Version 1.6, Oktober 2010

Xerox Secure Access Unified ID System®

Installationshandbuch

Übersetzung:
Xerox
CTC European Operations
Bessemer Road
Welwyn Garden City
Hertfordshire
AL7 1BU
Großbritannien

Inhalt

1 Sicherheitshinweise

Diese Sicherheitshinweise genau lesen und beachten, damit das Gerät sicher und den gesetzlichen Bestimmungen entsprechend betrieben wird.

Das Gerät wurde speziell entwickelt und getestet, um strenge Sicherheitsbestimmungen zu erfüllen. Hierbei handelt es sich unter anderem um die sicherheitstechnische Zulassung und die Einhaltung geltender Umweltstandards.

Vor der Inbetriebnahme des Geräts die nachstehenden Anweisungen sorgfältig lesen und bei Bedarf darauf zurückgreifen, um einen sicheren Betrieb des Geräts zu gewährleisten.

ACHTUNG: Jede unbefugte Veränderung, einschließlich der Erweiterung des Leistungsumfangs durch neue Funktionen und den Anschluss externer Geräte, kann zum Verlust der Produktzertifizierung führen. Detaillierte Informationen hierzu können beim Xerox-Partner erfragt werden

Netzanschluss

Das im Lieferumfang des Geräts enthaltende Netzteil ist an eine Steckdose anzuschließen, die die Anforderungen auf dem Typenschild erfüllt. Im Zweifelsfall den lokalen Stromversorger um Rat fragen.

Sicherheit des elektrischen Betriebs

- Nur das im Lieferumfang des Geräts enthaltene Netzteil verwenden.
- Den Installationsort so wählen, dass das Netzkabel außerhalb der Gehbereiche verlegt werden und niemand auf das Kabel oder das Netzteil treten kann.
- Keine Gegenstände auf das Netzkabel stellen.
- Unter den nachfolgenden Bedingungen ist unverzüglich das Gerät auszuschalten und der Netzstecker des Geräts zu ziehen. Dann einen autorisierten Servicetechniker rufen, um das Problem zu beheben.
  - Entwicklung ungewöhnlichen Geruchs
  - Netzkabel beschädigt
  - Sicherung durchgebrannt, Sicherungsautomat oder anderer Schutzschalter hat angesprochen
  - Gerät wurde Wasser ausgesetzt
  - Teil des Geräts beschädigt

Trennung vom Stromnetz

Zur Trennung des Geräts vom Stromnetz das Netzkabel abziehen. Um die Stromversorgung des Geräts ganz zu unterbrechen, den Netzstecker ziehen.

Rechtliche Informationen

Hochfrequenzenergie

United States, Canada

Hinweis: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used with this equipment to maintain compliance with FCC regulations in the United States

Canada

This Class "B" digital apparatus complies with Canadian ICES-003.

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

Europa

Durch Kennzeichnung dieses Produkts mit dem CE-Zeichen erklärt sich Xerox bereit, den folgenden Richtlinien der Europäischen Union zu entsprechen (mit Wirkung vom siehe Datum):

12. Dezember 2006:	Richtlinie 2006/95/EG des Europäischen Parlaments und des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen.
15. Dezember 2004:	Richtlinie 2004/108/EG des Europäischen Parlaments und des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit und zur Aufhebung der Richtlinie 89/336/EWG.
9. März 1999:	Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität.

Der vollständige Text der Konformitätserklärung einschließlich der Definition der entsprechenden Richtlinien sowie der jeweiligen Standards ist über den Xerox-Partner erhältlich.

ACHTUNG:

- Um eine fehlerfreie Funktion dieses Geräts in der Nähe von ISM-Geräten (Hochfrequenzgeräte für industrielle, wissenschaftliche, medizinische und ähnliche Zwecke) zu gewährleisten, ist es erforderlich, dass die Störstrahlung dieser Geräte reduziert oder auf andere Weise begrenzt wird.
- Gemäß der EU-Richtlinie 89/336/EWG müssen für dieses Gerät abgeschirmte Schnittstellenkabel verwendet werden.

Richtlinien für RFID-Geräte

Das mit diesem Produkt gelieferte Lesegerät erzeugt mit einer Induktionsschleife als RFID (Radio Frequency Identification) 13,56 MHz. Dieses RFID-Gerät entspricht den in der Richtlinie 1999/5/EG des Europäischen Rates sowie in sämtlichen nationalen gesetzlichen Regelungen enthaltenen Vorgaben.

Der Betrieb des Geräts unterliegt zwei Bedingungen: 1.) Das Gerät darf keine schädliche Interferenz erzeugen und 2.) das Gerät muss jegliche empfangenen Interferenzen, einschließlich solcher, durch die unerwünschte Betriebsbedingungen verursacht werden, akzeptieren.

Durch Änderungen an dem Gerät, die nicht ausdrückliche von Xerox genehmigt wurden, kann das Rechts auf den Betrieb des Geräts für den Nutzer hinfällig werden.

Recycling und Entsorgung des Geräts

Bei der Entsorgung des Geräts ist zu beachten, dass es Blei, Quecksilber und andere Stoffe enthalten kann, deren Entsorgung bestimmten Umweltschutzbestimmungen unterliegt. Der Gehalt an Blei und Quecksilber entspricht bei Markteinführung des Geräts den einschlägigen internationalen Bestimmungen.

Europäische Union

Entsorgungsinformationen für gewerbliche Nutzer

Dieses Symbol auf dem Gerät bedeutet, dass das Gerät in Übereinstimmung mit örtlichen Vorschriften entsorgt werden muss.

Elektrische und elektronische Altgeräte müssen gemäß europäischen Vorschriften entsorgt werden.

Vor der Entsorgung von Geräten beim örtlichen Xerox-Partner erkundigen, ob das Gerät eventuell zurückgenommen wird.

North America (USA, Canada)

Xerox operates a worldwide equipment take back and reuse/recycle program. Contact your Xerox sales representative (1-800-ASK-XEROX) to determine whether this Xerox product is part of the program. For more information about Xerox environmental programs, visit http://www.xerox.com/environment

If you are managing the disposal of your Xerox product, please note that the product may contain lead, mercury, Perchlorate, and other materials whose disposal may be regulated due to environmental considerations. The presence of these materials is fully consistent with global regulations applicable at the time that the product was placed on the market. For recycling and disposal information, contact your local authorities. In the United States, you may also refer to the Electronic Industries Alliance web site: http://www.eiae.org

Perchlorate Material – This product may contain one or more Perchlorate-containing devices, such as batteries. Special handling may apply; please see http://www.dtsc.ca.gov/hazardouswaste/perchlorate

Entsorgungsinformationen für private Nutzer

Mit diesem Symbol versehene Geräte dürfen nicht dem normalen Abfallprozess zugeführt werden.

