



# Markvision Enterprise

Versione 4.2

---

## Guida dell'amministratore

Settembre 2022

[www.lexmark.com](http://www.lexmark.com)

---

# Sommar

|                                                                                           |           |
|-------------------------------------------------------------------------------------------|-----------|
| <b>Cronologia delle modifiche.....</b>                                                    | <b>8</b>  |
| <b>Panoramica.....</b>                                                                    | <b>12</b> |
| Informazioni su Markvision Enterprise.....                                                | 12        |
| <b>Introduzione.....</b>                                                                  | <b>13</b> |
| Best practice.....                                                                        | 13        |
| Requisiti di sistema.....                                                                 | 15        |
| Lingue supportate.....                                                                    | 16        |
| Modelli di stampante supportati.....                                                      | 16        |
| Configurazione del database.....                                                          | 19        |
| Impostazione di Esegui come utente.....                                                   | 20        |
| Installazione di MVE.....                                                                 | 21        |
| Installazione di MVE invisibile all'utente.....                                           | 21        |
| Accesso a MVE.....                                                                        | 23        |
| Modifica della lingua.....                                                                | 24        |
| Modifica della password.....                                                              | 24        |
| <b>Manutenzione dell'applicazione.....</b>                                                | <b>25</b> |
| Aggiornamento a MVE 4.2.....                                                              | 25        |
| Backup e ripristino del database.....                                                     | 26        |
| Aggiornamento delle impostazioni del programma di installazione dopo l'installazione..... | 28        |
| <b>Configurazione dell'accesso utente.....</b>                                            | <b>29</b> |
| Panoramica.....                                                                           | 29        |
| Informazioni sui ruoli utente.....                                                        | 29        |
| Gestione degli utenti.....                                                                | 30        |
| Abilitazione dell'autenticazione tramite server LDAP.....                                 | 31        |
| Installazione dei certificati del server LDAP.....                                        | 33        |
| <b>Rilevamento delle stampanti.....</b>                                                   | <b>34</b> |
| Creazione di un profilo di ricerca.....                                                   | 34        |
| Gestione dei profili di ricerca.....                                                      | 36        |
| Scenario di esempio: rilevamento delle stampanti.....                                     | 37        |

**Gestione della dashboard di protezione..... 38**

|                                                                 |    |
|-----------------------------------------------------------------|----|
| Panoramica.....                                                 | 38 |
| Accesso al dashboard di protezione.....                         | 38 |
| Gestione di Informazioni sulla protezione della periferica..... | 38 |
| Gestione di Controllo conformità periferica.....                | 38 |

**Visualizzazione delle stampanti..... 40**

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Visualizzazione dell'elenco stampanti.....                                      | 40 |
| Visualizzazione delle informazioni della stampante.....                         | 43 |
| Esportazione dei dati della stampante.....                                      | 44 |
| Gestione delle visualizzazioni.....                                             | 44 |
| Modifica della visualizzazione dell'elenco stampanti.....                       | 46 |
| Filtraggio delle stampanti dalla barra di ricerca.....                          | 46 |
| Gestione delle parole chiave.....                                               | 47 |
| Uso delle ricerche salvate.....                                                 | 47 |
| Informazioni sugli stati del ciclo di vita della stampante.....                 | 47 |
| Esecuzione di una ricerca salvata.....                                          | 49 |
| Creazione di una ricerca salvata.....                                           | 49 |
| Informazioni sulle impostazioni delle regole di ricerca.....                    | 50 |
| Gestione delle ricerche salvate.....                                            | 53 |
| Scenario di esempio: monitoraggio dei livelli di toner del parco stampanti..... | 53 |

**Protezione delle comunicazioni della stampante..... 55**

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| Informazioni sugli stati di protezione della stampante.....                   | 55 |
| Protezione delle stampanti mediante le configurazioni predefinite.....        | 56 |
| Informazioni sulle autorizzazioni e i controlli di accesso alle funzioni..... | 58 |
| Configurazione della protezione della stampante.....                          | 58 |
| Protezione delle comunicazioni della stampante nel parco stampanti.....       | 59 |
| Altri modi per proteggere le stampanti.....                                   | 60 |

**Gestione delle stampanti..... 61**

|                                                             |    |
|-------------------------------------------------------------|----|
| Riavvio della stampante.....                                | 61 |
| Visualizzazione di Embedded Web Server della stampante..... | 61 |
| Controllo delle stampanti.....                              | 61 |
| Aggiornamento dello stato della stampante.....              | 61 |
| Impostazione dello stato della stampante.....               | 62 |
| Assegnazione di configurazioni alle stampanti.....          | 62 |

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Annullamento dell'assegnazione delle configurazioni.....                | 62 |
| Applicazione delle configurazioni.....                                  | 62 |
| Controllo della conformità di una stampante con una configurazione..... | 63 |
| Distribuzione dei file alle stampanti.....                              | 63 |
| Aggiornamento del firmware delle stampanti.....                         | 64 |
| Disinstallazione delle applicazioni dalle stampanti.....                | 65 |
| Assegnazione di eventi alle stampanti.....                              | 65 |
| Assegnazione di parole chiave alle stampanti.....                       | 65 |
| Immissione delle credenziali per le stampanti protette.....             | 66 |
| Configurazione manuale dei certificati predefiniti delle stampanti..... | 66 |
| Rimozione di stampanti.....                                             | 67 |

## **Gestione delle configurazioni..... 68**

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| Panoramica.....                                                                  | 68 |
| Creazione di una configurazione.....                                             | 68 |
| Creazione di una configurazione da una stampante.....                            | 71 |
| Scenario di esempio: clonazione di una configurazione.....                       | 71 |
| Creazione di un componente di protezione avanzata da una stampante.....          | 72 |
| Generazione di una versione stampabile delle impostazioni di configurazione..... | 72 |
| Informazioni sulle impostazioni dinamiche.....                                   | 72 |
| Informazioni sulle impostazioni delle variabili.....                             | 72 |
| Configurazione delle autorizzazioni per la stampa a colori.....                  | 73 |
| Creazione di un pacchetto di applicazioni.....                                   | 74 |
| Importazione o esportazione di una configurazione.....                           | 74 |
| Importazione di file nella libreria delle risorse.....                           | 75 |

## **Gestione dei certificati..... 76**

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| Configurazione di MVE per la gestione automatica dei certificati.....                                       | 76 |
| Informazioni sulla funzione di gestione automatica dei certificati .....                                    | 76 |
| Configurazione di MVE per la gestione automatica dei certificati .....                                      | 78 |
| Configurazione della CA Microsoft Enterprise con NDES.....                                                  | 80 |
| Gestione dei certificati con l'autorità di certificazione Microsoft tramite SCEP.....                       | 81 |
| Panoramica .....                                                                                            | 81 |
| Installazione del server CA radice .....                                                                    | 81 |
| Configurazione della CA Microsoft Enterprise con NDES.....                                                  | 82 |
| Configurazione del server CA subordinata .....                                                              | 83 |
| Configurazione delle impostazioni Punto di distribuzione CRL e Accesso alle informazioni dell'autorità..... | 84 |
| Configurazione dell'accessibilità al CRL .....                                                              | 85 |

|                                                                                                  |     |
|--------------------------------------------------------------------------------------------------|-----|
| Configurazione del server NDES .....                                                             | 85  |
| Configurazione di NDES per MVE .....                                                             | 86  |
| Gestione dei certificati con l'autorità di certificazione Microsoft tramite MSCEWS.....          | 88  |
| Requisiti di sistema .....                                                                       | 88  |
| Requisiti di connettività di rete.....                                                           | 88  |
| Creazione di certificati SSL per i server CEP e CES.....                                         | 89  |
| Creazione di modelli di certificato .....                                                        | 90  |
| Informazioni sui metodi di autenticazione .....                                                  | 90  |
| Requisiti di delega .....                                                                        | 91  |
| Configurazione dell'autenticazione integrata di Windows.....                                     | 92  |
| Configurazione dell'autenticazione con certificato client.....                                   | 94  |
| Configurazione dell'autenticazione con nome utente-password.....                                 | 97  |
| Gestione dei certificati con l'autorità di certificazione OpenXPKI tramite SCEP.....             | 99  |
| Configurazione di OpenXPKI CA .....                                                              | 99  |
| Configurazione manuale di OpenXPKI CA .....                                                      | 102 |
| Generazione delle informazioni del CRL .....                                                     | 107 |
| Configurazione dell'accessibilità al CRL .....                                                   | 108 |
| Abilitazione del servizio SCEP .....                                                             | 108 |
| Abilitazione del certificato del "firmatario per conto di" (agente di registrazione) .....       | 109 |
| Abilitazione dell'approvazione automatica delle richieste di certificato in OpenXPKI CA .....    | 109 |
| Creazione di una seconda area di autenticazione .....                                            | 110 |
| Abilitazione della presenza contemporanea di più certificati attivi .....                        | 113 |
| Impostazione del numero di porta predefinito per OpenXPKI CA.....                                | 113 |
| Rifiuto delle richieste di certificati senza password di verifica in OpenXPKI CA.....            | 113 |
| Aggiunta dell'EKU di autenticazione client nei certificati .....                                 | 114 |
| Recupero dell'oggetto del certificato completo quando si effettua la richiesta tramite SCEP..... | 114 |
| Revoca dei certificati e pubblicazione del CRL .....                                             | 115 |
| Gestione dei certificati con l'autorità di certificazione OpenXPKI tramite EST.....              | 116 |
| Configurazione di OpenXPKI CA .....                                                              | 116 |
| Configurazione manuale di OpenXPKI CA .....                                                      | 119 |
| Creazione di una seconda area di autenticazione .....                                            | 127 |

## **Gestione degli avvisi della stampante..... 133**

|                                                |     |
|------------------------------------------------|-----|
| Panoramica.....                                | 133 |
| Creazione di un'azione.....                    | 133 |
| Comprensione segnaposto azione.....            | 134 |
| Gestione delle azioni.....                     | 135 |
| Creazione di un evento.....                    | 135 |
| Informazioni sugli avvisi della stampante..... | 136 |
| Gestione degli eventi.....                     | 140 |

|                                                                                                                               |            |
|-------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Visualizzazione della cronologia e dello stato delle attività.....</b>                                                     | <b>141</b> |
| Panoramica.....                                                                                                               | 141        |
| Visualizzazione dello stato delle attività.....                                                                               | 141        |
| Interruzione delle attività.....                                                                                              | 141        |
| visualizzazione dei registri.....                                                                                             | 141        |
| Eliminazione dei registri.....                                                                                                | 141        |
| Esportazione dei registri.....                                                                                                | 142        |
| <b>Programmazione delle attività.....</b>                                                                                     | <b>143</b> |
| Creazione di un programma.....                                                                                                | 143        |
| Gestione delle attività programmate.....                                                                                      | 144        |
| <b>Esecuzione di altre attività amministrative.....</b>                                                                       | <b>145</b> |
| Configurazione delle impostazioni generali.....                                                                               | 145        |
| Configurazione delle impostazioni e-mail.....                                                                                 | 145        |
| Aggiunta di una declinazione di responsabilità prima dell'accesso.....                                                        | 146        |
| Firma del certificato MVE.....                                                                                                | 146        |
| Rimozione di informazioni e riferimenti dell'utente.....                                                                      | 147        |
| <b>Domande frequenti.....</b>                                                                                                 | <b>149</b> |
| Domande frequenti su Markvision Enterprise.....                                                                               | 149        |
| <b>Risoluzione dei problemi.....</b>                                                                                          | <b>152</b> |
| L'utente ha dimenticato la password.....                                                                                      | 152        |
| L'utente amministratore ha dimenticato la password.....                                                                       | 152        |
| La pagina non viene caricata.....                                                                                             | 153        |
| Impossibile rilevare una stampante di rete.....                                                                               | 153        |
| Informazioni stampante errate.....                                                                                            | 153        |
| MVE non riconosce una stampante come stampante protetta.....                                                                  | 154        |
| L'applicazione di configurazioni con più applicazioni non riesce al primo tentativo ma riesce con i tentativi successivi..... | 154        |
| L'applicazione di configurazioni con il certificato della stampante non riesce.....                                           | 155        |
| Autorità di certificazione OpenXPki.....                                                                                      | 155        |
| <b>Appendice.....</b>                                                                                                         | <b>158</b> |
| <b>Avvertenze.....</b>                                                                                                        | <b>162</b> |

---

|                       |            |
|-----------------------|------------|
| <b>Glossario.....</b> | <b>164</b> |
| <b>Indice.....</b>    | <b>165</b> |

# Cronologia delle modifiche

## Agosto 2022

- Aggiunte informazioni sui seguenti argomenti:
  - Protocollo Enrollment over Secure Transport (EST) come definito in RFC 7030
  - Dashboard di protezione
  - Assegnazione automatica delle parole chiave durante il rilevamento
  - Supporto per e-mail tramite SSL/TLS
  - Supporto per Windows Server 2022
- Aggiornate le informazioni relative ai seguenti argomenti:
  - Modelli di stampante supportati
  - Gestione dei certificati con l'autorità di certificazione Microsoft tramite i servizi Web di registrazione certificati di Microsoft (MSCEWS)
  - Configurazione del server OpenXPki CA
  - Gestione delle configurazioni MVE

## Marzo 2022

- Aggiornate le informazioni sui modelli di stampante supportati.
- Aggiunte informazioni sulla creazione di un certificato client.

## Maggio 2021

- Aggiornate le informazioni relative ai seguenti argomenti:
  - Modelli di stampante supportati
  - Gestione dell'autorità di certificazione (CA) Microsoft
  - Configurazione di Markvision™ Enterprise (MVE) per la gestione automatica dei certificati
  - Configurazione dell'autorità di certificazione Microsoft Enterprise con il servizio Registrazione dispositivi di rete (NDES)
- Aggiunte informazioni sui seguenti argomenti:
  - Gestione dei certificati con l'autorità di certificazione Microsoft tramite i servizi Web di registrazione certificati di Microsoft (MSCEWS)
  - Creazione del certificato SSL per i server del servizio Web di informazioni sulle registrazioni di certificati (CEP) e del servizio Web di registrazione certificati (CES)
  - Metodi di autenticazione per CEP e CES
  - Certificato periferica con nome

## Novembre 2020

- Aggiornate le informazioni relative ai seguenti argomenti:
  - Modelli di stampante supportati
  - Database supportati



- Aggiunte informazioni sui seguenti argomenti:
  - Gestione e implementazione delle configurazioni
  - Backup e ripristino del database
  - Gestione dei certificati tramite autorità di certificazione OpenXPki e Microsoft
- Aggiunto il supporto per le seguenti operazioni:
  - Gestione e implementazione delle configurazioni in un gruppo di modelli di stampante
  - Creazione di nomi di database personalizzati

## Febbraio 2020

- Aggiornate le informazioni relative ai seguenti argomenti:
  - Modelli di stampante supportati
  - Server supportati
  - Database supportati
  - Percorso di aggiornamento di MVE valido
- Aggiunte informazioni sui seguenti argomenti:
  - Istruzioni per le best practice
  - Istruzioni sulla gestione dei certificati automatici
  - Componenti di protezione avanzata predefiniti e relative impostazioni
  - Altri modi per proteggere le stampanti
  - Scenari di esempio

## Giugno 2019

- Aggiornate le informazioni relative ai seguenti argomenti:
  - Note a piè pagina aggiunte ai modelli di stampante che richiedono l'uso di certificati
  - Assegnazione di diritti dbo durante la configurazione del database
  - Percorso di aggiornamento valido quando si esegue l'aggiornamento alla versione 3.4
  - File necessari per il backup e il ripristino del database
  - Impostazioni per l'autenticazione tramite server LDAP
  - Parametri relativi a stato di validità del certificato, data e fuso orario aggiunti alle impostazioni delle regole di ricerca
  - Configurazione delle autorizzazioni e dei controlli di accesso alle funzioni nelle impostazioni di protezione della stampante
  - Selezione di un file del firmware dalla libreria delle risorse durante l'aggiornamento del firmware della stampante
  - Selezione della data di inizio, dell'ora di inizio e di pausa e dei giorni della settimana per l'aggiornamento del firmware della stampante
  - Gestione delle configurazioni
- Aggiunte informazioni sui seguenti argomenti:
  - Informazioni sugli stati di protezione della stampante
  - Configurazione dei componenti di protezione avanzata
  - Creazione di un componente di protezione avanzata da una stampante
  - Generazione di una versione stampabile delle impostazioni di configurazione

- Caricamento dell'autorità di certificazione di un parco stampanti
- Rimozione di informazioni e riferimenti dell'utente
- Informazioni sulle autorizzazioni e sui controlli di accesso alle funzioni
- Operazioni di risoluzione dei problemi quando l'applicazione di configurazioni con più applicazioni non riesce
- Operazioni di risoluzione dei problemi quando un utente Amministratore dimentica la password

## **Agosto 2018**

- Aggiornate le informazioni relative ai seguenti argomenti:
  - Modelli di stampante supportati
  - Configurazione del database
  - Aggiornamento a MVE 3.3
  - Domande frequenti
  - Creazione di un'azione
  - Creazione di un programma
- Aggiunte informazioni sui seguenti argomenti:
  - Configurazione di un account utente di dominio RunAs
  - Esportazione dei registri
  - Operazioni per la risoluzione dei problemi quando MVE non riconosce stampanti protette

## **Luglio 2018**

- Aggiornate le informazioni sull'aggiornamento a MVE 3.2.

