collegamento **Configure** (Configura) in cima alla pagina.

5. Immettere i seguenti codici per accedere:

   Nome utente: deviceadmin

   Password: pc_passwd

6. Modificare la password utilizzata per accedere all'applicazione di gestione Web. È possibile ripristinare la password in qualunque momento, ma è necessario ricordarsi di modificarla rispetto all'impostazione di default prima che il sistema Secure Access entri in funzione.
7. Nella sezione **Configure Xerox Secure Access Authentication Device** (Configura dispositivo di autenticazione di Xerox Secure Access), scegliere Static IP (IP statico) nel campo **Addressing mode** (Modo assegnazione indirizzi).
8. Immettere un indirizzo IP statico nel campo **IP Address** (Indirizzo IP) per impostare l'indirizzo di questo dispositivo di autenticazione.
9. Nella sezione **Configure server** (Configurazione server), immettere l'indirizzo IP del server DCE nel campo Server IP Address (Indirizzo IP server).
10. Fare clic sul pulsante **Update Configuration** (Aggiorna configurazione) visualizzato sotto i campi di Configure Server (Configurazione server).
11. Fare clic su **Restart** (Riavvia) nella parte superiore della pagina e fare clic su "Click here to confirm restart" (Fare clic qui per confermare il riavvio) per riavviare il terminale.

Ripetere questa procedura per ciascun dispositivo di autenticazione di Secure Access che si sta installando.

Nota: al termine, riconfigurare le proprietà Internet del portatile.

# Montaggio del dispositivo di autenticazione di Secure Access

Scheda di configurazione a pagina 35. Durante la procedura di installazione, compilare le colonne della scheda. Queste informazioni sono necessarie per configurare la comunicazione tra i dispositivi sul server di Secure Access.

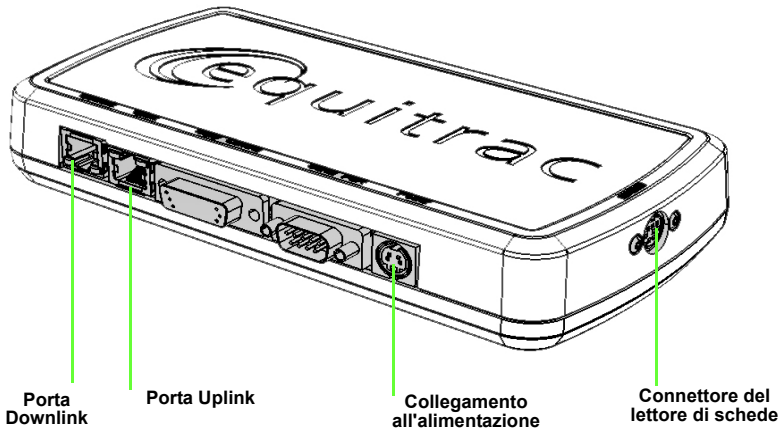

1. Appoggiare il dispositivo di autenticazione sul pavimento, dietro e accanto al lato di ingresso dell'MFP. **Collocare il dispositivo in un punto che non sia d'intralcio, ma a una distanza tale da consentire di collegare il cavo (180 cm circa) al lettore di schede**.
2. Installare il lettore di schede sul ripiano alla sinistra del pannello comandi dell'MFP utilizzando la striscia di velcro fornita. Se si dispone della pinzatrice esterna opzionale, porre il lettore di schede alla destra della pinzatrice di modo che si trovi tra la pinzatrice e l'MFP. **Prima di applicare la striscia di velcro assicurarsi che il coperchio superiore dell'alimentatore di documenti non sia ostruito dal lettore di schede e che possa essere aperto**.
3. Utilizzare la scheda staccabile per registrare gli indirizzi IP e MAC per il dispositivo di autenticazione e l'indirizzo IP e il nome host dell'MFP che verrà controllato da questo dispositivo di autenticazione.

   Nota: per le altre posizioni di installazione suggerite, consultare il CD di amministrazione del sistema MFP.