Geräte mit diesem Symbol sind gemäß europäischer Richtlinien zur Entsorgung von elektrischen und elektronischen Geräten vom normalen Hausmüll zu trennen.

Privathaushalte innerhalb eines EU-Mitgliedstaates sind berechtigt, gebrauchte elektrische und elektronische Geräte gebührenfrei bei den entsprechenden Sammelstellen abzugeben. Weitere Auskünfte erteilen die örtlichen Behörden.

In einigen Mitgliedsstaaten sind die Einzelhändler verpflichtet, beim Neukauf alte Geräte kostenlos zurückzunehmen. Weitere Auskünfte erteilen die Einzelhändler.

Andere Länder

Auskünfte beim örtlichen Abfallentsorgungsträger einholen.

Kontaktdaten für Informationen zu Umwelt- und Arbeitssicherheit

Kontaktdaten

Weitere Informationen zur Umwelt- und Arbeitssicherheit sind unter folgender Rufnummer bzw. Internetadresse erhältlich:

USA: 1-800 828-6571

Kanada: 1-800 828-6571

Europa: +44 1707 353 434

www.xerox.com/environment (Informationen zur Produktsicherheit für die USA)

www.xerox.environment_europe (Informationen zur Produktsicherheit für Europa)

2 Checkliste zur Installation

Das Installationshandbuch und das Systemhandbuch zu Xerox Secure Access enthalten schrittweise Anleitungen zur Installation und Konfiguration des Secure Access-Servers und der MFG. In der nachfolgenden Tabelle ist die Reihenfolge der Arbeitsschritte angegeben, die je nach Secure Access-Hardwarekonfiguration auszuführen sind.

Schritte (*) = obligatorisch	Xerox Secure Access mit USB-Kartenleser	Xerox Secure Access mit Authentifizierungsgerät und Kartenleser
Installationshandbuch		
1. Kapitel 3, „Installationsübersicht“, lesen	*	*
2. Kapitel 4, „Installation des Secure Access-Servers“: „Vorbereitung von Netzwerk und Datenbank“	*	*
3. Kapitel 4, „Installation des Secure Access-Servers“: „Ausführung des Installationsassistenten“	*	*
4. Kapitel 5, „Einrichtung der Secure Access-Hardware“, Schritt 1: „Einstellung der IP-Adresse des Authentifizierungsgeräts“	Überspringen	*
5. Kapitel 5, „Einrichtung der Secure Access-Hardware“, Schritt 2: „Installation des Secure Access-Authentifizierungsgeräts“	Überspringen	*
6. Kapitel 5, „Einrichtung der Secure Access-Hardware“, Schritt 3: „Anschluss der Hardware“	Überspringen	*
7. Kapitel 5, „Einrichtung der Secure Access-Hardware“, Schritt 4: „Installation des Secure Access-USB-Kartenlesers“	*	Überspringen
Systemhandbuch		
8. Kapitel 3, „Überblick über Secure Access“, lesen	*	*
9. Kapitel 4: „Konfigurationsverfahren“, Schritt 1: „Konfigurierung des MFGs für die Netzwerkauthentifizierung über Secure Access“	*	*
10. Kapitel 4: „Aufnahme von MFG in die Secure Access-Datenbank“	*	*
11. Kapitel 4: „Zuordnung eines Secure Access-Authentifizierungsgeräts zu einem MFG“	Überspringen	*
12. Kapitel 4: „Konfiguration des Follow-You-Drucks“ (optional)	*	*
13. Kapitel 4: „Einrichtung der Authentifizierungsparameter“	*	*
14. Kapitel 4: „Import und Synchronisierung von Benutzerkonten“	*	*
15. Kapitel 4: „Konfiguration des Diensts ‚Release My Documents‘“	*	*

Installationsübersicht 3

Themen dieses Kapitels:

Dieses Handbuch enthält Anweisungen zur Installation von Xerox Secure Access Unified ID System™-Serversoftware sowie zur Einrichtung der Authentifizierungsgeräte. Vor der Konfiguration der Authentifizierungsgeräte muss der Server installiert werden.

Nach der ordnungsgemäßen Installation der Secure Access-Serversoftware können Hardware und Software den detaillierten Anweisungen im Secure Access-Systemhandbuch entsprechend implementiert bzw. konfiguriert werden.

Dieses Kapitel enthält Informationen über:

- Komponenten des Secure Access-Servers
- Systemanforderungen

Secure Access-Komponenten

Xerox Secure Access Unified ID System (im Folgenden „Secure Access“ genannt) besteht aus folgenden Komponenten:

- Secure Access-Serversoftware zur Verwaltung der Benutzerdatenbank und Bereitstellung der Dienste, die mit den Multifunktionsgeräten (MFG) und den Secure Access-Authentifizierungsgeräten kommunizieren.
- Secure Access-Authentifizierungsgerät mit Kartenleser, das den Zugriff auf die Xerox-MFG steuert.

  –Oder–
- Secure Access-USB-Kartenleser

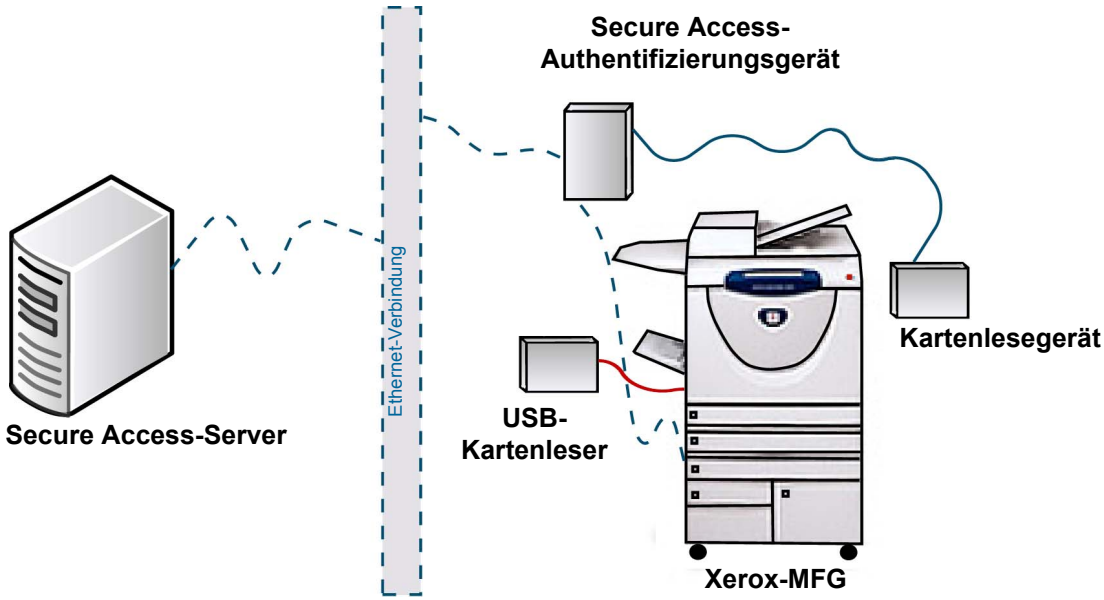


Abbildung 3-1: Secure Access-Komponenten

Für jede Installation der Secure Access-Serversoftware werden mindestens drei Dienste benötigt:

- Core Authentication Server (CAS)
- Device Control Engine (DCE)
- Document Routing Engine (DRE)

Darüber hinaus muss auch Secure Access Manager installiert werden, ein Verwaltungstool zur Herstellung der Kommunikation zwischen den verschiedenen Secure Access-Komponenten.