## **Aprile 2018**

- Aggiornate le informazioni relative ai seguenti argomenti:
  - Modelli di stampante supportati
  - Configurazione del database
  - Backup e ripristino dei file del database
  - URL di accesso a MVE
  - Informazioni sulle impostazioni delle variabili
- Aggiunte informazioni sui seguenti argomenti:
  - Configurazione dei certificati delle stampanti
  - Interruzione delle attività
  - Aggiornamento del firmware delle stampanti

## **Settembre 2017**

- Aggiornate le informazioni relative ai seguenti argomenti:
  - Requisiti di sistema
  - Comunicazione tra MVE e i modelli Lexmark<sup>TM</sup> Forms Printer 2580, 2581, 2590 e 2591
  - Rimozione manuale dei database di Microsoft SQL Server
  - Backup e ripristino dei file del database

- Impostazioni di protezione richieste per i controlli di accesso alle funzioni durante la distribuzione dei file del firmware e delle soluzioni alle stampanti
- Supporto per le licenze durante la distribuzione delle applicazioni
- Avvisi della stampante e azioni associate
- Ripristino automatico dello stato della stampante
- Assegnazione di eventi e parole chiave

## **Giugno 2017**

- Versione iniziale del documento per MVE 3.0.

# Panoramica

## Informazioni su Markvision Enterprise

Markvision Enterprise (MVE) è un software di utilità per la gestione delle stampanti basato su Web e destinato a professionisti IT.

Con MVE, è possibile gestire un ampio parco stampanti in un ambiente aziendale in modo efficiente, effettuando le seguenti operazioni:

- Rilevare, organizzare e tracciare un parco stampanti. È possibile controllare una stampante per raccogliere i dati ad essa relativi, ad esempio lo stato, le impostazioni e i materiali di consumo.
- Creare configurazioni e assegnarle alle stampanti.
- Implementare il firmware, i certificati della stampante, le autorità di certificazione (CA, Certificate Authority) e le applicazioni sulle stampanti.
- Controllare gli avvisi e gli eventi della stampante.

Questo documento fornisce informazioni su configurazione, utilizzo e risoluzione dei problemi relativi all'applicazione.

Questo documento è destinato agli amministratori.

# Introduzione

## Best practice

Questo argomento descrive le procedure consigliate per utilizzare MVE per la gestione efficace del parco stampanti.

### 1 Installare MVE nell'ambiente.

- a** Creare un server utilizzando l'ambiente Windows Server più recente.

Contenuto correlato:

[Requisiti del server Web](#)

- b** Creare un account utente di dominio che non disponga di accesso amministratore.

Contenuto correlato:

[Impostazione di Esegui come utente](#)

- c** Creare un database Microsoft SQL Server, configurare la crittografia e quindi concedere al nuovo account utente l'accesso ai database.

Contenuto correlato:

- [Requisiti del database](#)
- [Configurazione del database](#)

- d** Installare MVE utilizzando l'account utente di dominio e SQL Server con autenticazione Windows.

Contenuto correlato:

[Installazione di MVE](#)

### 2 Configurare MVE, quindi rilevare e organizzare il parco stampanti.

- a** Firmare il certificato del server.

Contenuto correlato:

- [Firma del certificato MVE](#)
- [Configurazione di MVE per la gestione automatica dei certificati](#)

- b** Configurare le impostazioni LDAP.

Contenuto correlato:

- [Abilitazione dell'autenticazione tramite server LDAP](#)
- [Installazione dei certificati LDAP](#)

- c** Eseguire la connessione a un server e-mail.

Contenuto correlato:

[Configurazione delle impostazioni e-mail](#)

- d** Rilevare il parco stampanti.

Contenuto correlato:

[Rilevamento delle stampanti](#)

- e** Programmare i controlli e gli aggiornamenti dello stato.

Contenuto correlato:

- [Controllo delle stampanti](#)
- [Aggiornamento dello stato della stampante](#)

- f** Configurare le impostazioni di base, ad esempio nomi di contatti, posizioni, etichette risorsa e fusi orari.
- g** Organizzare il parco stampanti. Utilizzare parole chiave, ad esempio le posizioni, per categorizzare le stampanti.

Contenuto correlato:

- [Assegnazione di parole chiave alle stampanti](#)
- [Creazione di una ricerca salvata](#)

### **3** Proteggete il parco stampanti.

- a** Proteggere l'accesso alla stampante utilizzando i componenti di protezione avanzata predefiniti.

Contenuto correlato:

- [Protezione delle stampanti mediante le configurazioni predefinite](#)
- [Informazioni sulle autorizzazioni e i controlli di accesso alle funzioni](#)
- [Altri modi per proteggere le stampanti](#)

- b** Creare una configurazione protetta che includa i certificati.

Contenuto correlato:

- [Creazione di una configurazione](#)
- [Importazione di file nella libreria delle risorse](#)

- c** Applicare la configurazione al parco stampanti corrente.

Contenuto correlato:

- [Assegnazione di configurazioni alle stampanti](#)
- [Applicazione delle configurazioni](#)

- d** Programmare le applicazioni e le verifiche di conformità.

Contenuto correlato:

[Creazione di un programma](#)

- e** Aggiungere configurazioni ai profili di ricerca per proteggere le nuove stampanti.

Contenuto correlato:

[Creazione di un profilo di ricerca](#)

- f** Firmare i certificati delle stampanti.

Contenuto correlato:

[Firma del certificato MVE](#)

### **4** Mantenere aggiornato il firmware.

Contenuto correlato:

[Aggiornamento del firmware delle stampanti](#)

### **5** Installare e configurare le applicazioni.

Contenuto correlato:

- [Creazione di una configurazione](#)
- [Importazione di file nella libreria delle risorse](#)

## 6 Monitorare il parco stampanti.

Contenuto correlato:

[Creazione di una ricerca salvata](#)

## Requisiti di sistema

È installato MVE come server Web ed è possibile accedervi da un browser Web su qualsiasi computer collegato alla rete. MVE utilizza inoltre un database per memorizzare le informazioni relative al parco stampanti. Di seguito vengono indicati i requisiti per server Web, database e sistema utente:

### Requisiti del server Web

|                          |                                                                                    |
|--------------------------|------------------------------------------------------------------------------------|
| <b>Processore</b>        | Processore dual-core da almeno 2 GHz che utilizza HTT (Hyper-Threading Technology) |
| <b>RAM</b>               | Almeno 4 GB                                                                        |
| <b>Unità disco fisso</b> | Almeno 60 GB                                                                       |

**Nota:** MVE, Lexmark Document Distributor (LDD) e Utilità di distribuzione delle periferiche non possono essere eseguiti sullo stesso server.

### Server supportati

- Windows Server 2022 Standard Edition
- Windows Server 2019
- Windows Server 2016 Standard Edition
- Windows Server 2012 Standard Edition
- Windows Server 2012 R2

**Nota:** MVE supporta la virtualizzazione per i server supportati in un ambiente locale.

### Requisiti del database

#### Database supportati

- Firebird® (database integrato)
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

**Nota:** la dimensione minima consigliata del database è 60 GB per allocare 20 MB per FRAMEWORK e 4,5 MB per MONITOR e QUARTZ. Per ulteriori informazioni, vedere ["Configurazione del database" a pagina 19](#).

## Requisiti del sistema utente

### Browser Web supportati

- Microsoft Edge
- Mozilla Firefox (versione più recente)
- Google Chrome™ (versione più recente)
- Apple Safari (versione più recente)

### Risoluzione schermo

Almeno 1280 x 768 pixel

## Lingue supportate

- Portoghese brasiliano
- Inglese
- Francese
- Tedesco
- Italiano
- Cinese semplificato
- Spagnolo

## Modelli di stampante supportati

- Lexmark 6500
- Lexmark B2236<sup>2</sup>
- Lexmark B2338<sup>2</sup>, B2442<sup>2</sup>, B2546<sup>2</sup>, B2650<sup>2</sup>, B2865<sup>1</sup>
- Lexmark B3440<sup>2</sup>, B3442<sup>2</sup>
- Lexmark C2132
- Lexmark C2240<sup>2</sup>, C2325<sup>2</sup>, C2425<sup>2</sup>, C2535<sup>2</sup>
- Lexmark C2335<sup>2</sup>
- Lexmark C3224<sup>2</sup>
- Lexmark C3326<sup>2</sup>
- Lexmark C3426<sup>2</sup>
- Lexmark C4150<sup>2</sup>, C6160<sup>2</sup>, C9235<sup>2</sup>
- Lexmark C4342<sup>2</sup>, C4352<sup>2</sup>
- Lexmark C746, C748
- Lexmark C792
- Lexmark C925<sup>1</sup>, C950
- Lexmark CS310, CS410, CS510
- Lexmark CS317, CS417, CS517
- Lexmark CS331<sup>2</sup>
- Lexmark CS421<sup>2</sup>, CS521<sup>2</sup>, CS622<sup>2</sup>



- Lexmark CS431<sup>2</sup>
- Lexmark CS531<sup>2</sup>, CS632<sup>2</sup>
- Lexmark CS720<sup>2</sup>, CS725<sup>2</sup>
- Lexmark CS727<sup>2</sup>, CS728<sup>2</sup>
- Lexmark CS730<sup>2</sup>
- Lexmark CS735<sup>2</sup>
- Lexmark CS820<sup>2</sup>, CS827<sup>2</sup>
- Lexmark CS921<sup>2</sup>, CS923<sup>2</sup>, CS927<sup>2</sup>
- Lexmark CS943<sup>2</sup>
- Lexmark CX310, CX410, CX510
- Lexmark CX317, CX417, CX517
- Lexmark CX331<sup>2</sup>
- Lexmark CX421<sup>2</sup>, CX522<sup>2</sup>, CX622<sup>2</sup>, CX625<sup>2</sup>
- Lexmark CX431<sup>2</sup>
- Lexmark CX532<sup>2</sup>
- Lexmark CX625<sup>2</sup>
- Lexmark CX635<sup>2</sup>
- Lexmark CX725<sup>2</sup>
- Lexmark CX728<sup>2</sup>
- Lexmark CX730<sup>2</sup>
- Lexmark CX735<sup>2</sup>
- Lexmark CX820<sup>2</sup>, CX825<sup>2</sup>, CX827<sup>2</sup>, CX860<sup>2</sup>
- Lexmark CX920<sup>2</sup>, CX921<sup>2</sup>, CX922<sup>2</sup>, CX923<sup>2</sup>, CX924<sup>2</sup>, CX927<sup>2</sup>
- Lexmark CX930<sup>2</sup>, CX931<sup>2</sup>
- Lexmark CX942<sup>2</sup>, CX943<sup>2</sup>, CX944<sup>2</sup>
- Lexmark Forms Printer 2580<sup>4</sup>, 2581<sup>4</sup>, 2590<sup>4</sup>, 2591<sup>4</sup>
- Lexmark M1140, M1145, M3150
- Lexmark M1242<sup>2</sup>, M1246<sup>2</sup>, M3250<sup>2</sup>, M5255<sup>2</sup>, M5265<sup>2</sup>, M5270<sup>2</sup>
- Lexmark M3350<sup>2</sup>
- Lexmark M5155, M5163, M5170
- Lexmark M5255<sup>2</sup>, M5265<sup>2</sup>, M5270<sup>2</sup>
- Lexmark MB2236<sup>2</sup>
- Lexmark MB2338<sup>2</sup>, MB2442<sup>2</sup>, MB2546<sup>2</sup>, MB2650<sup>2</sup>, MB2770<sup>2</sup>
- Lexmark MB3442<sup>2</sup>
- Lexmark MC2325<sup>2</sup>, MC2425<sup>2</sup>, MC2535<sup>2</sup>, MC2640<sup>2</sup>
- Lexmark MC3224<sup>2</sup>
- Lexmark MC3326<sup>2</sup>
- Lexmark MC3426<sup>2</sup>
- Lexmark MS310, MS312, MS315, MS410, MS415, MS510, MS610
- Lexmark MS317, MS417, MS517
- Lexmark MS321<sup>2</sup>, MS421<sup>2</sup>, MS521<sup>2</sup>, MS621<sup>2</sup>, MS622<sup>2</sup>

- Lexmark MS331<sup>2</sup>, MS431<sup>2</sup>
- Lexmark MS531<sup>2</sup>, MS631<sup>2</sup>, MS632<sup>2</sup>
- Lexmark MS617, MS817, MS818
- Lexmark MS710, MS711, MS810, MS811, MS812
- Lexmark MS725<sup>2</sup>, MS821<sup>2</sup>, MS822<sup>2</sup>, MS823<sup>2</sup>, MS824<sup>2</sup>, MS825<sup>2</sup>, MS826<sup>2</sup>
- Lexmark MS911
- Lexmark MX310, MX410, MX510, MX511, MX610, MX611
- Lexmark MX317, MX417, MX517
- Lexmark MX321<sup>2</sup>, MX421<sup>2</sup>, MX521<sup>2</sup>, MX522<sup>2</sup>, MX622<sup>2</sup>
- Lexmark MX331<sup>2</sup>, MX431<sup>2</sup>
- Lexmark MX432<sup>2</sup>
- Lexmark MX532<sup>2</sup>, MX632<sup>2</sup>
- Lexmark MX617, MX717, MX718
- Lexmark MX6500
- Lexmark MX710, MX711, MX810, MX811, MX812
- Lexmark MX721<sup>2</sup>, MX722<sup>2</sup>, MX725<sup>2</sup>, MX822<sup>2</sup>, MX824<sup>2</sup>, MX826<sup>2</sup>
- Lexmark MX910, MX911, MX912
- Lexmark MX931<sup>2</sup>
- Lexmark T650<sup>1</sup>, T652<sup>1</sup>, T654<sup>1</sup>, T656<sup>1</sup>
- Lexmark X651<sup>1</sup>, X652<sup>1</sup>, X654<sup>1</sup>, X656<sup>1</sup>, X658<sup>1</sup>, XS651<sup>1</sup>, XS652<sup>1</sup>, XS654<sup>1</sup>, XS658<sup>1</sup>
- Lexmark X746, X748, X792
- Lexmark X850<sup>1</sup>, X852<sup>1</sup>, X854<sup>1</sup>, X860<sup>1</sup>, X862<sup>1</sup>, X864<sup>1</sup>, XS864<sup>1</sup>
- Lexmark X925, X950, X952, X954
- Lexmark XC2130, XC2132
- Lexmark XC2235<sup>2</sup>, XC2240<sup>2</sup>, XC4240<sup>2</sup>
- Lexmark XC2335<sup>2</sup>
- Lexmark XC4140<sup>2</sup>, XC4150<sup>2</sup>, XC6152<sup>2</sup>, XC8155<sup>2</sup>, XC8160<sup>2</sup>
- Lexmark XC9225<sup>2</sup>, XC9235<sup>2</sup>, XC9245<sup>2</sup>, XC9255<sup>2</sup>, XC9265<sup>2</sup>
- Lexmark XC9325<sup>2</sup>, XC9335<sup>2</sup>
- Lexmark XC9445<sup>2</sup>, XC9455<sup>2</sup>, XC9465<sup>2</sup>
- Lexmark XM1135, XM1140, XM1145, XM3150
- Lexmark XM1242<sup>2</sup>, XM1246<sup>2</sup>, XM3250<sup>2</sup>
- Lexmark XM3142<sup>2</sup>
- Lexmark XM3350<sup>2</sup>
- Lexmark XM5163, XM5170, XM5263, XM5270
- Lexmark XM5365<sup>2</sup>, XM5370<sup>2</sup>
- Lexmark XM7155, XM7163, XM7170, XM7263, XM7270
- Lexmark XM7355<sup>2</sup>, MX7365<sup>2</sup>, MX7370<sup>2</sup>
- Lexmark XM9145, XM9155, XM9165
- Lexmark XM9335<sup>2</sup>
- Lexmark XC2326

- Lexmark XC2326
- Lexmark XC4342<sup>2</sup>, XC4352<sup>2</sup>

<sup>1</sup> È richiesto un aggiornamento del certificato della stampante. In questa versione, l'aggiornamento delle prestazioni e della protezione della piattaforma Java rimuove il supporto di alcuni algoritmi di firma del certificato, quali MD5 e SHA1. Questa modifica impedisce a MVE di funzionare su alcune stampanti. Per ulteriori informazioni, consultare la [relativa guida](#).

<sup>2</sup> È necessario attivare il supporto di SNMPv3 sulla stampante.

<sup>3</sup> Se sulla stampante è impostata una password di protezione avanzata, MVE non è in grado di supportare la stampante.

<sup>4</sup> MVE non può comunicare con i modelli Lexmark Forms Printer 2580, 2581, 2590 e 2591 con stato Non pronta. La comunicazione avviene solo se MVE ha comunicato in precedenza con la stampante in stato Pronta. La stampante potrebbe essere nello stato Non pronta quando si ricevono errori o avvertenze, ad esempio di materiali di consumo esauriti. Per modificare lo stato, risolvere l'errore o l'avvertenza, quindi premere **Pronta**.

## Configurazione del database

È possibile utilizzare Firebird o Microsoft SQL Server come database back-end. La tabella seguente può aiutare a scegliere il database da utilizzare.

|                                 | Firebird                                                                                                                                                                  | Microsoft SQL Server                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Installazione del server</b> | Deve essere installato sullo stesso server di MVE.                                                                                                                        | Può essere eseguito da qualsiasi server.                                                                                                                                     |
| <b>Comunicazione</b>            | Bloccato a soli localhost.                                                                                                                                                | Comunica tramite una porta statica o un'istanza dinamica denominata.<br>È supportata la comunicazione SSL/TLS con un server Microsoft SQL protetto.                          |
| <b>Prestazioni</b>              | Problemi di prestazioni con grandi parchi stampanti.                                                                                                                      | Migliori prestazioni per grandi parchi stampanti.                                                                                                                            |
| <b>Dimensioni del database</b>  | Le dimensioni predefinite per i database sono 6 MB per FRAMEWORK e 1 MB per MONITOR e QUARTZ. La tabella FRAMEWORK aumenta di 1 KB per ogni record di stampante aggiunto. | Le dimensioni predefinite per i database sono 20 MB per FRAMEWORK e 4,5 MB per MONITOR e QUARTZ. La tabella FRAMEWORK aumenta di 1 KB per ogni record di stampante aggiunto. |
| <b>Configurazione</b>           | Configurato automaticamente durante il processo di installazione.                                                                                                         | Richiede configurazione di pre-installazione.                                                                                                                                |

Se si utilizza Firebird, il programma di installazione MVE installa e configura Firebird senza richiedere altre configurazioni.