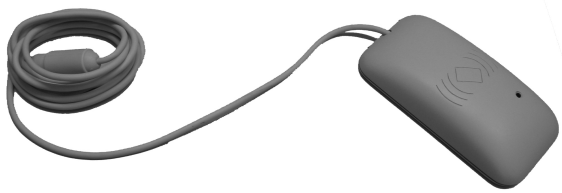
# Collegamento dell'hardware

Verificare di aver eseguito le operazioni di configurazione fornite in Configurazione dell'indirizzo IP del dispositivo di autenticazione a pagina 28 prima di collegare il dispositivo di autenticazione di Secure Access.

Collegare i componenti seguendo le indicazioni riportate nella figura sottostante. Si noti che il dispositivo di autenticazione è dotato di una porta seriale e di una porta di controllo copia che non vengono utilizzate in questa configurazione.




1. Utilizzare la scheda di configurazione per annotare l'indirizzo MAC del dispositivo di autenticazione. Immettere questo indirizzo nella stessa riga dell'MFP che deve controllare.
2. Collegare il cavo seriale del lettore di schede al connettore del lettore di schede sul dispositivo di autenticazione.

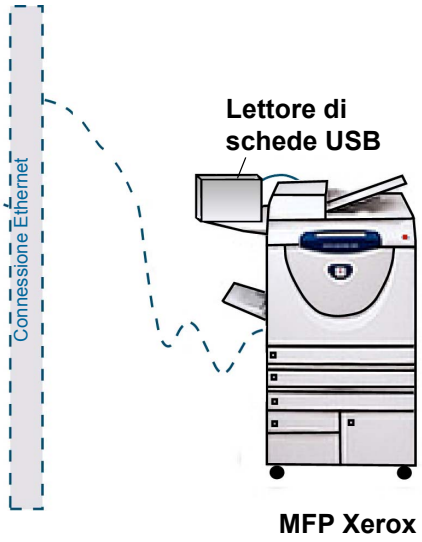


3. Collegare un'estremità del cavo Ethernet al punto di rete e l'altra estremità alla porta Uplink sul dispositivo di autenticazione di Secure Access.
4. Collegare il cavo Ethernet dell'MFP alla porta Downlink sul dispositivo di autenticazione.

   Nota: quando il dispositivo di autenticazione è spento, la connettività Ethernet dalla porta Downlink non è disponibile. In alternativa, è possibile collegare il cavo Ethernet dell'MFP direttamente a un'altra porta Ethernet. Il dispositivo di autenticazione è dotato di una porta Downlink nel caso non sia disponibile un'altra porta Ethernet.
5. Collegare un'estremità del cavo di alimentazione al dispositivo di autenticazione e l'altra estremità alla presa di corrente.

L'installazione dell'hardware è ora completa. Utilizzare le istruzioni nella Guida all'amministrazione di Secure Access per configurare il server di Secure Access e abilitare la comunicazione tra i dispositivi di autenticazione e gli MFP.

# Installazione/collegamento del lettore di schede USB di Secure Access




1. Installare il lettore di schede sul ripiano alla sinistra del pannello comandi dell'MFP utilizzando la striscia di velcro fornita. Se si dispone della pinzatrice esterna opzionale, porre il lettore di schede alla destra della pinzatrice di modo che si trovi tra la pinzatrice e l'MFP. **Prima di applicare la striscia di velcro assicurarsi che il coperchio superiore dell'alimentatore di documenti non sia ostruito dal lettore di schede e che possa essere aperto**.
2. Inserire il cavo del lettore di schede USB di Secure Access in una porta USB libera sul retro dell'MFP.

   per le altre posizioni di installazione suggerite, consultare il CD di amministrazione del sistema MFP.

# Scheda di configurazione

Staccare questa scheda e utilizzarla quando si esegue la configurazione fisica dei dispositivi di autenticazione. Si raccomanda di annotare con precisione l'indirizzo IP e MAC di ciascun dispositivo di autenticazione e del corrispondente MFP monitorato.

| | Dispositivo di autenticazione | | Dispositivo multifunzione | |
|---|---|---|---|---|
| | Indirizzo MAC | Indirizzo IP | Indirizzo IP | Nome host |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |
| 12 | | | | |
| 13 | | | | |
| 14 | | | | |
| 15 | | | | |
| 16 | | | | |
| 17 | | | | |
| 18 | | | | |
| 19 | | | | |
| 20 | | | | |