Core Authentication Server (CAS)

Auf dem Core Authentication Server (CAS) residiert die Datenbank, die alle Benutzer- und MFG-Daten enthält.

Für jede Secure Access-Installation ist eine vorinstallierte Datenbank erforderlich. Mit Hilfe der Datenbankinstanz erzeugt der CAS eine Kontendatenbank, die alle Benutzer- und Gerätedaten enthält. Informationen zu den unterstützten Datenbanken enthält der Abschnitt Systemanforderungen des Secure Access-Servers Seite 18.

Device Control Engine (DCE)

Die DCE (Device Control Engine) wickelt die gesamte Kommunikation mit den MFG ab. Wenn ein Benutzer die Kopier-, Scan- oder Faxfunktionalität eines MFG nutzen möchte, muss zunächst das Kartenlesegerät bedient werden. Eine Magnetstreifen- oder Transponderkarte löst eine Zugriffsanforderung aus.

Das Authentifizierungsgerät leitet die Anmeldeanforderung an die DCE weiter, welche dann den CAS auffordert, die Daten des zu der Karte gehörigen Benutzerkontos zu überprüfen.

Document Routing Engine (DRE)

Bei der Document Routing Engine (DRE) handelt es sich um den Druckserver. Ihre Hauptfunktion liegt in der Leitung der Dokumente von den Arbeitsstationen der Benutzer zu den MFG. Eines typischer DRE-Workflow sieht wie folgt aus:

1. Ein Benutzer generiert eine Druckanforderung an ein MFG, das in der Secure Access Manager-Datenbank registriert ist.
2. Wenn der Benutzer über eine Druckerwarteschlange druckt, die einen Secure Access Manager-Port nutzt, hält die DRE den Druckauftrag auf dem Druckserver.
3. Meldet sich der Benutzer beim MFG an, durchsucht die DRE die für diesen Drucker (und/oder diese Gerätegruppe) in der Warteschlange befindlichen Aufträge und gibt jene frei, die von dem angemeldeten Benutzer übermittelt wurden.

Wenn auf dem Gerät kein Secure Access-Port installiert ist, erfolgt der Druck des Auftrags ohne Überprüfung.

Sollen Aufträge gedruckt werden, die sich in einer geschützten Warteschlange befinden, kann die Funktion Follow-You-Druck konfiguriert werden. Um diese Funktion zu aktivieren, muss für das MFG anstelle eines Standardports die Nutzung eines Secure Access-Ports konfiguriert werden. Der Portmonitor lässt sich in das Windows-Drucksubsystem integrieren und agiert als Teil des Spooler-Diensts. So kann der Portmonitor Druckaufträge empfangen und in einer gesicherten virtuellen Warteschlange halten, bis ein verifizierter Benutzer sie zur Verarbeitung auf einem bestimmten MFG freigibt.

Zudem kann auf dem MFG der Dienst „Release My Documents“ eingerichtet werden. Mit seiner Hilfe können Benutzer ihre geschützten Aufträge direkt am MFG aufrufen. Ausführliche Informationen sind dem Secure Access-Systemhandbuch zu entnehmen.

Konfiguration mit mehreren Servern

Eine Installation, bei der alle Dienste auf einem Server installiert sind, wird als „lokale“ Installation bezeichnet. Möglicherweise sind bei einigen Installationen mehrere Server erforderlich, um den Verwaltungsaufwand zu verteilen. Installationen, bei denen Dienste auf zwei oder mehr Server verteilt sind, bezeichnet man als „remote“ Installationen.

Unabhängig von der Anzahl der verwendeten Server gilt, dass die DRE- und DCE-Dienste sich grundsätzlich auf demselben Server befinden müssen.

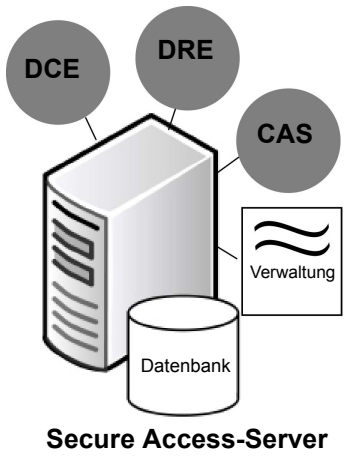


Abbildung 3-2: Lokale Installation

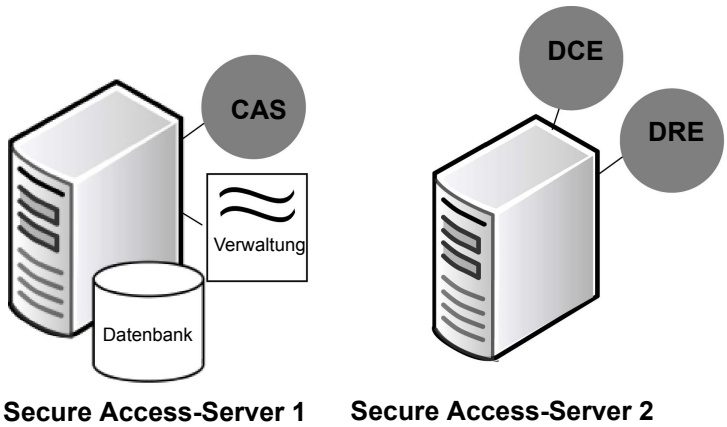


Abbildung 3-3: Remote Installation

Wenn Secure Access für die Verwaltung einer großen Anzahl von MFG zuständig ist, können darüber hinaus mehrere DRE-Druckserver installiert werden, um das Kommunikationsvolumen gleichmäßig zu verteilen.