Se si utilizza Microsoft SQL Server, prima di installare MVE attenersi alla seguente procedura:

- Consentire l'esecuzione automatica dell'applicazione.
- Impostare le librerie di rete per l'utilizzo dei socket TCP/IP.
- Creare i seguenti database:

**Nota:** i seguenti sono i nomi di database predefiniti. È anche possibile fornire nomi di database personalizzati.

- FRAMEWORK
- MONITOR
- QUARTZ

- Se si utilizza un'istanza denominata, impostare l'avvio automatico del servizio Microsoft SQL Server Browser. In alternativa, impostare una porta statica sui socket TCP/IP.
- Creare un account utente con diritti dbowner per tutti e tre i database utilizzati da MVE per connettersi al database e per configurarlo. Se l'utente corrisponde a un account Microsoft SQL Server, attivare Microsoft SQL Server e le modalità Autenticazione di Windows su Microsoft SQL Server.

**Nota:** la disinstallazione di MVE configurato per l'uso di Microsoft SQL Server non comporta la rimozione dei database o delle tabelle create. Dopo la disinstallazione, i database FRAMEWORK, MONITOR e QUARTZ devono essere rimossi manualmente.

- Assegnare i diritti dbo all'utente del database, quindi impostare lo schema dbo come lo schema predefinito.

## Impostazione di Esegui come utente

Durante l'installazione, è possibile specificare l'esecuzione di MVE come un account di sistema locale o come un account utente di dominio. L'esecuzione di MVE come account Esegui come utente di dominio fornisce un'installazione più sicura. L'account utente del dominio dispone di privilegi limitati rispetto a un account di sistema locale.

|                                                  | Esegui come utente di dominio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Esegui come sistema locale                                       |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| <b>Autorizzazioni di sistema locale</b>          | <ul style="list-style-type: none"> <li>• Accesso per tutti i file a quanto segue: <ul style="list-style-type: none"> <li>– \$MVE_INSTALL/tomcat/logs</li> <li>– \$MVE_INSTALL/tomcat/temp</li> <li>– \$MVE_INSTALL/tomcat/work</li> <li>– \$MVE_INSTALL/apps/library</li> <li>– \$MVE_INSTALL/apps/dm-mve/picture</li> <li>– \$MVE_INSTALL/./mve_truststore*</li> <li>– \$MVE_INSTALL/jre/lib/security/cacerts</li> <li>– \$MVE_INSTALL/apps/dm-mve/WEB-INF/ldap</li> <li>– \$MVE_INSTALL/apps/dm-mve/download</li> </ul> Dove \$MVE_INSTALL è la directory di installazione.</li> <li>• Privilegi di Windows: LOGON_AS_A_SERVICE</li> </ul> | Autorizzazioni di amministratore                                 |
| <b>Autenticazione della connessione database</b> | <ul style="list-style-type: none"> <li>• Autenticazione di Windows con Microsoft SQL Server</li> <li>• Autenticazione SQL</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Autenticazione SQL                                               |
| <b>Configurazione</b>                            | Un utente del dominio deve essere configurato prima dell'installazione.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Configurato automaticamente durante il processo di installazione |

Se si utilizza l'impostazione MVE come Esegui come account utente di dominio, creare l'utente sullo stesso dominio del server MVE.

## Installazione di MVE

- 1 Trasferire il file eseguibile in un percorso il cui nome non contenga spazi.
- 2 Eseguire il file come amministratore, quindi seguire le istruzioni visualizzate sullo schermo del computer.

### Note:

- Le password sono autenticate tramite hash e memorizzate in modo sicuro. Assicurarsi di memorizzare le password o di conservarle in una posizione sicura in quanto non possono essere decrittografate una volta archiviate.
- Se ci si connette a Microsoft SQL Server utilizzando l'autenticazione di Windows, non viene effettuata alcuna verifica della connessione durante l'installazione. Assicurarsi che l'utente designato per eseguire il servizio MVE di Windows abbia un account corrispondente nell'istanza di Microsoft SQL Server. L'utente designato deve avere i diritti dbowner per i database FRAMEWORK, MONITOR e QUARTZ.

## Installazione di MVE invisibile all'utente

### Impostazioni del database per l'installazione invisibile all'utente

| Impostazione                                        | Descrizione                                          | Valore                                                                                                                                                                            |
|-----------------------------------------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--help</b>                                       | Mostra l'elenco delle opzioni valide.                |                                                                                                                                                                                   |
| <b>--version</b>                                    | Mostra le informazioni sul prodotto.                 |                                                                                                                                                                                   |
| <b>--unattendedmodeui &lt;unattended-modeui&gt;</b> | L'interfaccia utente per la modalità automatica.     | Predefinito: <b>none</b><br>Consentito: <ul style="list-style-type: none"> <li>• <b>none</b></li> <li>• <b>minimal</b></li> <li>• <b>minimalWithDialogs</b></li> </ul>            |
| <b>--optionfile &lt;optionfile&gt;</b>              | Il file delle opzioni di installazione.              | Predefinito:                                                                                                                                                                      |
| <b>--debuglevel &lt;debuglevel&gt;</b>              | Il livello di dettaglio delle informazioni di debug. | Predefinito: <b>2</b><br>Consentito: <ul style="list-style-type: none"> <li>• <b>0</b></li> <li>• <b>1</b></li> <li>• <b>2</b></li> <li>• <b>3</b></li> <li>• <b>4</b></li> </ul> |
| <b>--mode &lt;mode&gt;</b>                          | La modalità di installazione.                        | Predefinito: <b>win32</b><br>Consentito: <ul style="list-style-type: none"> <li>• <b>win32</b></li> <li>• <b>unattended</b></li> </ul>                                            |
| <b>--debugtrace &lt;debugtrace&gt;</b>              | Il nome file di debug.                               | Predefinito:                                                                                                                                                                      |

| Impostazione                                                      | Descrizione                                       | Valore                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--installer-language &lt;installer-language&gt;</code>      | La selezione della lingua.                        | Predefinito: <b>en</b><br>Consentito:<br><ul style="list-style-type: none"> <li>• <b>en</b></li> <li>• <b>es</b></li> <li>• <b>de</b></li> <li>• <b>fr</b></li> <li>• <b>it</b></li> <li>• <b>pt_BR</b></li> <li>• <b>zh_CN</b></li> </ul> |
| <code>--encryptionKey &lt;encryptionKey&gt;</code>                | La chiave di crittografia.                        | Chiave di crittografia:<br>Predefinito:                                                                                                                                                                                                    |
| <code>--prefix &lt;prefix&gt;</code>                              | La directory di installazione.                    | Predefinito: <b>C:\Programmi</b>                                                                                                                                                                                                           |
| <code>--mveLexmark_runas &lt;mveLexmark_runas&gt;</code>          | Le opzioni di utente utilizzato per l'esecuzione. | Predefinito: <b>LOCAL_SYSTEM</b><br>Consentito:<br><ul style="list-style-type: none"> <li>• <b>LOCAL_SYSTEM</b></li> <li>• <b>SPECIFIC_USER</b></li> </ul>                                                                                 |
| <code>--serviceRunAsUsername &lt;service-RunAsUsername&gt;</code> | Il nome utente utilizzato per l'esecuzione.       | Nome utente:<br>Predefinito:                                                                                                                                                                                                               |
| <code>--serviceRunAsPassword &lt;service-RunAsPassword&gt;</code> | La password utente utilizzata per l'esecuzione.   | Password:<br>Predefinito:                                                                                                                                                                                                                  |
| <code>--mveLexmark_database &lt;mveLexmark_database&gt;</code>    | Il tipo di database.                              | Predefinito:<br>Consentito:<br><ul style="list-style-type: none"> <li>• <b>FIREBIRD</b></li> <li>• <b>SQL_SERVER</b></li> </ul>                                                                                                            |
| <code>--firebirdUsername &lt;firebirdUsername&gt;</code>          | Il nome utente del database Firebird.             | Nome utente:<br>Predefinito:                                                                                                                                                                                                               |
| <code>--firebirdPassword &lt;firebirdPassword&gt;</code>          | La password del database Firebird.                | Password:<br>Predefinito:                                                                                                                                                                                                                  |
| <code>--firebirdFWDbName &lt;firebirdFWDbName&gt;</code>          | Il nome del database Firebird per FRAMEWORK.      | Nomi database:<br>Predefinito: <b>FRAMEWORK</b>                                                                                                                                                                                            |
| <code>--firebirdMNDbName &lt;firebirdMNDbName&gt;</code>          | Il nome del database Firebird per MONITOR.        | Predefinito: <b>MONITOR</b>                                                                                                                                                                                                                |
| <code>--firebirdQZDbName &lt;firebirdQZDbName&gt;</code>          | Nome del database Firebird per QUARTZ.            | Predefinito: <b>QUARTZ</b>                                                                                                                                                                                                                 |
| <code>--databaseIPAddress &lt;databaseIPAddress&gt;</code>        | L'indirizzo IP o il nome host del database.       | Indirizzo IP o nome host:<br>Predefinito:                                                                                                                                                                                                  |
| <code>--databasePort &lt;databasePort&gt;</code>                  | Il numero della porta del database.               | Numero porta:<br>Predefinito:                                                                                                                                                                                                              |
| <code>--instanceName &lt;instanceName&gt;</code>                  | Il nome dell'istanza.                             | Nome istanza:<br>Predefinito:                                                                                                                                                                                                              |

| Impostazione                                                                       | Descrizione                                          | Valore                                                                                                                                                                                                |
|------------------------------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--instanceIdentifier &lt;instanceIdentifier&gt;</code>                       | L'istanza.                                           | Predefinito: <b>databasePort</b><br>Consentito:<br><ul style="list-style-type: none"> <li>• <b>databasePort</b></li> <li>• <b>instanceName</b></li> </ul>                                             |
| <code>--databaseUsername &lt;databaseUsername&gt;</code>                           | Il nome utente del database.                         | Nome utente:<br>Predefinito:                                                                                                                                                                          |
| <code>--databasePassword &lt;databasePassword&gt;</code>                           | La password del database.                            | Password:<br>Predefinito:                                                                                                                                                                             |
| <code>--sqlServerAuthenticationMethod &lt;sqlServerAuthenticationMethod&gt;</code> | Il metodo di autenticazione di Microsoft SQL Server. | Predefinito: <b>sqlServerDbAuthentication</b><br>Consentito:<br><ul style="list-style-type: none"> <li>• <b>sqlServerDbAuthentication</b></li> <li>• <b>sqlServerWindowsAuthentication</b></li> </ul> |
| <code>--fWDbName &lt;fWDbName&gt;</code>                                           | Il nome del database per FRAMEWORK.                  | Nomi database:<br>Predefinito: <b>FRAMEWORK</b>                                                                                                                                                       |
| <code>--mNDbName &lt;mNDbName&gt;</code>                                           | Il nome del database per MONITOR.                    | Predefinito: <b>MONITOR</b>                                                                                                                                                                           |
| <code>--qZDbName &lt;qZDbName&gt;</code>                                           | Nome del database per QUARTZ.                        | Predefinito: <b>QUARTZ</b>                                                                                                                                                                            |
| <code>--mveAdminUsername &lt;mveAdminUsername&gt;</code>                           | Il nome utente dell'amministratore.                  | Nome utente:<br>Predefinito: <b>admin</b>                                                                                                                                                             |
| <code>--mveAdminPassword &lt;mveAdminPassword&gt;</code>                           | La password dell'amministratore.                     | Password:<br>Predefinito:                                                                                                                                                                             |

## Accesso a MVE

Per accedere a MVE, utilizzare le credenziali di accesso create durante l'installazione. È anche possibile configurare altri metodi di accesso, come LDAP, Kerberos o altri account locali. Per ulteriori informazioni, vedere ["Configurazione dell'accesso utente" a pagina 29](#).

- 1 Aprire un browser web e digitare **https://MVE\_SERVER/mve/**, in cui **MVE\_SERVER** corrisponde al nome host o all'indirizzo IP del server che ospita MVE.
- 2 Se necessario, accettare la dichiarazione di responsabilità.
- 3 Immettere le proprie credenziali.
- 4 Fare clic su **Accedi**.

### Note:

- Dopo aver effettuato l'accesso, assicurarsi di modificare la password predefinita dell'amministratore utilizzata durante l'installazione. Per ulteriori informazioni, vedere ["Modifica della password" a pagina 24](#).
- Se MVE è inattivo per più di 30 minuti, l'utente viene disconnesso automaticamente.

## Modifica della lingua

- 1 Aprire un browser web e digitare **https://MVE\_SERVER/mve/**, in cui **MVE\_SERVER** corrisponde al nome host o all'indirizzo IP del server che ospita MVE.
- 2 Se necessario, accettare la dichiarazione di responsabilità.
- 3 Nell'angolo superiore destro della pagina, selezionare una lingua.

## Modifica della password

- 1 Aprire un browser web e digitare **https://MVE\_SERVER/mve/**, in cui **MVE\_SERVER** corrisponde al nome host o all'indirizzo IP del server che ospita MVE.
- 2 Se necessario, accettare la dichiarazione di responsabilità.
- 3 Immettere le proprie credenziali.
- 4 Fare clic su **Accedi**.
- 5 Nell'angolo superiore destro della pagina, fare clic sul nome utente, quindi su **Modifica password**.
- 6 Modificare la password.



# Manutenzione dell'applicazione

## Aggiornamento a MVE 4.2

Prima di iniziare l'aggiornamento, effettuare le seguenti operazioni:

- Eseguire il backup dei file del database, dell'applicazione e delle proprietà. Per ulteriori informazioni, vedere ["Backup e ripristino del database" a pagina 26](#).
- Se necessario, fornire i nomi di database personalizzati.

Se si effettua un aggiornamento dalla versione 1.x, è necessario innanzitutto aggiornare alla versione 2.0, quindi alla versione 3.3 e alla versione 4.0 prima di effettuare l'aggiornamento alla versione 4.2. Il processo di migrazione dei criteri viene eseguito solo quando si esegue l'aggiornamento a MVE 2.0.

|                                      |                                        |
|--------------------------------------|----------------------------------------|
| Percorso di aggiornamento valido     | <b>3.3 a 4.0 a 4.2</b>                 |
| Percorso di aggiornamento non valido | <b>1.6.x a 4.2</b><br><b>2.0 a 4.2</b> |

- 1 Eseguire il backup dei file del database e dell'applicazione. Qualsiasi aggiornamento o disinstallazione determina un rischio di perdita irreversibile dei dati. Sarà possibile utilizzare i file di backup per ripristinare lo stato precedente dell'applicazione nel caso in cui l'aggiornamento non riesca.

**Attenzione - Possibili danni:** quando si esegue l'aggiornamento di MVE, il database subisce delle modifiche. Non ripristinare un backup del database creato da una versione precedente.

**Nota:** Per ulteriori informazioni, vedere ["Backup e ripristino del database" a pagina 26](#).

- 2 Scaricare il file eseguibile in un percorso temporaneo.
- 3 Eseguire il programma di installazione come amministratore, quindi seguire le istruzioni visualizzate sullo schermo del computer.

**Note:**

- Quando si esegue l'aggiornamento a MVE 2.0, i criteri assegnati alle stampanti vengono trasferiti in una singola configurazione per ciascun modello di stampante. Ad esempio, se i criteri relativi a fax, copia, carta e stampa sono assegnati a una stampante X792, tali criteri vengono consolidati in una configurazione X792. Questa procedura non riguarda i criteri che non sono assegnati alle stampanti. MVE genera un file di registro che conferma l'avvenuta migrazione dei criteri a una configurazione. Per ulteriori informazioni, vedere ["Dove è possibile trovare i file di registro?" a pagina 149](#).
- Dopo aver eseguito l'aggiornamento, accertarsi di cancellare la cache del browser prima di accedere nuovamente all'applicazione.
- Quando si esegue l'aggiornamento di MVE alla versione 3.5 o successiva, i componenti di protezione avanzata vengono esclusi dalle configurazioni a cui appartengono. Se due o più componenti di protezione avanzata sono identici, questi vengono combinati in un unico componente. Il componente di protezione avanzata creato viene aggiunto automaticamente alla libreria dei componenti di protezione avanzata.

## Backup e ripristino del database

**Nota:** è possibile che si verifichi una perdita di dati durante l'esecuzione delle procedure di backup e ripristino. Assicurarsi di eseguirle correttamente.

### Backup dei file del database e dell'applicazione

Si consiglia di eseguire regolarmente il backup del database.

- 1** Arrestare il servizio Firebird e il servizio Markvision Enterprise.
  - a** Aprire la finestra di dialogo Esegui, quindi digitare **services.msc**.
  - b** Fare clic con il pulsante destro del mouse su **Firebird Guardian - DefaultInstance**, quindi fare clic su **Arresta**.
  - c** Fare clic con il pulsante destro del mouse su **Markvision Enterprise**, quindi fare clic su **Arresta**.
- 2** Selezionare la cartella in cui è installato Markvision Enterprise.  
Ad esempio, **C:\Programmi\**
- 3** Eseguire il backup dei file dell'applicazione e del database.

### Backup dei file dell'applicazione

Copiare i seguenti file in un repository sicuro.

- Lexmark\mve\_encryption.jceks
- Lexmark\mve\_truststore.p12
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\platform.properties
- Lexmark\Markvision Enterprise\apps\library
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\jre\lib\security\cacerts
- Lexmark\Markvision Enterprise\tomcat\conf\server.xml

**Nota:** assicurarsi che questi file siano memorizzati correttamente. Senza le chiavi di crittografia nel file mve\_encryption.jceks, i dati memorizzati in un formato crittografato nel database e nel file system non possono essere recuperati.

### Backup dei file del database

Effettuare una delle seguenti operazioni:

**Nota:** i seguenti file utilizzano i nomi di database predefiniti. Queste istruzioni si applicano anche ai nomi di database personalizzati.