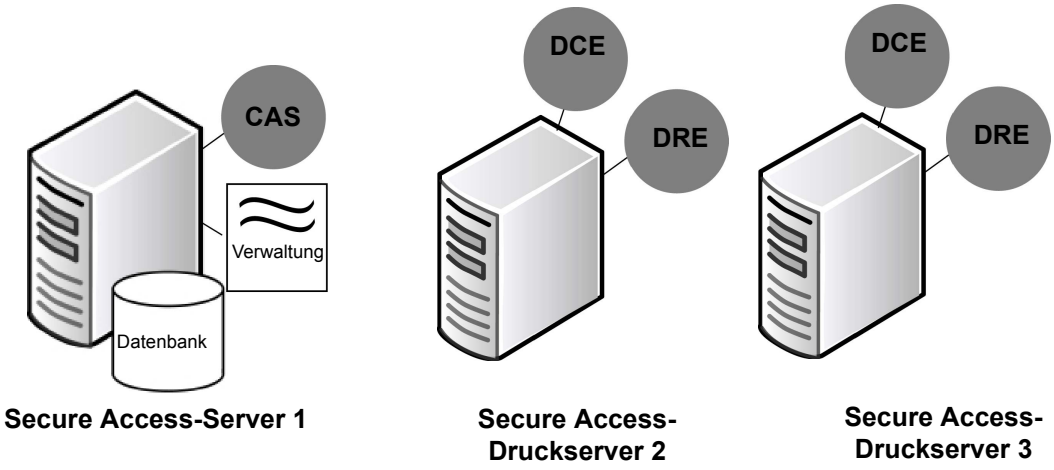


Abbildung 3-4: Implementierung mit mehreren Druckservern

Einzelheiten zum Installieren und Einrichten einer Implementierung mit mehreren Servern siehe Ausführung des Installationsassistenten Seite 23. Es ist möglich, im Installationsassistenten nur die Komponenten auszuwählen, die auf den einzelnen Servern installiert werden sollen. Die DRE- und DCE-Dienste können auf mehreren Servern installiert werden. Sie müssen sich grundsätzlich auf demselben Server befinden.

Systemanforderungen des Secure Access-Servers

Vor der Installation von Secure Access prüfen, ob alle Server, die verwendet werden sollen, die nachfolgend aufgeführten Mindestanforderungen erfüllen.

Die nachstehende Tabelle enthält nur eine Auflistung der Mindest-Betriebsanforderungen. Zur Erzielung maximaler Leistung bei hohen Druckvolumen sind mehr Festplatten- und Speicherkapazität sowie ein schnellerer Prozessor erforderlich.

Komponente	Mindestanforderungen
Hardware	• Prozessor: Pentium III, Athlon oder schneller • Systemspeicher: mindestens 512 MB • Kapazität Anwendungsdatenträger: 100 MB • Kapazität Datenbankdatenträger: 20 MB • Anzeigeauflösung: 1024 x 768
CAS/DCE/DRE-Betriebssystem	Eines der folgenden Betriebssysteme: • Windows Server 2003 (32-Bit) • Windows XP Professional (nur 32-Bit)[1] • Windows Server 2008 (32- und 64-Bit), 2008 R2 (64-Bit) Hinweis: Vor der Installation der Secure Access-Serversoftware müssen alle erforderlichen kritischen Betriebssystem-Updates installiert werden.
Datenbanken	• Microsoft SQL Server 2005 Express[2] • Microsoft SQL Server 2008 Express (64-Bit) Hinweis: Secure Access kann nicht auf einem Server installiert werden, auf dem eine MSDB-Anwendung wie FreeFlow™ SMARTsend™ ausgeführt wird, da diese Datenbanken Konflikte mit der SQL Server-Datenbank verursachen.

[1] Soll der CAS-Dienst auf einem Windows XP Professional-Server, der nicht Mitglied einer Domäne ist, installiert werden, die Benutzerauthentifizierung wie weiter unten erläutert konfigurieren.

[2] Für die Ausführung von SQL Server 2005 Express unter Windows Server 2008 oder 2008 R2 ist Windows Service Pack 2 (SP2) oder höher erforderlich.

Benutzerauthentifizierung unter Windows XP Professional

Soll der CAS-Dienst auf einem Windows XP Professional-Server, der nicht Mitglied einer Domäne ist, installiert werden, müssen die Windows XP-Sicherheitseinstellungen so modifiziert werden, dass eine Anmeldung unter Einsatz von Benutzerkonten möglich ist.

In der XP-Standardeinstellung werden Benutzer automatisch unter dem Gastkonto angemeldet. Sollen Benutzer sich unter eigenen Konten anmelden, muss diese Einstellung geändert werden.

Dies ist vor der Ausführung des Secure Access-Installationsassistenten zu erledigen.

1. Das Fenster „Lokale Sicherheitseinstellungen“ auf dem Rechner, auf dem CAS installiert werden soll, öffnen.
2. Im linken Fensterbereich auf **Lokale Richtlinien** klicken und dann auf **Sicherheitsoptionen** doppelklicken.
3. Im rechten Fensterbereich einen Bildlauf zum Eintrag **Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten** ausführen.
4. Auf diesen Eintrag doppelklicken und **Klassisch - lokale Benutzer authentifizieren sich als sie selbst** auswählen.
5. Auf **Anwenden** und dann auf **OK** klicken, um das Dialogfeld zu schließen.
6. Fenster „Lokale Sicherheitseinstellungen“ schließen.

Erforderliche Hardware

Für Secure Access ist folgende Hardware erforderlich:

Konfiguration 1

- Netzteil
- Netzkabel
- Bypass-Schlüssel (zur Rücksetzung des Geräts auf die Standardeinstellungen); siehe hierzu Rücksetzung von Authentifizierungsgeräten im Anhang des Systemhandbuchs.
- 10/100 Base-T Ethernet-Netzwerkkabel
- Kartenlesegerät

–Oder–

Konfiguration 2

- Secure Access-USB-Kartenleser

Unterstützte Kartenleser

Secure Access unterstützt folgende Kartenleser:

- ABA Magstripe
- Mifare (einschließlich HID iCLASS-Leser)
- Legic
- HID 125 kHz
- Indala
- EM Marin
- Hitag

4 Installation des Secure Access-Servers

Themen dieses Kapitels:

Dieser Abschnitt enthält Anweisungen zur Installation des Secure Access-Servers mit dem Secure Access-Server-Installationsassistenten. Die nachstehenden Anweisungen unbedingt genau ausführen und sicherstellen, dass die Server die im Abschnitt Systemanforderungen des Secure Access-Servers Seite 18 beschriebenen Betriebsanforderungen erfüllen.