- Se si utilizza un database Firebird, copiare i seguenti file in un repository sicuro. Per evitare perdite di dati, è necessario eseguire regolarmente il backup di questi file.
  - Lexmark\Markvision Enterprise\firebird\security2.fdb

Se si utilizzano nomi di database personalizzati, aggiornare quanto segue:

- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\application.yml
- Lexmark\Markvision Enterprise\firebird\aliases.conf
- Lexmark\Markvision Enterprise\firebird\data\QUARTZ.FDB
- Lexmark\Markvision Enterprise\firebird\data\MONITOR.FDB
- Lexmark\Markvision Enterprise\firebird\data\FRAMEWORK.FDB
- Se si utilizza Microsoft SQL Server, creare un backup per FRAMEWORK, MONITOR e QUARTZ.  
Per ulteriori informazioni, contattare l'amministratore di Microsoft SQL Server.

**4** Riavviare il servizio Firebird e il servizio Markvision Enterprise.

**a** Aprire la finestra di dialogo Esegui, quindi digitare **services.msc**.

**b** Fare clic con il pulsante destro del mouse su **Firebird Guardian - DefaultInstance**, quindi fare clic su **Riavvia**.

**c** Fare clic con il pulsante destro del mouse su **Markvision Enterprise**, quindi fare clic su **Riavvia**.

## Ripristino dei file del database e dell'applicazione

**Attenzione - Possibili danni:** quando si esegue l'aggiornamento di MVE, il database può subire delle modifiche. Non ripristinare un backup del database creato da una versione precedente.

**1** Arrestare il servizio Markvision Enterprise.

Per ulteriori informazioni, vedere [passaggio 1](#) di ["Backup dei file del database e dell'applicazione" a pagina 26](#).

**2** Selezionare la cartella in cui è installato Markvision Enterprise.

Ad esempio, **C:\Programmi\**

**3** Ripristinare i file dell'applicazione.

Sostituire i seguenti file con i file salvati durante il processo di backup:

- Lexmark\mve\_encryption.jceks
- Lexmark\mve\_truststore.p12
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\platform.properties
- Lexmark\Markvision Enterprise\apps\library
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\jre\lib\security\cacerts
- Lexmark\Markvision Enterprise\tomcat\conf\server.xml

**Nota:** è possibile ripristinare un backup del database in una nuova installazione MVE solo se la versione di tale installazione è la stessa.

**4** Ripristinare i file del database.

Effettuare una delle seguenti operazioni:

- Se si usa un database Firebird, sostituire i seguenti file salvati durante il processo di backup:

**Nota:** i seguenti file utilizzano i nomi di database predefiniti. Questa istruzione si applica anche ai nomi di database personalizzati.

- Lexmark\Markvision Enterprise\firebird\security2.fdb

Se si utilizzano nomi di database personalizzati, vengono ripristinati anche i seguenti file:

- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\application.yml
- Lexmark\Markvision Enterprise\firebird\aliases.conf
- Lexmark\Markvision Enterprise\firebird\data\QUARTZ.FDB
- Lexmark\Markvision Enterprise\firebird\data\MONITOR.FDB
- Lexmark\Markvision Enterprise\firebird\data\FRAMEWORK.FDB
- Se si usa un database Microsoft SQL Server, contattare l'amministratore di Microsoft SQL Server.

## 5 Riavviare il servizio Markvision Enterprise.

Per ulteriori informazioni, vedere [passaggio 4](#) di "[Backup dei file del database e dell'applicazione](#)" a [pagina 26](#).

# Aggiornamento delle impostazioni del programma di installazione dopo l'installazione

L'utility password di Markvision Enterprise consente di aggiornare le impostazioni di Microsoft SQL Server configurate durante l'installazione senza dover reinstallare MVE. L'utility consente inoltre di aggiornare le credenziali dell'account di dominio Esegui come utente, ad esempio il nome utente e la password. È inoltre possibile utilizzare la utility per creare un altro utente amministratore se vengono dimenticate le credenziali dell'utente amministratore precedente.

## 1 Selezionare la cartella in cui è installato Markvision Enterprise.

Ad esempio, **C:\Programmi\**

## 2 Avviare il file **mvepwdutility-windows.exe** nella cartella Lexmark\Markvision Enterprise\.

## 3 Selezionare una lingua, quindi fare clic su **OK > Avanti**.

## 4 Seguire le istruzioni visualizzate sullo schermo del computer.

# Configurazione dell'accesso utente

## Panoramica

MVE consente di aggiungere utenti interni direttamente al server MVE o di utilizzare gli account utente registrati in un server LDAP. Per ulteriori informazioni sull'aggiunta di utenti interni, vedere ["Gestione degli utenti" a pagina 30](#). Per ulteriori informazioni sull'utilizzo di account utente LDAP, vedere ["Abilitazione dell'autenticazione tramite server LDAP" a pagina 31](#).

Quando si aggiungono utenti, devono essere assegnati dei ruoli. Per ulteriori informazioni, vedere ["Informazioni sui ruoli utente" a pagina 29](#).

Durante l'autenticazione, il sistema verifica le credenziali degli utenti interni presenti nel server MVE. Se MVE non è in grado di eseguire l'autenticazione dell'utente, prova ad autenticarlo sul server LDAP. Se il nome dell'utente esiste sia sul server MVE che sul server LDAP, viene utilizzata la password del server MVE.

## Informazioni sui ruoli utente

Gli utenti MVE possono essere assegnati a uno o più ruoli. A seconda del ruolo, gli utenti possono effettuare le seguenti attività:

- **Amministratore:** accedere ed eseguire le attività di tutti i menu. Essi dispongono inoltre di privilegi amministrativi che consentono, ad esempio, di aggiungere utenti al sistema o di configurare le impostazioni del sistema. Solo gli utenti con il ruolo di amministratore possono interrompere le attività in esecuzione indipendentemente dal tipo di utente che le ha avviate.
- **Stampanti**
  - Gestire i profili di ricerca.
  - Impostare gli stati della stampante.
  - Eseguire un controllo.
  - Gestire categorie e parole chiave.
  - Programmare un controllo, un'esportazione dati e la ricerca della stampante.
- **Configurazioni**
  - Gestire le configurazioni, comprese l'importazione e l'esportazione dei file di configurazione.
  - Caricare i file nella libreria delle risorse.
  - Assegnare e applicare le configurazioni alle stampanti.
  - Programmare un controllo di conformità e l'applicazione delle configurazioni.
  - Distribuire i file alle stampanti.
  - Aggiornare il firmware della stampante.
  - Generare le richieste di firma per il certificato della stampante.
  - Scaricare le richieste di firma per il certificato della stampante.
- **Gestione degli eventi**
  - Gestire azioni ed eventi.
  - Assegnare eventi alle stampanti.
  - Effettuare il test delle azioni.

- **Assistenza**

- Aggiornare lo stato della stampante.
- Riavviare le stampanti.
- Eseguire un controllo di conformità.
- Applicare le configurazioni alle stampanti.

**Note:**

- Tutti gli utenti di MVE possono visualizzare la pagina delle informazioni della stampante e gestire viste e ricerche salvate.
- Per ulteriori informazioni sull'assegnazione dei ruoli utente, vedere ["Gestione degli utenti" a pagina 30](#).

## Gestione degli utenti

- 1 Fare clic su  nell'angolo superiore destro della pagina.
- 2 Fare clic su **Utente**, quindi effettuare una delle seguenti operazioni:

### Aggiungere un utente

- a Fare clic su **Crea**.
- b Digitare il nome utente, l'ID utente e la password.
- c Selezionare i ruoli.

**Nota:** Per ulteriori informazioni, vedere ["Informazioni sui ruoli utente" a pagina 29](#).

- d Fare clic su **Crea utente**.

### Modificare un utente

- a Selezionare un ID utente.
- b Configurare le impostazioni.
- c Fare clic su **Salva modifiche**.

### Eliminare utenti

- a Selezionare uno o più utenti.
- b Fare clic su **Elimina**, quindi confermare l'eliminazione.

**Nota:** Un account utente è bloccato dopo tre tentativi consecutivi di accesso non riusciti. Solo un utente Amministratore può riattivare l'account utente. Se l'utente Amministratore è bloccato, il sistema lo riattiva automaticamente dopo cinque minuti.

## Abilitazione dell'autenticazione tramite server LDAP

LDAP è un protocollo estendibile tra più piattaforme, basato su standard, che viene eseguito direttamente su TCP/IP e utilizzato per accedere a database specializzati denominati directory.

Per evitare di gestire più credenziali utente, è possibile utilizzare il server LDAP della società per autenticare gli ID utente e le password.

Come prerequisito, il server LDAP deve contenere gruppi utenti corrispondenti ai ruoli utente richiesti. Per ulteriori informazioni, vedere ["Informazioni sui ruoli utente" a pagina 29](#).

- 1 Fare clic su  nell'angolo superiore destro della pagina.
- 2 Fare clic su **LDAP**, quindi selezionare **Abilita LDAP per autenticazione**.
- 3 Nel campo Nome host server LDAP digitare l'indirizzo IP o il nome host del server LDAP in cui viene eseguita l'autenticazione.  
  
**Nota:** se si desidera utilizzare la comunicazione crittografata tra il server MVE e il server LDAP, utilizzare il nome di dominio completo (FQDN).
- 4 Specificare il numero di porta del server in base al protocollo di crittografia selezionato.
- 5 Selezionare il protocollo di crittografia.
  - **Nessuna**
  - **TLS:** un protocollo di sicurezza che utilizza la crittografia dei dati e l'autenticazione del certificato per proteggere la comunicazione tra un server e un client. Se si seleziona questa opzione, viene inviato un comando START\_TLS al server LDAP una volta stabilita la connessione. Utilizzare questa impostazione se si desidera una comunicazione protetta tramite la porta 389.
  - **SSL/TLS:** un protocollo di sicurezza che utilizza la crittografia a chiave pubblica per autenticare la comunicazione tra un server e un client. Utilizzare questa opzione se si desidera una comunicazione protetta dall'inizio del binding LDAP. Questa opzione viene generalmente utilizzata per la porta 636 o altre porte LDAP protette.
- 6 Selezionare il tipo di binding.
  - **Semplice:** il server MVE produce le credenziali specificate al server LDAP al fine di utilizzare la funzione di ricerca del server LDAP.
    - a Digitare il nome utente di binding.
    - b Digitare la password di binding, quindi confermarla.
  - **Kerberos:** per configurare le impostazioni, effettuare le seguenti operazioni:
    - a Digitare il nome utente di binding.
    - b Digitare la password di binding, quindi confermarla.
    - c Fare clic su **Scegli file**, quindi selezionare il file krb5.conf.
  - **SPNEGO:** per configurare le impostazioni, effettuare le seguenti operazioni:
    - a Digitare il nome principale del servizio.
    - b Fare clic su **Scegli file**, quindi selezionare il file krb5.conf.
    - c Fare clic su **Scegli file**, quindi selezionare il file keytab Kerberos.

Questa opzione viene utilizzata solo per configurare il meccanismo SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) per supportare la funzionalità Single Sign-On.

## 7 Nella sezione Opzioni avanzate effettuare le seguenti operazioni:

- **Base di ricerca:** il nome distinto di base (DN) del nodo radice. Nella gerarchia del server community LDAP, questo nodo deve essere il predecessore del nodo utente e del nodo gruppo. Ad esempio, **dc=mvetest,dc=com**.  
**Nota:** quando si specifica il DN radice, accertarsi che solo **dc** e **o** facciano parte del DN radice. Se **ou** o **cn** è il predecessore dei nodi utente e gruppo, utilizzare **ou** o **cn** nelle basi di ricerca utenti o gruppi.
- **Base di ricerca utenti:** il nodo nel server community LDAP in cui è presente l'oggetto utente. Questo nodo si trova nel DN radice in cui sono elencati tutti i nodi utente. Ad esempio, **ou=people**.
- **Filtro di ricerca utenti:** il parametro per individuare un oggetto utente nel server community LDAP. Ad esempio, **(uid={0})**.

### Esempi di più condizioni ed espressioni complesse consentite

| Accesso con                   | Nel campo Filtro di ricerca utenti digitare |
|-------------------------------|---------------------------------------------|
| Nome comune                   | <b>(CN={0})</b>                             |
| Nome di accesso               | <b>(sAMAccountName={0})</b>                 |
| Nome principale utente        | <b>(userPrincipalName={0})</b>              |
| Numero di telefono            | <b>(telephoneNumber={0})</b>                |
| Nome di accesso o nome comune | <b>(   (sAMAccountName={0}) (CN={0}) )</b>  |

**Nota:** l'unico modello valido è **{0}**, che indica che MVE cerca il nome di accesso utente MVE.

- **Cerca oggetto base utenti e sottoalbero intero:** il sistema ricerca tutti i nodi nella base di ricerca utenti.
- **Base di ricerca gruppi:** il nodo nel server community LDAP che contiene i gruppi utenti corrispondenti ai ruoli MVE. Questo nodo si trova nel DN radice in cui sono elencati tutti i nodi gruppo. Ad esempio, **ou=group**.
- **Filtro di ricerca gruppi:** il parametro per individuare un utente all'interno di un gruppo che corrisponde a un ruolo MVE.

**Nota:** possono essere utilizzati solo i modelli **{0}** e **{1}**. Se si utilizza **{0}**, MVE cerca il DN utente LDAP. Se si utilizza **{1}**, MVE cerca il nome di accesso utente MVE.

- **Attributo ruolo gruppo:** digitare l'attributo LDAP per il nome completo del gruppo. Un attributo LDAP ha un significato specifico e definisce un mapping tra l'attributo e il nome di un campo. Ad esempio, l'attributo LDAP **cn** viene associato al campo Nome. Anche l'attributo LDAP **commonname** viene associato al campo Nome. In genere, questo attributo deve essere lasciato impostato sul valore predefinito di **cn**.
- **Cerca oggetto base utenti e sottoalbero intero:** il sistema ricerca tutti i nodi nella base di ricerca gruppi.

## 8 Nella sezione Mapping gruppi LDAP a ruoli MVE immettere i nomi dei gruppi LDAP che corrispondono ai ruoli MVE.

### Note:

- Per ulteriori informazioni, vedere ["Informazioni sui ruoli utente" a pagina 29](#).
- È possibile assegnare un gruppo LDAP a più ruoli MVE. È inoltre possibile immettere più di un gruppo LDAP in un campo di ruolo, utilizzando il carattere barra verticale (|) per separare i gruppi. Ad esempio, per includere i gruppi **admin** e **assets** per il ruolo Amministratore, digitare **admin|assets** nel campo Gruppi LDAP per amministratore.



- Se si desidera utilizzare solo il ruolo Amministratore e non gli altri ruoli MVE, lasciare i campi vuoti.

**9** Fare clic su **Salva modifiche**.

## Installazione dei certificati del server LDAP

Per stabilire una comunicazione crittografata tra il server MVE e il server LDAP, MVE deve considerare attendibile il certificato del server LDAP. Nell'architettura MVE, quando MVE si autentica con un server LDAP, MVE è il client e il server LDAP è il peer.

- 1** Fare clic su  nell'angolo superiore destro della pagina.
- 2** Fare clic su **LDAP**, quindi configurare le impostazioni LDAP. Per ulteriori informazioni, vedere ["Abilitazione dell'autenticazione tramite server LDAP" a pagina 31](#).
- 3** Fare clic su **Prova LDAP**.
- 4** Immettere un nome utente LDAP e una password validi, quindi fare clic su **Avvia prova**.
- 5** Esaminare la validità del certificato, quindi accettarlo.

# Rilevamento delle stampanti

## Creazione di un profilo di ricerca

Utilizzare un profilo di ricerca per trovare le stampanti in rete e aggiungerle al sistema. In un profilo di ricerca, effettuare una delle seguenti operazioni per includere o escludere un elenco di indirizzi IP o nomi host:

- Aggiunta di singole voci
- Importazione di voci da un file TXT o CSV

Inoltre, è possibile assegnare e applicare automaticamente una configurazione a un modello di stampante compatibile. Una configurazione deve contenere impostazioni della stampante, applicazioni, licenze, firmware e certificati CA che possono essere distribuiti sulle stampanti.

- 1 Nel menu Stampanti fare clic su **Profili di ricerca > Crea**.
- 2 Nella sezione Impostazioni generali digitare un nome univoco e una descrizione per il profilo di ricerca, quindi configurare le seguenti opzioni:
  - **Timeout**: l'intervallo di tempo per cui il sistema deve attendere la risposta di una stampante.
  - **Tentativi**: il numero di tentativi di comunicazione del sistema con una stampante.
  - **Gestisci automaticamente stampanti rilevate**: le nuove stampanti rilevate vengono impostate automaticamente sullo stato Gestito e lo stato Nuovo viene ignorato durante la ricerca.
- 3 Nella sezione Indirizzi effettuare una delle seguenti operazioni:

### Aggiungere gli indirizzi

a Selezionare **Includi** o **Escludi**.

b Digitare l'indirizzo IP, il nome host, la subnet o l'intervallo di indirizzi IP.