Dieses Kapitel enthält Informationen zu:

- Vorbereitung von Netzwerk und Datenbank vor der Installation
- Einsatz des Installationsassistenten für die Installation von Komponenten auf den einzelnen Secure Access-Servern

Vorbereitung von Netzwerk und Datenbank

Auch wenn das Secure Access-Installationsverfahren sehr einfach ist, sind vor Ausführung des Installationsassistenten folgende Schritte durchzuführen:

1. Systemfunktionen planen.
2. Xerox Secure Access auf dem MFG mithilfe der CentreWare Internet-Services aktivieren.

   Hinweise:

   - Über einen Webbrowser bei den CentreWare Internet-Services des MFGs anmelden. Die Seite zur Aktivierung von Xerox Secure Access aufrufen. Für diese Installation muss SSL aktiviert und ein Zertifikat erzeugt werden. Weitere Informationen hierzu sind der mit dem MFG gelieferten Systemverwaltungs-CD zu entnehmen.
   - Bei Einsatz eines USB-Kartenlesers muss möglicherweise die Software des MFGs aktualisiert werden. Xerox-Partner kontaktieren oder auf der Xerox-Website (www.xerox.com) im Bereich „Support und Treiber“ die Supportseite zum jeweiligen MFG aufrufen.
3. Installationsziel für jede der Secure Access-Komponenten festlegen.

   Hinweis: Vor der Implementierung von Secure Access im Netzwerk sicherstellen, dass für alle Geräte, die installiert und konfiguriert werden müssen, Administratorrechte vorhanden sind.
4. Prüfen, ob die aktuelle Netzwerkkonfiguration die Kommunikation zwischen Secure Access-Komponenten unterstützt.
5. Mit Windows Update sicherstellen, dass alle erforderlichen wichtigen Betriebssystem-Updates installiert sind.
6. Microsoft .NET Framework 2.0 installieren.

   Hinweis: Eine vollständige Liste der Voraussetzungen für die Installation von SQL Server 2005 oder 2008 Express Edition ist auf der Microsoft-Website erhältlich.
7. Die Datenbank installieren und konfigurieren.

   Hinweis: Bei Einsatz von SQL Server 2005 oder 2008 Express muss die Datenbank für die Verwendung des Windows-Authentifizierungsmodus konfiguriert werden. Die Authentifizierung im gemischten Modus wird von Secure Access nicht unterstützt.

Ausführung des Installationsassistenten

Während der Secure Access-Installation können im Installationsassistenten die für die einzelnen Server zu installierenden Funktionen ausgewählt werden. Werden die Komponenten auf mehrere Server verteilt, den Installationsassistenten auf jedem Server ausführen und nur die jeweils benötigten Komponenten auswählen. Erfolgt die Installation auf einem einzelnen Server, braucht der Assistent nur einmal ausgeführt zu werden.

Pro Implementierung ist mindestens ein CAS, eine DCE, eine DRE und eine Instanz von Secure Access Manager erforderlich.

1. Sicherstellen, dass die unter „Vorbereitung von Netzwerk und Datenbank“ beschriebenen Schritte vor Durchführung der Installation abgeschlossen sind.
2. Vor dem Start der Secure Access-Installation alle anderen Anwendungen auf dem Server schließen.
3. Den Secure Access-Installationsassistenten starten.
   - Bei der Installation von der Secure Access-CD die Datei **32-bit Setup.exe** auswählen, um die Installation für ein 32-Bit-Gerät zu starten. Falls auf einem 64-Bit-Gerät installiert wird, die Datei **64-bit Setup.exe** auswählen.

   –Oder–

   - Bei der Installation über das Internet die ZIP-Datei herunterladen und die Datei **Setup.exe** für den 32- oder 64-Bit-Server ausführen.

   Hinweis: Erscheint bei dem Versuch, setup.exe auszuführen, eine Fehlermeldung, ist möglicherweise eine Aktualisierung auf eine neuere Version des Microsoft-Installationsprogramms erforderlich. In diesem Fall die neueste Version des Installationsprogramms für das verwendete Betriebssystem von der Microsoft-Website herunterladen und installieren.
4. Auf der ersten Seite den Installationsvorgang mit einem Klick auf **Weiter** starten.
5. Die Software-Lizenzvereinbarung lesen und dann nacheinander auf **I accept** (Ich akzeptiere) und **Weiter** klicken.
6. Die Optionen wählen, die auf diesem Gerät installiert werden sollen, und anschließend auf **Weiter** klicken.

   Standardmäßig sind alle Komponenten markiert. Nur die Komponenten auswählen, die auf dem jeweiligen Server benötigt werden. Wenn dieses Gerät beispielsweise als Druckserver eingesetzt wird, sind nur die Komponenten DRE und DCE zu installieren. Dann das Installationsprogramm auf einem anderen Server ausführen, um die übrigen Komponenten den jeweiligen Anforderungen entsprechend zu installieren.

   Hinweis: Vor der Installation einer Komponente die Komponentenbeschreibungen im Abschnitt Secure Access-Komponenten Seite 14 lesen. Diese Informationen dienen dazu, die für die Anforderungen des Unternehmens optimale Implementierung der Komponenten zu ermitteln.
7. Im Fenster **Select Language** (Sprache wählen) die gewünschte Anzeigesprache auswählen. Die hier gewählte Spracheinstellung gilt nur für Secure Access Manager. Die Anzeigesprache am MFG-Steuerpult wird am MFG selbst eingestellt.

8. Im Fenster **Instance for SQL Express** (Instanz für SQL Express) den Namen der für die SQL Express-Datenbank erzeugten Datenbankinstanz eingeben. Auf **Weiter** klicken.

   Hinweis: Der in dieses Feld eingegebene Instanzname MUSS mit dem bei der Installation von SQL Express für die Secure Access-Datenbank angegebenen Instanznamen identisch sein. Ohne den korrekten Instanznamen kann die Installation nicht fortgesetzt werden. Wenn eine standardmäßige SQL Express-Installation durchgeführt wurde und für alle Parameter die Standardwerte übernommen wurden, die Einstellung SQLEXPRESS beibehalten und auf „Weiter“ klicken.

9. Im Fenster **User Name for Services** (Benutzername für Dienste) eine **UserID** (Benutzerkennung) und das **Password** (Kennwort) für die Dienste eingeben.

   Werden die Komponenten auf mehreren Systemen implementiert, sind bei jeder Installation UNBEDINGT dieselben Benutzerdaten einzugeben. Diese Angaben werden benötigt, um alle Dienste zu starten und auszuführen. Werden nicht auf allen Komponenten dieselben Benutzerdaten eingegeben, reagiert der Core Authentication Server nicht auf Anforderungen von DCE oder DRE.

   Für Domänenkonten ist der Domänenname zu verwenden (zum Beispiel: Domäne\Benutzername).

   Zwar sind für dieses Konto keine Administratorrechte auf dem Secure Access-Server erforderlich, doch muss das Konto Bedienerrechte für den Drucker besitzen, damit die DRE Druckanforderungen verarbeiten kann.