Addresses

Include

Examples: 10.20.xx.xx, myprinter.domain.com, 2001:dbx::x:x  
2001:dbx::x:x

Search Address/Range

| <input type="checkbox"/> | Address/Range              | Include/Exclude |
|--------------------------|----------------------------|-----------------|
| <input type="checkbox"/> | 10.195.x.x-10.195.x.xx.xxx | Include         |

Aggiungere una sola voce per volta. Utilizzare i seguenti formati per gli indirizzi:

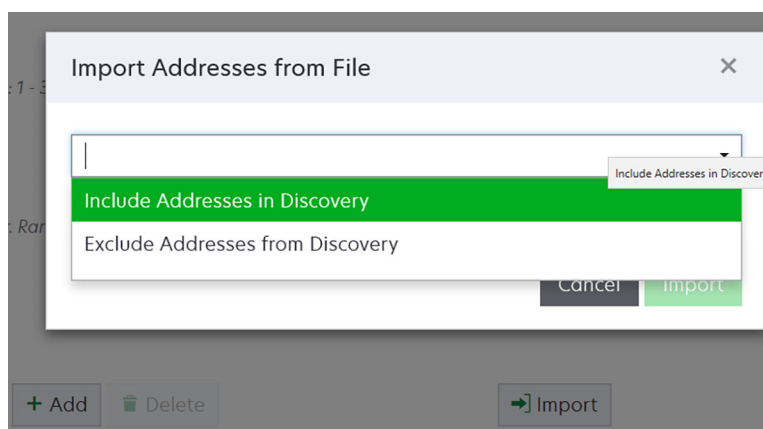
- **10.195.10.1** (indirizzo IPv4 singolo)
- **myprinter.example.com** (nome host singolo)
- **10.195.10.3-10.195.10.255** (intervallo di indirizzi IPv4)
- **10.195.\*.\*** (caratteri jolly)
- **10.195.10.1/22** (notazione IPv4 CIDR (Classless Inter-Domain Routing))
- **2001:db8:0:0:0:0:2:1** (indirizzo IPv6 completo)
- **2001:db8::2:1** (indirizzo IPv6 compresso)

**Nota:** se vengono creati profili di ricerca separati per l'indirizzo IPv6 e l'indirizzo IPv4 per la stessa stampante, viene visualizzato l'ultimo indirizzo rilevato. Ad esempio, se una stampante viene rilevata tramite IPv6, quindi viene nuovamente rilevata tramite IPv4, nell'elenco delle stampanti viene visualizzato solo l'indirizzo IPv4.

- c Fare clic su **Aggiungi**.

## Importare gli indirizzi

- a Fare clic su **Importa**.
- b Scegliere se includere o escludere degli indirizzi IP durante la ricerca.



- c Selezionare il file di testo contenente l'elenco di indirizzi. Ciascuna voce di indirizzo deve trovarsi su una riga separata.

File di testo di esempio

```
10.195.10.1
myprinter.example.com
10.195.10.3-10.195.10.255
10.195.*.*
10.195.10.1/22
2001:db8:0:0:0:0:2:1
2001:db8::2:1
```

- d Fare clic su **Importa**.

- 4 Nella sezione SNMP selezionare **Versione 1**, **Versione 2c** o **Versione 3**, quindi impostare le autorizzazioni di accesso.

**Nota:** per eseguire la ricerca delle stampanti che utilizzano SNMP versione 3, creare un nome utente e una password in Embedded Web Server della stampante, quindi riavviare la stampante. Se non è possibile stabilire una connessione, rilevare nuovamente le stampanti. Per ulteriori informazioni, consultare la *Guida dell'amministratore di Embedded Web Server*.

- 5 Se necessario, nella sezione Immetti le credenziali, selezionare il metodo di autenticazione utilizzato per le stampanti, quindi immettere le credenziali.

**Nota:** questa funzione consente di stabilire la comunicazione con le stampanti protette durante il rilevamento. È necessario fornire le credenziali corrette per eseguire attività sulle stampanti protette, come controllo, aggiornamento dello stato e aggiornamento del firmware.

- 6 Se necessario, nella sezione Assegna configurazioni, associare una configurazione a un modello di stampante. Per informazioni sulla creazione di una configurazione, vedere ["Creazione di una configurazione" a pagina 68](#).

- 7** Se necessario, nella sezione Assegna parole chiave, associare una parola chiave a un modello di stampante durante il rilevamento. Per informazioni sull'assegnazione delle parole chiave alle stampanti, vedere ["Assegnazione di parole chiave alle stampanti" a pagina 65](#).

**Note:**

- A tutte le stampanti rilevate tramite questo profilo vengono assegnate le nuove parole chiave.
- Le nuove parole chiave vengono aggiunte all'elenco esistente di parole chiave già assegnate a una stampante.

- 8** Fare clic su **Salva profilo** o su **Salva ed esegui profilo**.

**Nota:** è possibile programmare l'esecuzione periodica di una ricerca. Per ulteriori informazioni, vedere ["Creazione di un programma" a pagina 143](#).

## Gestione dei profili di ricerca

- 1** Dalla scheda Stampanti, fare clic su **Profili di ricerca**.

- 2** Effettuare una delle seguenti operazioni:

### Modificare un profilo

- a** Selezionare un profilo, quindi fare clic su **Modifica**.
- b** Configurare le impostazioni.
- c** Fare clic su **Salva profilo** o su **Salva ed esegui profilo**.

### Copiare un profilo

- a** Selezionare un profilo, quindi fare clic su **Copia**.
- b** Configurare le impostazioni.
- c** Aggiungere gli indirizzi IP. Per ulteriori informazioni, vedere ["Aggiungere gli indirizzi" a pagina 34](#).
- d** Fare clic su **Salva profilo** o su **Salva ed esegui profilo**.

### Eliminare un profilo

- a** Selezionare uno o più profili.
- b** Fare clic su **Elimina**, quindi confermare l'eliminazione.

### Eseguire un profilo

- a** Selezionare uno o più profili.
- b** Fare clic su **Esegui**. Controllare lo stato di ricerca dal menu Attività.

## Scenario di esempio: rilevamento delle stampanti

La società ABC è una grande azienda di produzione che occupa un edificio di nove piani. La società ha appena acquistato 30 nuove stampanti Lexmark, distribuite sui nove piani. Il personale IT deve aggiungere queste nuove stampanti a MVE. Le stampanti sono già collegate alla rete, ma non si conoscono tutti gli indirizzi IP.

Si desidera proteggere le seguenti nuove stampanti situate nel reparto contabilità.

**10.194.55.60**

**10.194.56.77**

**10.194.55.71**

**10.194.63.27**

**10.194.63.10**

### Esempio di implementazione

- 1** Creare un profilo di ricerca per le stampanti situate nel reparto contabilità.
- 2** Aggiungere i cinque indirizzi IP.
- 3** Creare una configurazione che protegga le stampanti specificate.
- 4** Includere le configurazioni nel profilo di ricerca.
- 5** Salvare ed eseguire il profilo.
- 6** Creare un altro profilo di ricerca per le rimanenti stampanti.
- 7** Includere gli indirizzi IP utilizzando un carattere jolly. Utilizzare il seguente formato: **10.194.\*.\***
- 8** Escludere i cinque indirizzi IP delle stampanti situate nel reparto contabilità.
- 9** Salvare e quindi eseguire il profilo.

# Gestione della dashboard di protezione

## Panoramica

Il dashboard di protezione consente di visualizzare lo stato delle impostazioni di protezione delle periferiche attraverso una rappresentazione visiva di varie impostazioni di protezione, quali porte, protocolli, stato di crittografia disco, account di amministratore periferica e stato del certificato predefinito. Fornisce visibilità sul livello di sicurezza del parco dispositivi, aiutando gli amministratori a identificare e correggere le impostazioni che non sono conformi.

## Accesso al dashboard di protezione

- 1 Nel portale Web MVE, fare clic su **Dashboard**.

**Nota:** Il dashboard di protezione è la pagina di destinazione predefinita per gli utenti Admin.

- 2 Fare clic su uno dei seguenti widget:
  - **Informazioni sulla protezione della periferica**
  - **Controllo conformità periferica**

## Gestione di Informazioni sulla protezione della periferica

Questo widget riepiloga la vista della protezione del parco dispositivi.

- 1 Fare clic su una barra qualsiasi del grafico per accedere alla finestra Informazioni sulla protezione della periferica.
- 2 Passare il mouse sulle barre per visualizzare i seguenti dettagli:
  - Numero porta
  - Numero di stampanti associate
  - Se le impostazioni della stampante sono aperte/abilite
- 3 Fare clic su **Stampa** per ottenere un formato stampabile della vista dettagliata.

### Note:

- La finestra Informazioni sulla protezione della periferica dispone di una funzione di drill-down.
- Facendo clic su un elemento della barra nel grafico, l'utente può accedere a una vista filtrata della pagina di elenco delle stampanti. Per ulteriori informazioni, vedere ["Visualizzazione dell'elenco stampanti" a pagina 40](#).

## Gestione di Controllo conformità periferica

Questo widget riepiloga la vista dettagliata del controllo di conformità del parco dispositivi.

- 1 Fare clic su una sezione qualsiasi del grafico a torta per passare alla finestra Controllo conformità periferica.
- 2 Nel riquadro a sinistra, applicare il filtro Intervallo date.

**Nota:** l'intervallo predefinito è 7 giorni.

**3** Fare clic su **Stampa** per ottenere un formato stampabile della vista dettagliata.

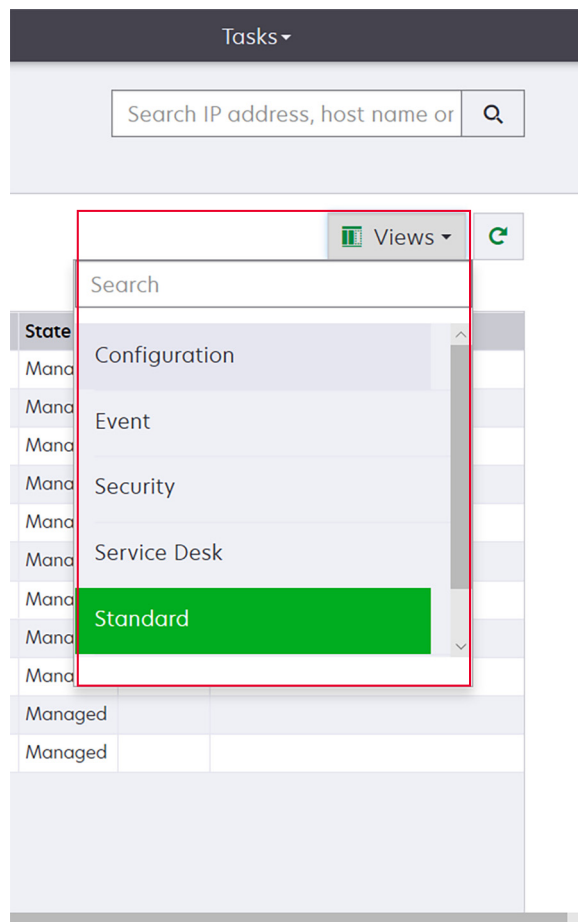
**Note:**

- La finestra Controllo conformità periferica dispone di una funzione di drill-down.
- Facendo clic su una sezione del grafico a torta, l'utente può accedere a una vista filtrata della pagina di elenco delle stampanti. Per ulteriori informazioni, vedere ["Visualizzazione dell'elenco stampanti" a pagina 40](#).





- Modificare la visualizzazione dell'elenco stampanti. Per ulteriori informazioni, vedere ["Modifica della visualizzazione dell'elenco stampanti" a pagina 46](#).



**Nota:** se si sta utilizzando la casella di ricerca, l'applicazione cerca tutte le stampanti presenti nel sistema. I filtri selezionati e le ricerche salvate vengono ignorati. Se si esegue una ricerca salvata, vengono utilizzati i criteri specificati nella ricerca salvata. I filtri selezionati e l'indirizzo IP o il nome host immesso nella casella di ricerca vengono ignorati. È anche possibile utilizzare i filtri per restringere i risultati di ricerca correnti.

- Utilizzare i filtri.

The screenshot shows the 'All Printers' interface. On the left, there are filter sections: 'Keywords' (No keywords (4)), 'Subnets' (157184.205.\* (4), 10.195.7\* (3), 10.194.29\* (1), 10.195.0\* (1), 10.195.6\* (1)), 'Supply Status Severity' (Unknown supply status (4)), 'Printer Status Severity' (Unknown printer status (4)), 'Configuration Conform...' (Clear), and 'Model Names' (Clear). On the right, there are buttons for 'Printer', 'Configure', 'Assign', and 'Security'. Below these, it says '4 total items' and shows a table of printers.

| IP Address     | Model            | Contact Name |
|----------------|------------------|--------------|
| 157184.205.135 | Lexmark B2236dw  |              |
| 157184.205.186 | Lexmark CX922de  |              |
| 157184.205.212 | Lexmark CX725    |              |
| 157184.205.250 | Lexmark MX611dhe |              |

- Eseguire una ricerca salvata. Per ulteriori informazioni, vedere ["Esecuzione di una ricerca salvata" a pagina 49.](#)

The screenshot shows the 'All Printers' interface with the 'Run Saved Search' dropdown menu open. The menu lists various search criteria: 'All Printers', 'Managed (Changed) Printers', 'Managed Printers', 'Managed (Found) Printers', 'Managed (Missing) Printers', 'Managed (Normal) Printers', 'New Printers', 'Retired Printers', 'Unmanaged Printers', and 'C2lite'. The background shows the same filter sections and printer table as the previous screenshot.

- Per ordinare le stampanti, dalla tabella con l'elenco delle stampanti, fare clic su qualsiasi intestazione di colonna. Le stampanti sono ordinate in base all'intestazione della colonna selezionata.
- Per visualizzare ulteriori informazioni sulle stampanti, ridimensionare le colonne. Posizionare il cursore sul bordo verticale dell'intestazione della colonna, quindi trascinare il bordo a sinistra o a destra.

## Visualizzazione delle informazioni della stampante

Per vedere l'elenco completo delle informazioni, assicurarsi che il controllo sia eseguito sulla stampante. Per ulteriori informazioni, vedere ["Controllo delle stampanti" a pagina 61](#).

**1** Nel menu Stampanti fare clic su **Elenco stampanti**.

**2** Fare clic sull'indirizzo IP della stampante.

**3** Visualizzare le seguenti informazioni:

- **Stato:** stato della stampante.
- **Materiali di consumo:** dettagli sui materiali di consumo e percentuale dei materiali rimanenti.
- **Identificazione:** informazioni di identificazione della rete della stampante.

**Nota:** le informazioni sul fuso orario sono disponibili solo in determinati modelli di stampante.

- **Date:** la data in cui la stampante viene aggiunta al sistema, la data di ricerca e la data del controllo più recente.
- **Firmware:** proprietà e livelli del codice del firmware della stampante.
- **Funzionalità:** funzioni della stampante.
- **Opzioni di memoria:** dimensione del disco fisso e spazio libero sulla memoria flash dell'utente.
- **Opzioni di alimentazione:** impostazioni per i vassoi disponibili.
- **Opzioni di uscita:** impostazioni per i raccoglitori disponibili.
- **Applicazioni eSF:** informazioni relative alle applicazioni eSF (Embedded Solutions Framework) installate sulla stampante.
- **Statistiche stampante:** valori specifici di ciascuna proprietà della stampante.
- **Modifica dettagli:** informazioni relative alle modifiche della stampante.

**Nota:** queste informazioni sono disponibili solo nelle stampanti con stato Gestito (modificato). Per ulteriori informazioni, vedere ["Informazioni sugli stati del ciclo di vita della stampante" a pagina 47](#).

- **Credenziali stampante:** credenziali utilizzate per la configurazione assegnata alla stampante.
- **Certificato della stampante :** proprietà dei seguenti certificati della stampante:
  - Predefinito
  - HTTPS
  - 802.1x
  - IPSec

**Note:**

- Queste informazioni sono disponibili solo su alcuni modelli di stampante.
- Uno stato di validità Scadenza imminente indica la data di scadenza, come impostato nella sezione Autorità di certificazione in Configurazione di sistema.
- **Proprietà di configurazione:** proprietà della configurazione assegnata alla stampante.
- **Avvisi attivi:** gli avvisi della stampante in attesa di essere cancellati.
- **Eventi assegnati:** eventi assegnati alla stampante.

## Esportazione dei dati della stampante

MVE consente di esportare le informazioni relative alla stampante che è disponibile nella visualizzazione corrente.

**1** Nella cartella Stampanti , fare clic su **Elenco stampanti**.

**2** Selezionare una o più stampanti.

**3** Fare clic su **Stampante > Esporta i dati**.

**Note:**

- I dati esportati vengono salvati in un file CSV.
- È possibile programmare l'esecuzione periodica di un'esportazione dati. Per ulteriori informazioni, vedere ["Creazione di un programma" a pagina 143](#).

## Gestione delle visualizzazioni

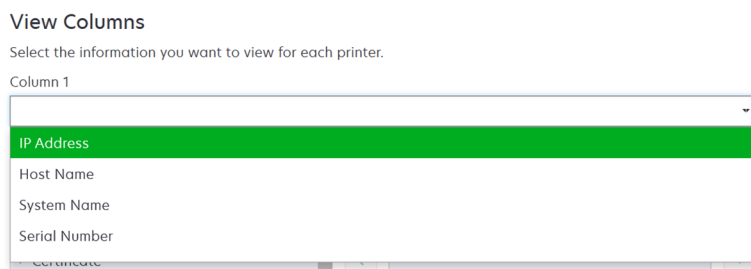
La funzione Visualizzazioni consente di personalizzare le informazioni contenute nella pagina dell'elenco stampanti.

**1** Nel menu Stampanti fare clic su **Visualizzazioni**.

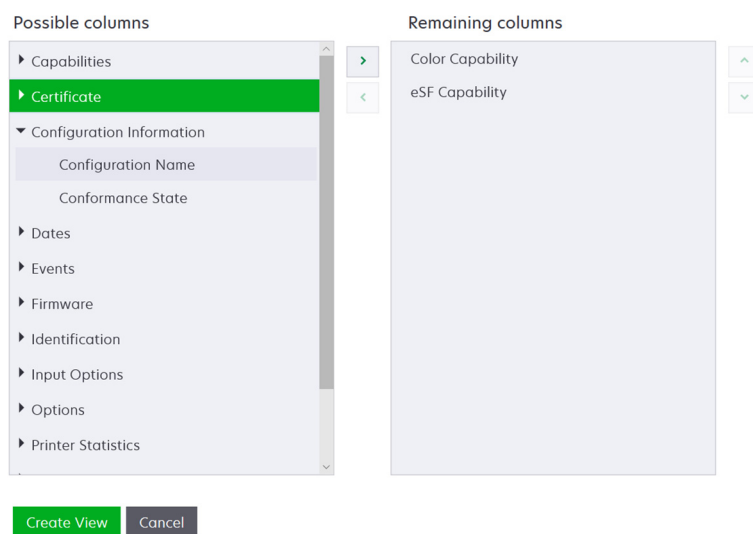
**2** Effettuare una delle seguenti operazioni:

### Creare una visualizzazione

- Fare clic su **Crea**.
- Digitare un nome univoco per la visualizzazione e la relativa descrizione.
- Nella scheda Visualizza colonne, nel menu Colonna 1, selezionare la colonna dell'identificativo.



- d Nella sezione Colonne possibili espandere una categoria e selezionare le informazioni che si desidera mostrare sotto forma di colonna, quindi fare clic su >.



- **Funzionalità:** indica se le funzionalità selezionate sono supportate sulla stampante.
- **Certificato:** mostra la data di creazione del certificato della stampante, lo stato di registrazione, la data di scadenza, la data di rinnovo, il numero di revisione, l'oggetto del certificato, la validità e lo stato della firma.
- **Informazioni sulla configurazione:** mostra le informazioni associate alla configurazione della stampante, come conformità, nome della configurazione e stato.
- **Date:** consente di visualizzare l'ultimo controllo, l'ultima verifica di conformità, l'ultima ricerca e la data in cui la stampante è stata aggiunta al sistema.
- **Eventi:** mostra le informazioni relative agli eventi della stampante.
- **Firmware:** mostra le informazioni relative al firmware, ad esempio la versione del firmware.
- **Identificazione:** mostra le informazioni relative alla stampante, ad esempio l'indirizzo IP, il nome host e il numero di serie.
- **Opzioni di alimentazione:** mostra le informazioni sulle opzioni di input, ad esempio le dimensioni del vassoio e il tipo di supporto.
- **Opzioni:** mostra informazioni sulle opzioni della stampante, ad esempio disco fisso e unità flash.
- **Statistiche stampante:** mostra informazioni sull'utilizzo della stampante, ad esempio il numero di pagine stampate o acquisite tramite scansione, e il numero totale di lavori inviati via fax.
- **Soluzioni:** mostra le applicazioni eSF installate sulla stampante e i numeri delle relative versioni.
- **Stato:** mostra lo stato della stampante e dei materiali di consumo.
- **Materiali di consumo:** mostra le informazioni relative ai materiali di consumo.
- **Porte della stampante:** mostra le informazioni correlate alle porte.

**Nota:** Un'opzione **Sconosciuto** nel valore della porta significa che la porta non esiste sulla stampante o che MVE non è in grado di recuperare la porta.

- **Opzioni di protezione della stampante:** mostra le informazioni TLS e di crittografia.

- e Fare clic su **Crea visualizzazione**.

### Modificare una visualizzazione

- a** Selezionare una visualizzazione.
- b** Fare clic su **Modifica**, quindi modificare le impostazioni.
- c** Fare clic su **Salva modifiche**.

### Copiare una visualizzazione

- a** Selezionare una visualizzazione.
- b** Fare clic su **Copia**, quindi configurare le impostazioni.
- c** Fare clic su **Crea visualizzazione**.

### Eliminare visualizzazioni

- a** Selezionare una o più visualizzazioni.
- b** Fare clic su **Elimina**, quindi confermare l'eliminazione.

### Impostare una visualizzazione predefinita

- a** Selezionare una visualizzazione.
- b** Fare clic su **Imposta come predefinito**.

Le seguenti visualizzazioni sono generate dal sistema e non possono essere modificate o eliminate:

- Configurazione
- Elenco stampanti
- Evento
- Protezione
- Service Desk
- Vassoio standard

## Modifica della visualizzazione dell'elenco stampanti

Per ulteriori informazioni, vedere ["Gestione delle visualizzazioni" a pagina 44](#).

- 1** Nel menu Stampante, fare clic su **Elenco stampanti**.
- 2** Fare clic su **Visualizzazioni**, quindi selezionare una visualizzazione.

## Filtraggio delle stampanti dalla barra di ricerca

Per cercare le stampanti dalla barra di ricerca, tenere presente quanto segue.

- Per cercare un indirizzo IP, assicurarsi di digitare l'intervallo o l'indirizzo IP completo.

Ad esempio:

- 10.195.10.1
- 10.195.10.3–10.195.10.255
- 10.195.\*.\*
- 2001:db8:0:0:0:0:2:1

- Se la stringa di ricerca non è un indirizzo IP completo, le stampanti vengono cercate in base al nome host, al nome del sistema o al numero di serie.
- Il carattere di sottolineatura ( \_ ) può essere utilizzato come carattere jolly.

## Gestione delle parole chiave

Le parole chiave consentono di creare etichette personalizzate e di assegnarle alle stampanti.

- 1 Nel menu Stampanti fare clic su **Parole chiave**.
- 2 Effettuare una delle seguenti operazioni:
  - Aggiungere, modificare o eliminare una categoria.  
**Nota:** le categorie raggruppano insieme le parole chiave.
  - Aggiungere, modificare o eliminare una parola chiave.

Per informazioni sull'assegnazione delle parole chiave alle stampanti, vedere ["Assegnazione di parole chiave alle stampanti" a pagina 65](#).

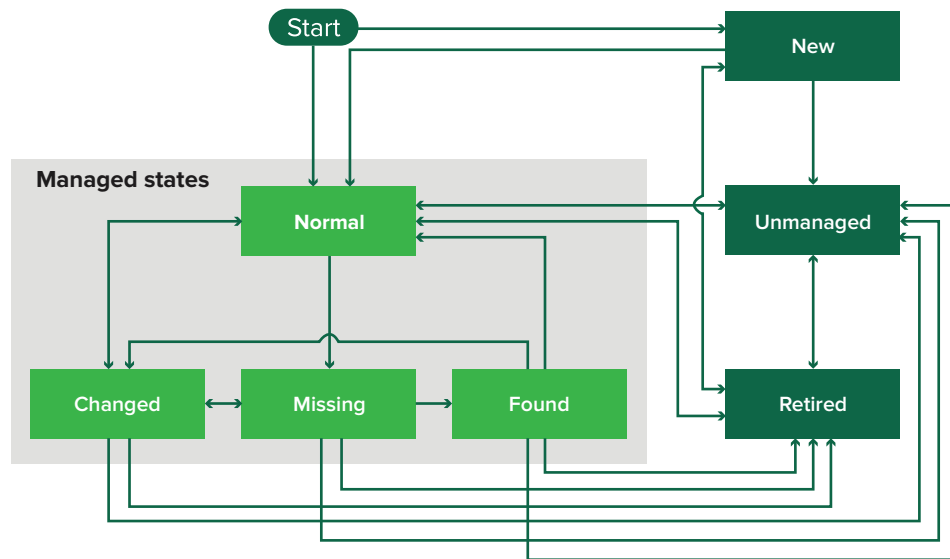
## Uso delle ricerche salvate

### Informazioni sugli stati del ciclo di vita della stampante

Le ricerche salvate generate dal sistema mostrano le stampanti con i seguenti stati del ciclo di vita della stampante:

- **Tutte le stampanti:** tutte le stampanti nel sistema.
- **Stampanti gestite:** le stampanti visualizzate possono essere in uno dei seguenti stati:
  - Gestito (normale)
  - Gestito (modificato)
  - Gestito (mancante)
  - Gestito (trovato)
- **Stampanti gestite (modificate):** stampanti del sistema le cui proprietà seguenti sono cambiate dall'ultimo controllo:
  - Etichetta proprietà
  - Nome host
  - Nome contatto
  - Posizione contatto
  - Dimensione memoria
  - Fronte/retro
  - Materiali di consumo (livelli esclusi)
  - Opzioni di input
  - Opzioni di stampa
  - Applicazioni eSF
  - Certificato della stampante predefinita
- **Stampanti gestite (trovate):** stampanti segnalate come mancanti, ma che ora sono state trovate.

- **Stampanti gestite (mancanti):** stampanti con le quali il sistema non è in grado di comunicare.
- **Stampanti gestite (normali):** stampanti del sistema, le cui proprietà sono rimaste invariate dall'ultimo controllo.
- **Nuove stampanti:** stampanti appena rilevate che non sono state impostate automaticamente sullo stato Gestito.
- **Stampanti ritirate:** stampanti non più attive nel sistema.
- **Stampanti non gestite:** stampanti contrassegnate per l'esclusione dalle attività eseguite nel sistema.



| Stato iniziale                | Stato finale                    | Transizione                                                              |
|-------------------------------|---------------------------------|--------------------------------------------------------------------------|
| Avvia                         | Normale                         | Rilevata. <sup>1</sup>                                                   |
| Avvia                         | Nuovo                           | Rilevata. <sup>2</sup>                                                   |
| Qualsiasi                     | Normale, Non gestito o Ritirato | Manuale (Mancante non viene modificato in Normale).                      |
| Ritirato                      | Normale                         | Rilevata. <sup>1</sup>                                                   |
| Ritirato                      | Nuovo                           | Rilevata. <sup>2</sup>                                                   |
| Normale, Mancante o Trovato   | Modificato                      | Nuovo indirizzo rilevato.                                                |
| Normale                       | Modificato                      | Le proprietà di controllo non corrispondono alle proprietà del database. |
| Normale, Modificato o Trovato | Mancante                        | Stato non trovato su controllo o di aggiornamento.                       |
| Modificato                    | Normale                         | Le proprietà di controllo corrispondono alle proprietà del database.     |
| Mancante                      | Trovato                         | Stato rilevato, di controllo o di aggiornamento.                         |
| Trovato                       | Normale                         | Stato rilevato, di controllo o di aggiornamento.                         |

<sup>1</sup> L'impostazione "Gestisci automaticamente stampanti rilevate" è attivata nel profilo di ricerca.

<sup>2</sup> L'impostazione "Gestisci automaticamente stampanti rilevate" è disattivata nel profilo di ricerca.

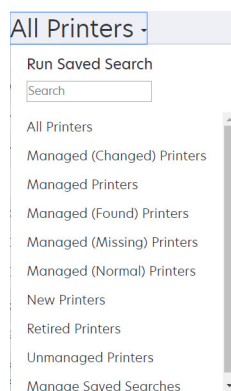


## Esecuzione di una ricerca salvata

Una ricerca salvata è un insieme di parametri salvato che restituisce le informazioni più recenti sulle stampanti in base a tali parametri.

È possibile creare ed eseguire una ricerca salvata personalizzata oppure eseguire le ricerche salvate predefinite generate dal sistema. Le ricerche salvate generate dal sistema mostrano le stampanti nei relativi stati del ciclo di vita. Per ulteriori informazioni, vedere ["Informazioni sugli stati del ciclo di vita della stampante" a pagina 47](#).

- 1 Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2 Nel menu a discesa, selezionare una ricerca salvata.



## Creazione di una ricerca salvata

### Uso dei filtri

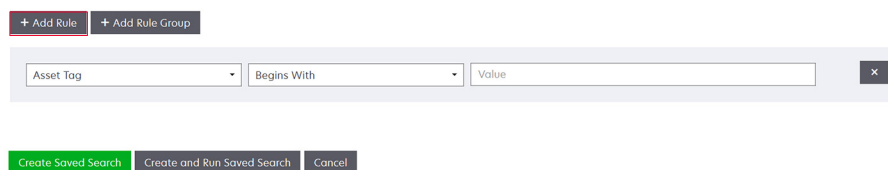
- 1 Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2 Sul lato sinistro della pagina, selezionare i filtri.  
**Nota:** i filtri selezionati sono elencati sopra l'intestazione dei risultati di ricerca.
- 3 Fare clic su **Salva**, quindi digitare un nome univoco per la ricerca salvata e la relativa descrizione.
- 4 Fare clic su **Crea ricerca salvata**.

### Uso della pagina Ricerca salvata

- 1 Nel menu Stampanti fare clic su **Ricerche salvate > Crea**.
- 2 Nella sezione Impostazioni generali digitare un nome univoco per la ricerca salvata e la relativa descrizione.
- 3 Nella sezione Regole e gruppi di regole, nel menu Corrispondenza, specificare se i risultati della ricerca devono corrispondere a tutte o ad alcune regole.
- 4 Effettuare una delle seguenti operazioni:

### Aggiungere una regola

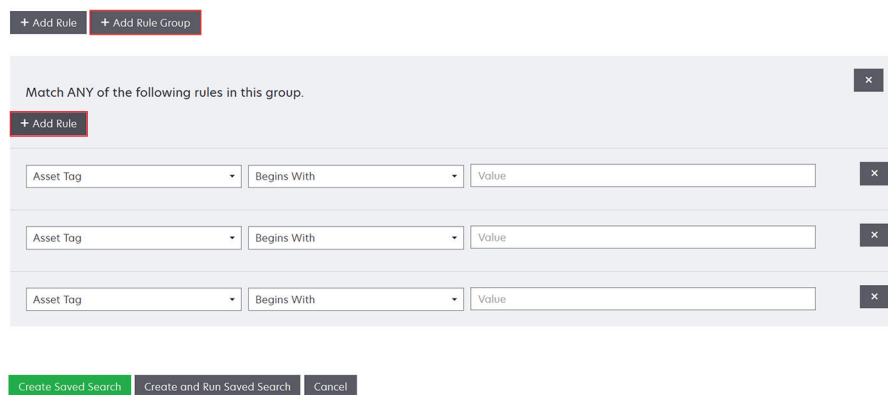
- a Fare clic su **Aggiungi regola**.
- b Specificare il parametro, l'operazione e il valore della regola di ricerca. Per ulteriori informazioni, vedere ["Informazioni sulle impostazioni delle regole di ricerca" a pagina 50](#).



### Aggiungere un gruppo di regole

Un gruppo di regole può contenere una combinazione di regole. Se il menu Corrispondenza è impostato su **QUALSIASI regola e gruppi di regole**, il sistema esegue la ricerca delle stampanti che corrispondono a tutte le regole nel gruppo di regole. Se il menu Corrispondenza è impostato su **TUTTE le regole e gruppi di regole**, il sistema esegue la ricerca delle stampanti che corrispondono a qualsiasi regola nel gruppo di regole.

- a Fare clic su **Aggiungi gruppo di regole**.
- b Specificare il parametro, l'operazione e il valore della regola di ricerca. Per ulteriori informazioni, vedere ["Informazioni sulle impostazioni delle regole di ricerca" a pagina 50](#).
- c Per aggiungere un'altra regola, fare clic su **Aggiungi regola**.



- 5 Fare clic su **Crea ricerca salvata** o **Crea ed esegui ricerca salvata**.

## Informazioni sulle impostazioni delle regole di ricerca

Cercare le stampanti utilizzando uno o più dei seguenti parametri:

| Parametro                                                 | Descrizione                                                         |
|-----------------------------------------------------------|---------------------------------------------------------------------|
| <b>Etichetta risorsa</b>                                  | Il valore dell'impostazione dell'etichetta risorsa sulla stampante. |
| <b>Data creazione del certificato<sup>1</sup></b>         | La data in cui il certificato è stato creato.                       |
| <b>Stato di registrazione del certificato<sup>1</sup></b> | Lo stato di registrazione del certificato.                          |
| <b>Data di scadenza certificato<sup>1</sup></b>           | La data di scadenza del certificato.                                |

| Parametro                                            | Descrizione                                                                                                                                                                                                                                                        |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data di rinnovo certificato<sup>1</sup></b>       | La data in cui il certificato viene rinnovato.                                                                                                                                                                                                                     |
| <b>Numero di revisione certificato<sup>1</sup></b>   | Il numero di revisione del certificato.                                                                                                                                                                                                                            |
| <b>Stato di firma del certificato<sup>1</sup></b>    | Lo stato del certificato.                                                                                                                                                                                                                                          |
| <b>Stato di validità del certificato<sup>1</sup></b> | La validità del certificato.<br><b>Nota:</b> lo stato Scadenza imminente indica che il certificato scade entro 30 giorni.                                                                                                                                          |
| <b>Funzionalità Colore</b>                           | La stampante stampa a colori o in bianco e nero.                                                                                                                                                                                                                   |
| <b>Configurazione</b>                                | Il nome della configurazione assegnato alla stampante.                                                                                                                                                                                                             |
| <b>Conformità configurazione</b>                     | Lo stato di conformità della stampante a fronte della configurazione assegnata.                                                                                                                                                                                    |
| <b>Posizione contatto</b>                            | Il valore dell'impostazione della posizione di contatto sulla stampante.                                                                                                                                                                                           |
| <b>Nome contatto</b>                                 | Il valore dell'impostazione del nome di contatto sulla stampante.                                                                                                                                                                                                  |
| <b>Copia</b>                                         | La stampante supporta la funzione Copia.                                                                                                                                                                                                                           |
| <b>Data: Aggiunta al sistema</b>                     | La data in cui la stampante è stata aggiunta al sistema.                                                                                                                                                                                                           |
| <b>Data: Ultimo controllo</b>                        | La data in cui è stato eseguito l'ultimo controllo della stampante.                                                                                                                                                                                                |
| <b>Data: Ultimo controllo conformità</b>             | La data in cui è stato eseguito l'ultimo controllo della conformità alla configurazione della stampante.                                                                                                                                                           |
| <b>Data: Ultima rilevazione</b>                      | La data in cui la stampante è stata rilevata l'ultima volta.                                                                                                                                                                                                       |
| <b>Codifica disco</b>                                | La stampante è configurata per la crittografia del disco.                                                                                                                                                                                                          |
| <b>Pulizia disco</b>                                 | La stampante è configurata per la pulizia del disco.                                                                                                                                                                                                               |
| <b>Fronte/retro</b>                                  | La stampante supporta la stampa su due lati.                                                                                                                                                                                                                       |
| <b>Funzionalità eSF</b>                              | La stampante supporta la gestione delle applicazioni eSF.                                                                                                                                                                                                          |
| <b>Informazioni eSF</b>                              | Le informazioni sull'applicazione eSF installata sulla stampante, ad esempio il nome, lo stato e la versione.                                                                                                                                                      |
| <b>Nome evento</b>                                   | Il nome degli eventi assegnati.                                                                                                                                                                                                                                    |
| <b>Nome fax</b>                                      | Il valore dell'impostazione del nome fax sulla stampante.                                                                                                                                                                                                          |
| <b>Numero fax</b>                                    | Il valore dell'impostazione del numero fax sulla stampante.                                                                                                                                                                                                        |
| <b>Ricezione fax</b>                                 | La stampante supporta la ricezione dei fax.                                                                                                                                                                                                                        |
| <b>Informazioni firmware</b>                         | Le informazioni sul firmware installato sulla stampante.<br><ul style="list-style-type: none"> <li>• <b>Nome:</b> il nome del firmware. Ad esempio, <b>Base</b> o <b>Kernel</b>.</li> <li>• <b>Versione:</b> la versione del firmware della stampante.</li> </ul>  |
| <b>Nome host</b>                                     | Il nome host della stampante.                                                                                                                                                                                                                                      |
| <b>Indirizzo IP</b>                                  | L'indirizzo IP della stampante.<br><b>Nota:</b> è possibile utilizzare un asterisco negli ultimi tre ottetti per cercare più voci. Ad esempio, <b>123.123.123.*</b> , <b>123.123.*.*</b> , <b>123.*.*.*</b> , <b>2001:db8::2:1</b> e <b>2001:db8:0:0:0:0:2:1</b> . |
| <b>Parola chiave</b>                                 | Le parole chiave assegnate.                                                                                                                                                                                                                                        |
| <b>Conteggio pagine complessive</b>                  | Il conteggio totale delle pagine della stampante.                                                                                                                                                                                                                  |