10. Den Namen des Xerox Secure Access-Authentifizierungsservers eingeben.

    Beim Starten von Secure Access Manager ist der Core Authentication Server mit dem hier eingegebenen Namen zu identifizieren.

11. Auf **Install** (Installieren) klicken, um den Installationsvorgang zu starten. Es werden nun Dateien kopiert, Dienste eingerichtet und Verknüpfungen für Secure Access Manager erstellt.

12. Nach Abschluss der Installation auf **Fertig stellen** klicken, um den Installationsassistenten zu schließen.

13. Damit ist die Installation des Secure Access-Servers abgeschlossen. Anweisungen zur Einrichtung der Secure Access-Hardware enthält Kapitel 5.

Aktualisierung von Secure Access

Im Folgenden wird die Aktualisierung von Secure Access mit dem Installationsassistenten erläutert. Diese Anweisungen gelten sowohl für die schrittweise Aktualisierung einzelner Komponenten als auch für die gleichzeitige Aktualisierung aller Komponenten während einer geplanten Downtime.

Hinweis: Es empfiehlt sich, vor der Durchführung einer Aktualisierung eine Sicherungskopie der Datenbank anzulegen.

Im Rahmen der Secure Access-Aktualisierung werden die bereits auf dem Gerät installierten Secure Access-Komponenten ermittelt (beispielsweise die Datenbank). Diese Komponenten sind im Installationsassistenten automatisch markiert. Es besteht die Möglichkeit, entweder die Standardauswahl zu übernehmen oder zusätzliche Komponenten für die Installation auszuwählen.

Zur Aktualisierung von Secure Access wie folgt vorgehen:

1. Vor dem Start der Secure Access-Installation alle anderen Anwendungen auf dem Server schließen.
2. Den Secure Access-Installationsassistenten starten.
   - Bei der Installation von der Secure Access-CD die Datei **32-bit Setup.exe** auswählen, um die Installation für ein 32-Bit-Gerät zu starten. Falls auf einem 64-Bit-Gerät installiert wird, die Datei **64-bit Setup.exe** auswählen.

   –Oder–

   - Bei der Installation über das Internet die ZIP-Datei herunterladen und die Datei **Setup.exe** für den 32- oder 64-Bit-Server ausführen.

   Hinweis: Erscheint bei dem Versuch, setup.exe auszuführen, eine Fehlermeldung, ist möglicherweise eine Aktualisierung auf eine neuere Version des Microsoft-Installationsprogramms erforderlich. In diesem Fall die neueste Version des Installationsprogramms für das verwendete Betriebssystem von der Microsoft-Website herunterladen und installieren.
3. Auf der ersten Seite den Installationsvorgang mit einem Klick auf **Weiter** starten.
4. Die Software-Lizenzvereinbarung lesen und dann nacheinander auf **I accept** (Ich akzeptiere) und **Weiter** klicken.
5. Die Optionen wählen, die auf diesem Gerät installiert werden sollen, und anschließend auf **Weiter** klicken.

   Standardmäßig sind alle Komponenten markiert. Nur die Komponenten auswählen, die auf dem jeweiligen Server benötigt werden. Wenn dieses Gerät beispielsweise als Druckserver eingesetzt wird, sind nur die Komponenten DRE und DCE zu installieren. Dann das Installationsprogramm auf einem anderen Server ausführen, um die übrigen Komponenten den jeweiligen Anforderungen entsprechend zu installieren.
6. Den Namen des Xerox Secure Access-Authentifizierungsservers eingeben.
7. Auf **Fertig stellen** klicken, um den Installationsassistenten zu beenden.

Damit ist die Aktualisierung des Secure Access-Servers abgeschlossen. Anweisungen zur Einrichtung der Secure Access-Hardware enthält Kapitel 5.

5 Einrichtung der Secure Access-Hardware

Themen dieses Kapitels:

Dieses Kapitel enthält Anweisungen zur Einrichtung der Secure Access-Hardware. Vor der Einrichtung der Hardware ist die Secure Access-Serversoftware zu installieren. Anweisungen zur Installation des Secure Access-Servers enthält Kapitel 4.

Bei Verwendung eines USB-Kartenlesers mit dem Abschnitt „Installation des Secure Access-USB-Kartenlesers“ fortfahren.

1. IP-Adresse für jedes Authentifizierungsgerät angeben.
2. Secure Access-Authentifizierungsgerät am MFG oder in dessen Nähe aufstellen.
3. Netz- und Schnittstellenkabel anschließen.

Einstellung der IP-Adresse des Authentifizierungsgeräts

ACHTUNG: Erfolgt die Zuweisung der IP-Adressen nicht über einen DHCP-Server, das Authentifizierungsgerät erst NACH der manuellen Einstellung der IP-Adresse in das Netzwerk einbinden. Siehe Manuelle IP-Adresszuweisung Seite 29.

Secure Access-Authentifizierungsgeräte sind standardmäßig für DHCP-Kommunikation konfiguriert. Jedem Authentifizierungsgerät ist eine IP-Adresse zuzuweisen. Außerdem muss die Server-IP-Adresse der DCE-Komponente eingestellt werden. Die IP-Adresse kann auf zweifache Weise zugewiesen werden:

- Über einen DHCP-Server (siehe Einrichtung des DHCP-Servers für die Ortung der Authentifizierungsgeräte Seite 28)
- Wird kein DHCP-Server verwendet oder soll die Option 230 auf dem benutzten DHCP-Server nicht eingestellt werden, müssen die Adressen mit der Webverwaltungsanwendung manuell festgelegt werden. Siehe hierzu Manuelle IP-Adresszuweisung Seite 29.

Einrichtung des DHCP-Servers für die Ortung der Authentifizierungsgeräte

Die nachfolgenden Anweisungen gelten für Windows-DHCP-Server. Läuft auf dem Server ein anderes Betriebssystem (z. B. UNIX, Linux, OS X, OpenVMS, AS/400), darauf achten, dass der DHCP-Server die DCE-Serveradresse im Wert 230 übergibt.

Hinweis: Weitere Informationen zur IP-Adresszuweisung über DHCP stehen auf der Xerox-Website zur Verfügung.

1. In der Windows-Verwaltung die DHCP-Serververwaltungskonsole öffnen.
2. Den Root-Knoten des DHCP-Servers wählen.
3. Im Menü **Aktion** die Option **Vordefinierte Optionen einstellen** wählen.
4. In der Dropdown-Liste **Optionsklasse** den Eintrag **DHCP-Standardoptionen** wählen.
5. Im Abschnitt **Optionsname** auf **Hinzufügen** klicken.
   a. In das Feld **Name** „Xerox Secure Access“ eingeben.

   Hinweis: Der hier eingegebene Name dient zu Identifikationszwecken.

   b. In der Dropdown-Liste **Datentyp** den Eintrag „Zeichenfolge“ wählen.
   c. In das Feld **Code** „230“ eingeben.
   d. In das Feld **Beschreibung** „Secure Access“ eingeben.
6. Auf **OK** klicken.
7. Im Abschnitt **Zeichenfolgenwert** „EQ;A;<IP-Adresse des DCE-Servers> in das Feld **Zeichenfolge** eingeben, wobei <IP-Adresse des DCE-Servers> die IP-Adresse des eigenen DCE-Servers ist.
8. Den Knoten **Bereich** erweitern und **Bereichsoptionen** wählen.
9. Im Menü **Aktion** die Option **Optionen konfigurieren** wählen.

10. **230** wählen.
11. Auf **OK** klicken, um die Änderungen zu speichern.

Manuelle IP-Adresszuweisung

Vorgehen wie nachfolgend beschrieben, wenn die IP-Adresse des Authentifizierungsgeräts nicht über einen DHCP-Server eingestellt wird ODER zwar ein DHCP-Server benutzt wird, aber statt der Option 230 statische IP-Adressen verwendet werden sollen.

Nach dem erstmaligen Einschalten sucht das Authentifizierungsgerät nach einem DHCP-Server, um eine IP-Adresse zu erhalten. Wird kein DHCP-Server gefunden, schaltet das Gerät auf statische Kommunikation um und stellt standardmäßig die statische IP-Adresse 192.168.2.1 ein. Mit einem Ethernet-Kabel kann jedes Authentifizierungsgerät mit einem System (z. B. mit einem Laptop) verbunden werden. Dann kann mit einer Webverwaltungsanwendung die IP-Adresse geändert und die IP-Adresse des DCE-Servers eingegeben werden.

Bevor mit der manuellen Zuweisung der IP-Adresse begonnen wird, die Konfigurationsübersicht auf Seite 32 ausdrucken. Auf diesem Blatt können die den einzelnen Authentifizierungsgeräten zugewiesenen IP-Adressen notiert werden.

Laptop einrichten:

Das System, auf dem die Webverwaltungsanwendung läuft, muss die statische IP-Adresse erkennen. Erst dann kann auf die Anwendung zugegriffen werden.

1. Auf dem Laptop, auf dem die Webverwaltungsanwendung ausgeführt werden wird, **Netzwerkverbindungen** > **LAN-Verbindung** > **Eigenschaften** wählen.
2. Auf **Internetprotokoll (TCP/IP)** doppelklicken. Anschließend auf **Erweitert** klicken.
3. Im Feld „IP-Adressen“ auf **Hinzufügen** klicken.
4. Folgendes eingeben:
   IP-Adresse: 192.168.2.x (wobei x ein nicht zugewiesener Wert ist)
   Subnetzmaske: 255.255.255.0
5. Auf **Hinzufügen** klicken, um die vorgenommenen Änderungen zu speichern.

IP-Adresse über Webverwaltungsanwendung festlegen:

Auf jedem Authentifizierungsgerät die nachfolgend beschriebenen Schritte ausführen.

1. Mit einem normalen Ethernet-Kabel einen Laptop mit dem Downlink-Anschluss des Secure Access-Authentifizierungsgeräts verbinden.
2. Das Netzkabel an das Authentifizierungsgerät und eine nahe gelegene Steckdose anschließen.
3. Einen Web-Browser starten und 192.168.2.1 in das Adressfeld eingeben.
   Hierbei handelt es sich um die dem Secure Access-Authentifizierungsgerät werkseitig zugewiesene Standard-IP-Adresse.

   Hinweis: Für Französisch den bereitgestellten Link wählen.
4. Oben auf der Seite auf den Link **Configure** (Konfigurieren) klicken.

5. Bei der Anmeldung Folgendes eingeben:

   Benutzername: deviceadmin

   Kennwort: pc_passwd

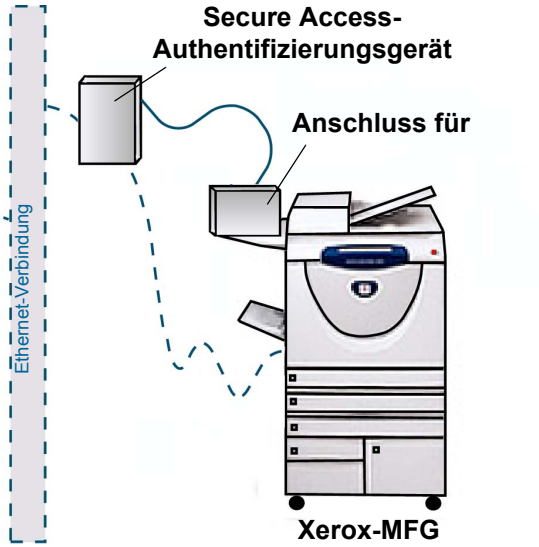
6. Das für den Aufruf der Webverwaltungsanwendung benutzte Kennwort ändern. Das Kennwort kann jederzeit zurückgesetzt werden. Vor der Inbetriebnahme des Secure Access-Systems sollte das Kennwort jedoch unbedingt geändert werden.
7. Im Abschnitt **Configure Xerox Secure Access Authentication Device** (Xerox Secure Access-Authentifizierungsgerät konfigurieren) im Feld **Addressing mode** (Adressierungsmodus) die Option „Static IP“ (Statische IP-Adresse) wählen.
8. In das Feld **IP Address** (IP-Adresse) eine statische IP-Adresse für das Authentifizierungsgerät eingeben.
9. Im Abschnitt **Configure Server** (Server konfigurieren) die IP-Adresse des DCE-Servers in das Feld „Server IP Address“ (Server-IP-Adresse) eingeben.
10. Auf die Schaltfläche **Update Configuration** (Konfiguration aktualisieren) klicken. Diese befindet sich unterhalb der „Configure Server“-Felder.
11. Zunächst auf den oben auf der Seite befindlichen Link **Restart** (Neustart) und dann auf „Click here to confirm restart“ (Hier klicken, um den Neustart zu bestätigen) klicken, um das Terminal neu zu starten.

Diese Schritte für jedes Secure Access-Authentifizierungsgerät ausführen, das implementiert werden soll.

Hinweis: Abschließend nicht vergessen, die Internet-Eigenschaften des Laptops auf den vorherigen Zustand zurückzusetzen.

Installation des Secure Access-Authentifizierungsgeräts

Zunächst die Konfigurationsübersicht Seite 35 ausdrucken. Bei Ausführung der nachstehenden Anweisungen die einzelnen Spalten dieser Übersicht ausfüllen. Diese Informationen werden bei der Konfiguration der Kommunikation zwischen den Geräten auf dem Secure Access-Server benötigt.