| Parametro                                           | Descrizione                                                                                                                                                |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Indirizzo MAC</b>                                | L'indirizzo MAC della stampante.                                                                                                                           |
| <b>Contatore manutenzione</b>                       | Il valore del contatore di manutenzione della stampante.                                                                                                   |
| <b>Produttore</b>                                   | Il nome del produttore della stampante.                                                                                                                    |
| <b>Tecnologia contrassegno</b>                      | La tecnologia di contrassegno supportata dalla stampante.                                                                                                  |
| <b>Funzionalità MFP</b>                             | La stampante è un prodotto multifunzione (MFP).                                                                                                            |
| <b>Modello</b>                                      | Il nome del modello di stampante.                                                                                                                          |
| <b>Numero di serie modulare</b>                     | Il numero di serie modulare.                                                                                                                               |
| <b>Stato stampante</b>                              | Lo stato della stampante. Ad esempio, <b>Pronta</b> , <b>Inceppamento carta</b> , <b>Vassoio 1 mancante</b> .                                              |
| <b>Gravità stato stampante</b>                      | Il valore dello stato più grave sulla stampante. Ad esempio, <b>Sconosciuto</b> , <b>Pronta</b> , <b>Avvertenza</b> o <b>Errore</b> .                      |
| <b>Profilo</b>                                      | La stampante supporta i profili.                                                                                                                           |
| <b>Scan to E-mail</b>                               | La stampante supporta la funzione di acquisizione su e-mail                                                                                                |
| <b>Scan to Fax</b>                                  | La stampante supporta la funzione di acquisizione su fax.                                                                                                  |
| <b>Acquisisci su rete</b>                           | La stampante supporta l'acquisizione su rete.                                                                                                              |
| <b>Stato comunicazioni protette</b>                 | Lo stato di autenticazione o di protezione della stampante.                                                                                                |
| <b>Numero di serie</b>                              | Il numero di serie della stampante.                                                                                                                        |
| <b>Stato</b>                                        | Lo stato attuale della stampante nel database.                                                                                                             |
| <b>Stato materiale di consumo</b>                   | Lo stato dei materiali di consumo della stampante.                                                                                                         |
| <b>Gravità dello stato dei materiali di consumo</b> | Il valore dello stato dei materiali di consumo più grave sulla stampante. Ad esempio, <b>Sconosciuto</b> , <b>OK</b> , <b>Avvertenza</b> o <b>Errore</b> . |
| <b>Nome sistema</b>                                 | Il nome di sistema della stampante.                                                                                                                        |
| <b>Fuso orario</b>                                  | Il fuso orario dell'area in cui si trova la stampante.                                                                                                     |
| <b>TLI</b>                                          | Il valore dell'impostazione TLI sulla stampante.                                                                                                           |

<sup>1</sup>I parametri relativi al certificato sono applicabili ai seguenti certificati periferica:

- **Predefinito**
- **HTTPS**
- **802.1x**
- **IPSec**

Utilizzare i seguenti operatori durante la ricerca delle stampanti:

- **Corrisponde esattamente:** un parametro è uguale a un valore specificato.
- **È diverso da:** un parametro è diverso da un valore specificato.
- **Contiene:** un parametro contiene un valore specificato.
- **Non contiene:** un parametro non contiene un valore specificato.
- **Inizia con:** un parametro inizia con un valore specificato.
- **Termina con:** un parametro termina con un valore specificato.

- **Data**

- **Meno recente di:** parametro che consente di eseguire la ricerca nei giorni precedenti a quelli specificati.
- **Ultimo periodo specificato:** parametro che consente di eseguire la ricerca nei giorni specificati prima di oggi.
- **Entro i prossimi:** parametro che consente di eseguire la ricerca entro i giorni specificati dopo oggi.

**Nota:** per cercare stampanti che presentano parametri con valori vuoti, utilizzare **\_EMPTY\_OR\_NULL\_**. Ad esempio, per cercare stampanti con Nome fax non specificato, nel campo Valore, digitare **\_EMPTY\_OR\_NULL\_**.

## Gestione delle ricerche salvate

**1** Nel menu Stampanti, fare clic su **Ricerche salvate**.

**2** Effettuare una delle seguenti operazioni:

### Modificare una ricerca salvata

**a** Selezionare una ricerca salvata, quindi fare clic su **Modifica**.

**Nota:** Le ricerche salvate generate dal sistema non possono essere modificate. Per ulteriori informazioni, vedere ["Informazioni sugli stati del ciclo di vita della stampante" a pagina 47](#).

**b** Configurare le impostazioni.

**c** Fare clic su **Salva modifiche** o su **Salva ed esegui**.

### Copiare una ricerca salvata

**a** Selezionare una ricerca salvata, quindi fare clic su **Copia**.

**b** Configurare le impostazioni.

**c** Fare clic su **Crea ricerca salvata** o **Crea ed esegui ricerca salvata**.

### Eliminare le ricerche salvate

**a** Selezionare una o più ricerche salvate.

**Nota:** Le ricerche salvate generate dal sistema non possono essere eliminate. Per ulteriori informazioni, vedere ["Informazioni sugli stati del ciclo di vita della stampante" a pagina 47](#).

**b** Fare clic su **Elimina**, quindi confermare l'eliminazione.

## Scenario di esempio: monitoraggio dei livelli di toner del parco stampanti

Il personale IT della società ABC deve organizzare il parco stampanti al fine di monitorarlo con facilità e desidera monitorare l'utilizzo del toner delle stampanti per determinare se i materiali di consumo devono essere sostituiti.

### Esempio di implementazione

**1** Creare una ricerca salvata che recupera le stampanti i cui materiali di consumo presentano errori o avvertenze.

Regola di esempio per la ricerca salvata

Parametro: **Gravità dello stato dei materiali di consumo**

Operazione: **Non è**

Valore: **Materiali di consumo OK**

- 2 Creare una visualizzazione che mostri lo stato, la capacità e il livello dei materiali di consumo per ciascuna stampante.

Colonne di esempio da mostrare nella visualizzazione dei materiali di consumo

**Stato materiale di consumo**

**Funzionalità Cartuccia nero**

**Livello cartuccia nero**

**Funzionalità Cartuccia ciano**

**Livello cartuccia ciano**

**Funzionalità Cartuccia magenta**

**Livello cartuccia magenta**

**Funzionalità Cartuccia giallo**

**Livello cartuccia giallo**

- 3 Eseguire la ricerca salvata mentre si utilizza la visualizzazione.

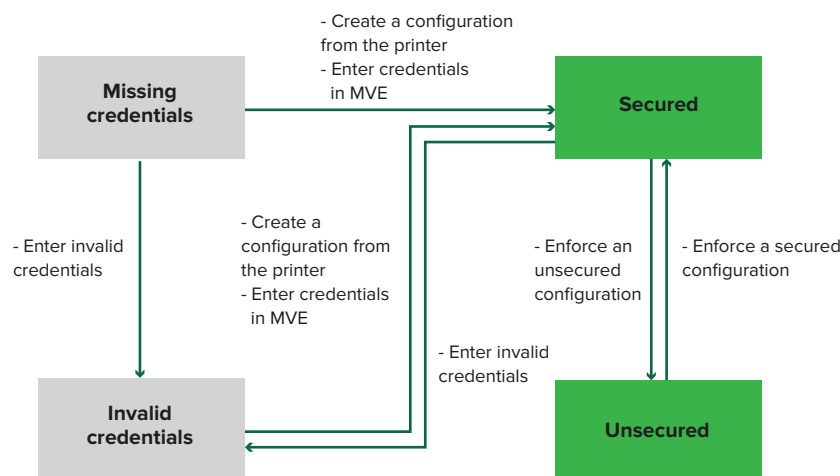
**Nota:** le informazioni visualizzate nella visualizzazione dell'elenco stampanti si basano sull'ultimo controllo. Eseguire un controllo e un aggiornamento dello stato per ottenere lo stato corrente della stampante.

# Protezione delle comunicazioni della stampante

## Informazioni sugli stati di protezione della stampante

Durante la ricerca, la stampante può trovarsi in uno dei seguenti stati:

- **Non protetto:** MVE non necessita di credenziali per comunicare con il dispositivo.
- **Protetto:** MVE necessita di credenziali che sono state fornite.
- **Credenziali mancanti:** MVE necessita di credenziali che non sono state fornite.
- **Credenziali non valide:** MVE necessita di credenziali, ma sono state fornite credenziali non corrette.



La stampante è in stato Credenziali non valide quando durante la ricerca, il controllo, l'aggiornamento dello stato, la verifica della conformità o l'applicazione della configurazione le credenziali fornite non vengono ritenute valide.

La stampante è in stato Non protetto solo quando non richiede credenziali durante la ricerca.

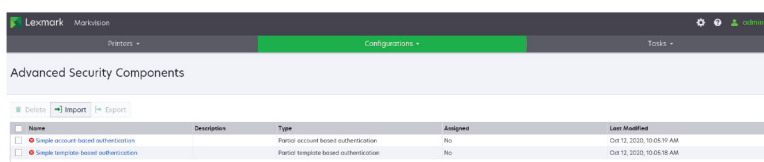
Per modificare lo stato da Non protetto a Protetto, applicare una configurazione protetta.

Per modificare lo stato Credenziali mancanti o Credenziali non valide di una stampante, immettere manualmente le credenziali in MVE oppure creare una configurazione dalla stampante.

## Protezione delle stampanti mediante le configurazioni predefinite

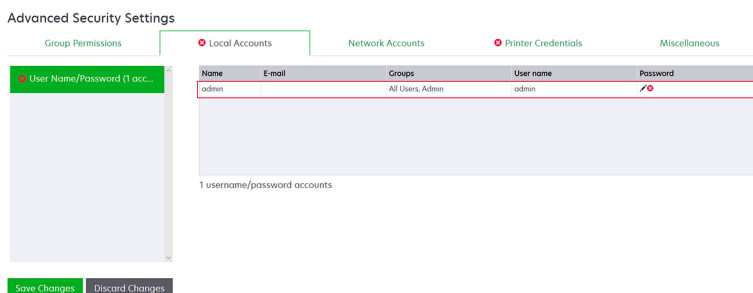
Su alcuni modelli di stampante non esiste un utente amministratore predefinito. L'utente guest può entrare liberamente senza bisogno di eseguire l'accesso. Questa impostazione consente all'utente di accedere a tutte le autorizzazioni e ai controlli di accesso della stampante. MVE gestisce questo rischio tramite le configurazioni predefinite. Dopo una nuova installazione, vengono creati automaticamente due componenti di protezione avanzata, ognuno dei quali contiene le impostazioni di protezione predefinite e l'account amministratore locale preconfigurato. È possibile utilizzare questi componenti di protezione durante la creazione di una configurazione e quindi distribuire e applicare la configurazione alle nuove stampanti.

Nel menu Configurazioni fare clic su **Tutti i componenti di protezione avanzata**.

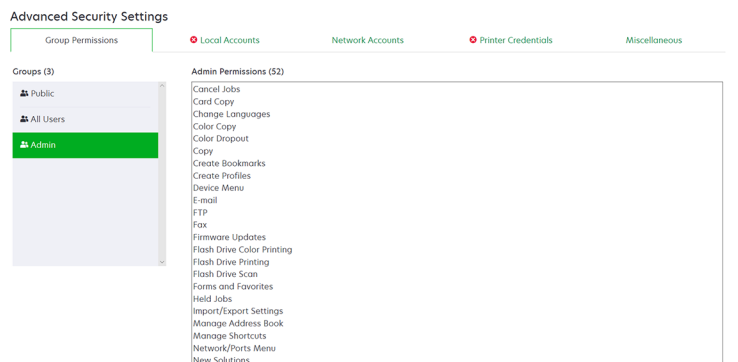


## Autenticazione semplice basata sull'account

Questo componente di protezione contiene un account locale nome utente/password chiamato **amministratore**.



L'account **amministratore** è un membro del gruppo Amministratore, le cui autorizzazioni includono le autorizzazioni e i controlli di accesso alle funzioni per proteggere la stampante e limitare l'accesso pubblico. Per ulteriori informazioni, vedere ["Informazioni sulle autorizzazioni e i controlli di accesso alle funzioni" a pagina 58](#).





Prima di aggiungere questo componente a una configurazione, assicurarsi di impostare la password per **amministratore** e le credenziali stampante.

Local Accounts Network Accounts Printer Credentials Miscellaneous

| Name  | E-mail | Groups           | User name | Password                 |
|-------|--------|------------------|-----------|--------------------------|
| admin |        | All Users, Admin | admin     | <input type="password"/> |

Advanced Security Settings

Group Permissions Local Accounts Network Accounts Printer Credentials

Select the appropriate authentication method and enter the credentials. These credentials will be used by Markvision to communicate with the set configuration is assigned.

Authentication method

Password ☒

Save Changes Discard Changes

## Autenticazione semplice basata sul modello

Questo componente di protezione contiene un modello di protezione denominato Con protezione password amministratore configurato con un Account locale password.

Local Accounts Network Accounts Printer Credentials Security Templates Access Controls Miscellaneous

Password (1 accounts)

| Name           | Admin Password | Password                 |
|----------------|----------------|--------------------------|
| Admin Password | Yes            | <input type="password"/> |

Advanced Security Settings

Local Accounts Network Accounts Printer Credentials Security Templates Access Controls Miscellaneous

| Template Name            | Authentication Setup | Authorization Setup | Group Authorization Setup |
|--------------------------|----------------------|---------------------|---------------------------|
| Admin Password Protected | Admin Password       |                     |                           |

Questo modello di protezione viene applicato ai seguenti controlli di accesso:

- Aggiornamenti firmware
- Gestione remota
- Menu Protezione da remoto

Gli altri controlli di accesso sono impostati su **Nessuna protezione**. Tuttavia, è sempre possibile impostare gli altri menu amministrativi in modo da utilizzare il modello di protezione per maggiore sicurezza. Per ulteriori informazioni sui controlli di accesso, vedere ["Informazioni sulle autorizzazioni e i controlli di accesso alle funzioni" a pagina 58](#).

Prima di aggiungere questo componente a una configurazione, assicurarsi di impostare la password e le credenziali stampante.

Advanced Security Settings

Local Accounts Network Accounts Printer Credentials Security Templates Access Controls Miscellaneous

Password (1 accounts)

| Name           | Admin Password | Password                 |
|----------------|----------------|--------------------------|
| Admin Password | Yes            | <input type="password"/> |

Advanced Security Settings

Local Accounts Network Accounts Printer Credentials Security Templates

Select the appropriate authentication method and enter the credentials. These credentials will be used by Markvision configuration is assigned.

Authentication method

Password ☒

Save Changes Discard Changes

## Informazioni sulle autorizzazioni e i controlli di accesso alle funzioni

È possibile configurare le stampanti in modo da limitare l'accesso pubblico ai menu amministrativi e alle funzioni di gestione periferiche. Nei modelli più nuovi le autorizzazioni per accedere alle funzioni della stampante si possono proteggere con diversi metodi di autenticazione. Nei modelli meno recenti è possibile applicare un modello di protezione a un controllo di accesso alle funzioni (FAC).

Per comunicare con e gestire le stampanti protette, MVE richiede alcune autorizzazioni o FAC, a seconda del modello della stampante.

Nella tabella riportata di seguito sono illustrate le funzioni della stampante che si possono essere gestire in MVE e le autorizzazioni o FAC necessari.

MVE richiede le credenziali di autenticazione quando la funzione Gestione remota è protetta. Se altri menu amministrativi e autorizzazioni di gestione periferiche o FAC sono protetti, è necessario proteggere anche Gestione remota. In caso contrario, MVE non potrà eseguire le funzioni.

Tali autorizzazioni e controlli di accesso alle funzioni sono predefiniti in MVE come componenti di protezione avanzata predefiniti e possono essere immediatamente utilizzati in una configurazione. Per ulteriori informazioni, vedere ["Protezione delle stampanti mediante le configurazioni predefinite" a pagina 56](#).