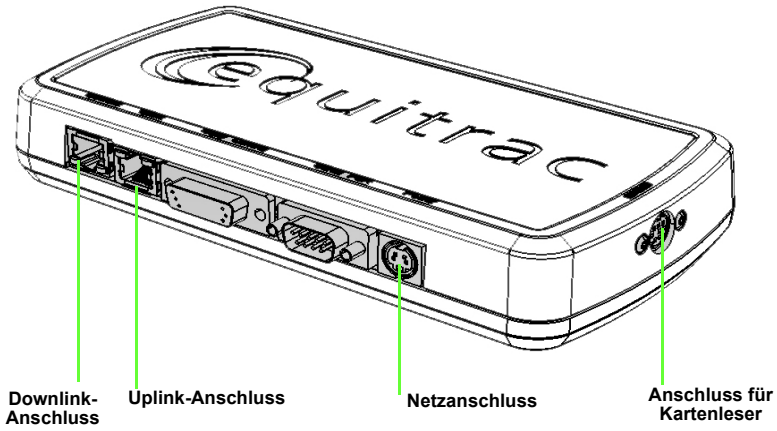
1. Das Authentifizierungsgerät an der Rückseite des MFGs auf dem Boden aufstellen. **Das Gerät darf nicht im Weg stehen, allerdings ist zu berücksichtigen, dass das Anschlusskabel des Kartenlesers ca. 1,80 m lang ist.**
2. Den Kartenleser mit dem im Lieferumfang enthaltenen Klettband auf der Ablage links neben dem Steuerpult des MFGs anbringen. Ist der optionale Offline-Hefter installiert, den Kartenleser rechts neben dem Hefter platzieren, so dass sich der Kartenleser zwischen Hefter und MFG befindet. **Vor dem Anbringen des Klettbands prüfen, ob sich die obere Abdeckung des Vorlageneinzugs ohne Behinderung durch den Kartenleser öffnen lässt.**
3. In der Konfigurationsübersicht die IP- und MAC-Adresse des Authentifizierungsgeräts sowie die IP-Adresse und den Hostnamen des MFGs notieren, das von diesem Authentifizierungsgerät überwacht werden soll.

   Hinweis: Weitere Möglichkeiten zur Anbringung sind der mit dem MFG gelieferten CD zur Systemverwaltung zu entnehmen.

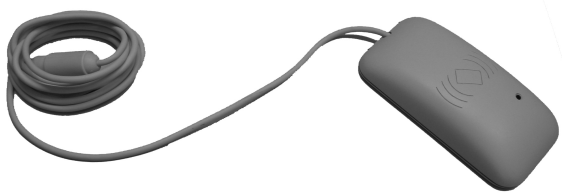
Anschluss der Hardware

Vor dem Anschließen des Secure Access-Authentifizierungsgeräts prüfen, ob alle unter Einstellung der IP-Adresse des Authentifizierungsgeräts Seite 28 beschriebenen Konfigurationsmaßnahmen ausgeführt wurden.

Die Komponenten anhand der nachstehenden Abbildung anschließen. Das Authentifizierungsgerät verfügt über einen seriellen Anschluss und einen Anschluss für einen Kostenzähler. Diese Anschlüsse bleiben in der aktuellen Konfiguration jedoch unbenutzt.



1. Die MAC-Adresse des Authentifizierungsgeräts in der Konfigurationsübersicht notieren. Diese Adresse in die Zeile des MFGs eintragen, das von dem Authentifizierungsgerät überwacht werden soll.
2. Das serielle Kabel des Kartenlesers mit dem Kartenleseranschluss des Authentifizierungsgeräts verbinden.



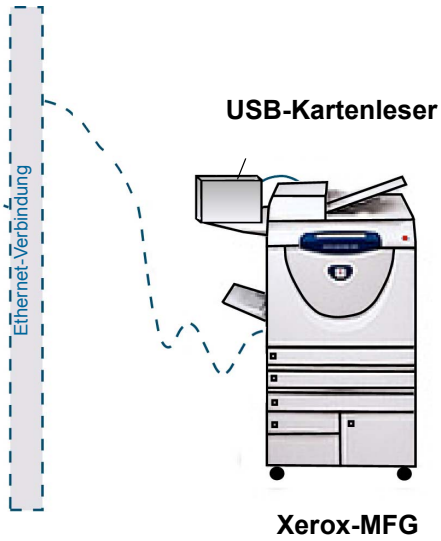
3. Ein Ende des Ethernet-Kabels mit dem Netzwerkanschluss und das andere Ende mit dem Uplink-Anschluss des Secure Access-Authentifizierungsgeräts verbinden.
4. Das Ethernet-Kabel des MFGs mit dem Downlink-Anschluss des Authentifizierungsgeräts verbinden.

   Hinweis: Nach dem Ausschalten des Authentifizierungsgeräts besteht vom Downlink-Anschluss aus keine Ethernet-Verbindung mehr. Alternativ kann das Ethernet-Kabel des MFGs direkt mit einem anderen Ethernet-Anschluss verbunden werden. Der Downlink-Anschluss des Authentifizierungsgeräts ist für den Fall gedacht, dass kein anderer Ethernet-Anschluss verfügbar ist.

5. Das Netzkabel des Authentifizierungsgeräts am Gerät und einer nahe gelegenen Steckdose anschließen.

Damit ist die Konfiguration der Hardware abgeschlossen. Nun kann entsprechend den Anweisungen im Secure Access-Systemhandbuch der Secure Access-Server konfiguriert und die Kommunikation zwischen den Authentifizierungsgeräten und den MFG aktiviert werden.

Installation des Secure Access-USB-Kartenlesers



1. Den Kartenleser mit dem im Lieferumfang enthaltenen Klettband auf der Ablage links neben dem Steuerpult des MFGs anbringen. Ist der optionale Offline-Hefter installiert, den Kartenleser rechts neben dem Hefter platzieren, so dass sich der Kartenleser zwischen Hefter und MFG befindet. **Vor dem Anbringen des Klettbands prüfen, ob sich die obere Abdeckung des Vorlageneinzugs ohne Behinderung durch den Kartenleser öffnen lässt.**
2. Das USB-Kabel des Kartenlesers an einem freien USB-Anschluss an der MFG-Rückseite anschließen.

   Weitere Möglichkeiten zur Anbringung sind der mit dem MFG gelieferten CD zur Systemverwaltung zu entnehmen.

Konfigurationsübersicht

Diese heraustrennbare Konfigurationsübersicht ist als Hilfsmittel bei der Einrichtung der Authentifizierungsgeräte gedacht. Die IP- und MAC-Adresse jedes Authentifizierungsgeräts und des von dem betreffenden Gerät kontrollierten MFGs sind hier sorgfältig einzutragen.

	Authentifizierungsgerät		MFG	
	MAC-Adresse	IP-Adresse	IP-Adresse	Hostname
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				