Se non si utilizzano i componenti di protezione avanzata predefiniti, assicurarsi che tali autorizzazioni e controlli di accesso alle funzioni siano configurati manualmente nella stampante. Per ulteriori informazioni, vedere ["Configurazione della protezione della stampante" a pagina 58](#).

| Autorizzazioni o FAC                                                                                         | Descrizione                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Gestione remota</b>                                                                                       | La possibilità di leggere e scrivere le impostazioni da remoto. Se una qualsiasi altra autorizzazione o FAC riportato in questa tabella è protetto, è necessario proteggere anche Gestione remota. |
| <b>Aggiornamenti firmware</b>                                                                                | La possibilità di aggiornare il firmware con qualsiasi metodo.                                                                                                                                     |
| <b>Configurazione applicazioni</b>                                                                           | La possibilità di installare o rimuovere applicazioni dalla stampante e inviare i file di impostazione delle applicazioni alla stampante.                                                          |
| <b>Importa/Esporta tutte le impostazioni</b><br>o<br><b>Importazione/esportazione file di configurazione</b> | La possibilità di inviare file di configurazione alla stampante.                                                                                                                                   |
| <b>Menu Protezione</b><br>o<br><b>Menu Protezione da remoto</b>                                              | La possibilità di gestire i metodi di accesso e configurare le opzioni di protezione della stampante.                                                                                              |

Per proteggere i modelli di stampante più recenti in MVE, disabilitare l'accesso pubblico per le autorizzazioni di Gestione remota e Menu Protezione. Per i modelli meno recenti, applicare un modello di protezione al FAC di Gestione remota.

## Configurazione della protezione della stampante

- 1 Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2 Fare clic sull'indirizzo IP della stampante, quindi fare clic su **Apri server Web incorporato**.

**3** Fare clic su **Impostazioni** o **Configurazione**.

**4** A seconda del modello di stampante, svolgere una delle seguenti operazioni:

- Fare clic su **Protezione** > **Metodi di accesso**, quindi effettuare le seguenti operazioni:

#### **Per i modelli di stampante più recenti**

- Nella sezione Protezione creare un metodo di accesso.
  - Fare clic su **Gestisci gruppi/autorizzazioni** o **Gestisci autorizzazioni** accanto al metodo di accesso.
  - Espandere **Menu amministrativi**, quindi selezionare **Menu Protezione**.
  - Espandere **Gestione periferiche**, quindi selezionare le seguenti opzioni:
    - **Gestione remota**
    - **Aggiornamenti firmware**
    - **Configurazione applicazioni**
    - **Importa/Esporta tutte le impostazioni**
  - Fare clic su **Salva**.
  - Dalla sezione Pubblico, fare clic su **Gestisci autorizzazioni**.
  - Espandere **Menu amministrativi**, quindi deselezionare **Menu Protezione**.
  - Espandere **Gestione periferiche**, quindi deselezionare **Gestione remota**.
  - Fare clic su **Salva**.
- Fare clic su **Protezione** > **Impostazione di protezione** o **Modifica impostazioni di protezione**, quindi effettuare le seguenti operazioni:

#### **Per i modelli meno recenti**

- Nella sezione Impostazione di protezione avanzata creare un blocco e un modello di protezione.
- Fare clic su **Controlli accesso**, quindi espandere **Menu amministrativi**.
- Nel menu Menu Protezione da remoto selezionare il modello di protezione.
- Espandere **Gestione**, quindi selezionare il modello di protezione per le seguenti controlli di accesso alle funzioni:
  - **Configurazione applicazioni**
  - **Gestione remota**
  - **Aggiornamenti firmware**
  - **Importazione/esportazione file di configurazione**
- Fare clic su **Invia**.

## **Protezione delle comunicazioni della stampante nel parco stampanti**

**1** Rilevare una stampante protetta. Per ulteriori informazioni, vedere ["Rilevamento delle stampanti" a pagina 34](#).

#### **Note:**

- Una stampante è protetta quando accanto al nome è visualizzata l'icona . Per informazioni sulla protezione di una stampante, vedere il [documento della Guida](#).

- Per ulteriori informazioni sugli stati di protezione della stampante, vedere ["Informazioni sugli stati di protezione della stampante" a pagina 55](#).
- 2** Creare una configurazione da una stampante. Per ulteriori informazioni, vedere ["Creazione di una configurazione da una stampante" a pagina 71](#).
- 3** Assegnare la configurazione al parco periferiche. Per ulteriori informazioni, vedere ["Assegnazione di configurazioni alle stampanti" a pagina 62](#).
- 4** Applicare la configurazione. Per ulteriori informazioni, vedere ["Applicazione delle configurazioni" a pagina 62](#). Il simbolo del lucchetto viene visualizzato accanto alla stampante protetta.

## Altri modi per proteggere le stampanti

Per ulteriori informazioni sulle impostazioni di protezione della stampante, consultare la *Guida dell'amministratore di Embedded Web Server* per la stampante in uso.

Verificare le seguenti impostazioni delle stampanti:

- La crittografia disco è abilitata.
- Le seguenti porte sono limitate:
  - TCP 79 (Finger)
  - TCP 21 (FTP)
  - UDP 69 (TFTP)
  - TCP 5001 (IPDS)
  - TCP 9600 (IPDS)
  - TCP 10000 (Telnet)
- L'elenco crittografie predefinito è la stringa di crittografia OWASP "B".

## Gestione delle stampanti

### Riavvio della stampante

- 1 Nella cartella Stampanti , fare clic su **Elenco stampanti**.
- 2 Selezionare l'indirizzo IP della stampante.
- 3 Fare clic su **Riavvia stampante**.

### Visualizzazione di Embedded Web Server della stampante

Embedded Web Server è un software incorporato in una stampante che fornisce un pannello di controllo per la configurazione della stampante da qualsiasi browser Web.

- 1 Nella cartella Stampanti , fare clic su **Elenco stampanti**.
- 2 Selezionare l'indirizzo IP della stampante.
- 3 Fare clic su **Apri Embedded Web Server**

### Controllo delle stampanti

Un controllo raccoglie le informazioni relative alle stampanti con stato Gestito e salva tali informazioni nel sistema. Per assicurarsi che le informazioni nel sistema siano aggiornate, eseguire periodicamente un controllo.

- 1 Nel menu Stampante, fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Stampante > Controllo**.

**Nota:** È possibile programmare l'esecuzione periodica di un controllo. Per ulteriori informazioni, vedere ["Creazione di un programma" a pagina 143](#).

### Aggiornamento dello stato della stampante

La funzione Aggiorna stato consente di aggiornare lo stato della stampante e le informazioni sui materiali di consumo. Per assicurarsi che lo stato della stampante e le informazioni sui materiali di consumo siano aggiornate, aggiornare regolarmente lo stato.

- 1 Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Stampante > Aggiorna stato**.

**Nota:** è possibile programmare l'esecuzione periodica di un aggiornamento di stato. Per ulteriori informazioni, vedere ["Creazione di un programma" a pagina 143](#).

## Impostazione dello stato della stampante

Per ulteriori informazioni sugli stati della stampante, vedere ["Informazioni sugli stati del ciclo di vita della stampante" a pagina 47](#).

- 1 Nel menu Stampante, fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Stampante**, quindi selezionare una delle seguenti opzioni:
  - **Imposta stato su Gestito**: la stampante viene inclusa in tutte le attività che è possibile eseguire sul sistema.
  - **Imposta stato su Non gestito**: la stampante viene esclusa da tutte le attività che è possibile eseguire sul sistema.
  - **Imposta stato su Ritirato**: la stampante viene rimossa dalla rete. Il sistema conserva le informazioni della stampante, ma non prevede di rilevare nuovamente la stampante sulla rete.

## Assegnazione di configurazioni alle stampanti

Prima di iniziare, assicurarsi che sia stata creata una configurazione per la stampante. L'assegnazione di una configurazione a una stampante consente al sistema di eseguire controlli di conformità e applicazioni. Per ulteriori informazioni, vedere ["Creazione di una configurazione" a pagina 68](#).

- 1 Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Configura > Assegna configurazioni**.
- 4 Nella sezione Configurazione selezionare una configurazione.

**Nota:** se il sistema è impostato su **Utilizzare Markvision per gestire i certificati della periferica**, selezionare **Periferiche selezionate attendibili**. Questa conferma consente all'utente di verificare che le stampanti siano periferiche reali e non falsificate.
- 5 Fare clic su **Assegna configurazioni**.

## Annullamento dell'assegnazione delle configurazioni

- 1 Nel menu Stampante, fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Configura > Annulla assegnazione configurazioni**.
- 4 Fare clic su **Annulla assegnazione configurazioni**.

## Applicazione delle configurazioni

MVE esegue un controllo di conformità sulla stampante. Se alcune impostazioni risultano non conformi, MVE le modifica sulla stampante. MVE esegue un controllo di conformità finale dopo aver modificato le impostazioni. Il completamento degli aggiornamenti che prevedono il riavvio della stampante, ad esempio gli aggiornamenti del firmware, potrebbe richiedere una seconda applicazione.

Prima di iniziare, assicurarsi alla stampante sia stata assegnata una configurazione. Per ulteriori informazioni, vedere ["Assegnazione di configurazioni alle stampanti" a pagina 62](#).

- 1 Nella cartella Stampanti , fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Configura > Applica configurazioni**.

**Note:**

- Se la stampante è in stato di errore, alcune impostazioni potrebbero non essere aggiornate.
- Affinché MVE distribuisca i file del firmware e delle soluzioni su una stampante, il controllo di accesso alla funzione Aggiornamenti firmware deve essere impostato su **Nessuna protezione**. Se la protezione è applicata, il controllo di accesso alla funzione Aggiornamenti firmware deve utilizzare lo stesso modello di protezione del controllo di accesso Gestione remota. Per ulteriori informazioni, vedere ["Distribuzione dei file alle stampanti" a pagina 63](#).
- È possibile programmare l'esecuzione periodica di un'applicazione. Per ulteriori informazioni, vedere ["Creazione di un programma" a pagina 143](#).

## Controllo della conformità di una stampante con una configurazione

Durante un controllo di conformità, MVE controlla le impostazioni della stampante e verifica se corrispondono alla configurazione assegnata. MVE non apporta alcuna modifica alla stampante durante questa operazione.

Prima di iniziare, assicurarsi alla stampante sia stata assegnata una configurazione. Per ulteriori informazioni, vedere ["Assegnazione di configurazioni alle stampanti" a pagina 62](#).

- 1 Nella cartella Stampanti , fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Configura > Controllo di conformità**.

**Note:**

- È possibile visualizzare i risultati nella pagina di stato dell'attività.
- È possibile programmare l'esecuzione periodica di un controllo di conformità. Per ulteriori informazioni, vedere ["Creazione di un programma" a pagina 143](#).

## Distribuzione dei file alle stampanti

È possibile implementare i seguenti file alla stampante:

- **Certificati CA:** i file **.cer** o **.pem** aggiunti all'archivio attendibile della stampante.
- **Configurazione bundle:** i file **.zip** che vengono esportati da una stampante supportata o ottenuti direttamente da Lexmark.
- **Aggiornamento del firmware:** un file **.fls** che viene caricato nella stampante.

- **File generici:** tutti i file che si desidera inviare alla stampante.
  - **Socket di tipo raw:** inviati tramite la porta 9100. La stampante li considera come qualsiasi altro tipo di dati di stampa.
  - **FTP:** consente di inviare file tramite FTP. Questo metodo di distribuzione non è supportato su stampanti protette.
- **Certificato stampante:** un certificato firmato che è installato sulla stampante come il certificato predefinito.
- **UCF (Universal Configuration File):** un file di configurazione esportato da una stampante.
  - **Servizio Web:** il servizio Web HTTPS viene utilizzato quando il modello di stampante lo supporta. In caso contrario, la stampante utilizza il servizio Web HTTP.
  - **FTP:** consente di inviare file tramite FTP. Questo metodo di distribuzione non è supportato su stampanti protette.

- 1 Nella cartella Stampanti , fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Configura > Distribuisci file a stampanti**.
- 4 Fare clic su **Scegli file**, quindi selezionare il file.
- 5 Selezionare un tipo di file, quindi selezionare un metodo di distribuzione.
- 6 Fare clic su **Distribuisci file**.

**Note:**

- Affinché MVE distribuisca i file del firmware e delle soluzioni su una stampante, il controllo di accesso alla funzione Aggiornamenti firmware deve essere impostato su **Nessuna protezione**. Se la protezione è applicata, il controllo di accesso alla funzione Aggiornamenti firmware deve utilizzare lo stesso modello di protezione del controllo di accesso Gestione remota.
- È possibile programmare l'esecuzione periodica di una distribuzione. Per ulteriori informazioni, vedere ["Creazione di un programma" a pagina 143](#).

## Aggiornamento del firmware delle stampanti

- 1 Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Configura > Aggiorna firmware su stampanti**.
- 4 Selezionare un file del firmware dalla libreria delle risorse oppure fare clic su **Scegli file**, quindi cercare il file del firmware.

**Nota:** per ulteriori informazioni sull'aggiunta di file del firmware alla libreria, vedere ["Importazione di file nella libreria delle risorse" a pagina 75](#).
- 5 Se necessario, per pianificare l'aggiornamento, selezionare **Definisci intervallo di tempo di aggiornamento**, quindi selezionare la data di inizio, l'ora di inizio e di interruzione e i giorni della settimana.

**Nota:** Il firmware viene inviato alle stampanti nell'intervallo tra l'ora di inizio specificata e il tempo di pausa. L'attività viene messa in pausa dopo il tempo di pausa, quindi riprende all'ora di inizio successiva finché non viene completata.
- 6 Fare clic su **Aggiorna firmware**.



**Nota:** Affinché MVE aggiorni il firmware della stampante, il controllo di accesso alla funzione Aggiornamenti firmware deve essere impostato su **Nessuna protezione**. Se la protezione è applicata, il controllo di accesso alla funzione Aggiornamenti firmware deve utilizzare lo stesso modello di protezione del controllo di accesso Gestione remota. In questo caso, MVE deve gestire la stampante nella modalità protetta. Per ulteriori informazioni, vedere ["Protezione delle comunicazioni della stampante" a pagina 55](#).

## Disinstallazione delle applicazioni dalle stampanti

MVE può disinstallare solo applicazioni aggiunte al sistema nel formato Package Builder. Per ulteriori informazioni sul caricamento delle applicazioni nel sistema, vedere ["Importazione di file nella libreria delle risorse" a pagina 75](#).

- 1 Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Configura > Disinstalla app dalle stampanti**.
- 4 Selezionare le applicazioni.
- 5 Fare clic su **Disinstalla app**.

## Assegnazione di eventi alle stampanti

L'assegnazione degli eventi alle stampanti consente a MVE di eseguire l'azione associata ogni volta che si verifica uno degli avvisi associati sulla stampante assegnata. Per ulteriori informazioni sulla creazione di eventi, vedere ["Gestione degli avvisi della stampante" a pagina 133](#).

**Nota:** Gli eventi possono essere assegnati solo alle stampanti non protette.

- 1 Nel menu Stampante, fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Assegna > gli Eventi**.
- 4 Selezionare uno o più eventi.

**Nota:** Se l'evento è già assegnato ad alcune delle stampanti selezionate, nella casella di controllo è visualizzato un trattino. Se si lascia il trattino, l'evento non viene modificato. Se si seleziona la casella di controllo, l'evento viene assegnato a tutte le stampanti selezionate. Se si deseleziona la casella di controllo, l'evento viene rimosso dalle stampanti a cui era precedentemente assegnato.

- 5 Fare clic su **Assegna eventi**.

## Assegnazione di parole chiave alle stampanti

L'assegnazione di parole chiave alle stampanti permette di organizzare le stampanti. Per ulteriori informazioni sulla creazione di parole chiave, vedere ["Gestione delle parole chiave" a pagina 47](#).

- 1 Nel menu Stampante, fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Assegna > Parole chiave**.

**4** Se necessario, nel menu **Visualizza**, selezionare una categoria.

**5** Selezionare una o più parole chiave.

**Nota:** Le parole chiave sono elencate seguendo una categoria. Se la parola chiave è già assegnata ad alcune delle stampanti selezionate, nella casella di controllo è visualizzato un trattino. Se si lascia il trattino, la parola chiave non viene assegnata o rimossa dalle stampanti selezionate. Se si seleziona la casella di controllo, la parola chiave viene assegnata a tutte le stampanti selezionate. Se si deseleziona la casella di controllo, la parola chiave viene rimossa dalle stampanti a cui era precedentemente assegnata.

**6** Fare clic su **Assegna parole chiave**.

## Immissione delle credenziali per le stampanti protette

È possibile individuare e registrare le stampanti protette. Per comunicare con tali stampanti, è possibile applicare una configurazione o immettere le credenziali direttamente in MVE.

**Nota:** Una stampante è protetta quando accanto al nome è visualizzata l'icona .

Per immettere le credenziali, effettuare una delle seguenti operazioni:

**1** Nel menu Stampanti fare clic su **Elenco stampanti**.

**2** Selezionare una o più stampanti protette.

**3** Fare clic su **Protezione > Immetti le credenziali**.

**4** Selezionare il metodo di autenticazione, quindi immettere le credenziali.

**5** Fare clic su **Immetti le credenziali**.

**Nota:** Le stampanti registrate e protette che non hanno però le credenziali corrette salvate in MVE sono contrassegnate come Credenziali mancanti sotto il filtro Comunicazioni. Dopo l'immissione delle credenziali corrette, le stampanti vengono contrassegnate con lo stato Protetto.

## Configurazione manuale dei certificati predefiniti delle stampanti

Quando non si utilizza la funzione di gestione automatica dei certificati, MVE può facilitare il processo di firma del certificato predefinito della stampante su un parco stampanti. MVE raccoglie le richieste di firma dei certificati dal parco dispositivi, quindi distribuisce i certificati firmati sulle stampanti appropriate dopo la firma.

Un amministratore di sistema deve effettuare le seguenti operazioni:

**1** Generare le richieste di firma del certificato della stampante.

**a** Nel menu Stampanti fare clic su **Elenco stampanti**.

**b** Selezionare una o più stampanti.

**c** Fare clic su **Protezione > Genera richieste di firma certificato stampante**.

**Nota:** è possibile selezionare una o più stampanti quando si generano richieste di firma dei certificati, ma può essere presente un solo gruppo di richieste per volta. Per evitare la sovrascrittura di eventuali richieste di firma dei certificati esistenti, è necessario scaricare le richieste di firma dei certificati prima di generare un altro gruppo.

- 2 Attendere il completamento dell'attività, quindi scaricare le richieste di firma dei certificati della stampante.
  - a Nel menu Stampanti fare clic su **Elenco stampanti**.
  - b Fare clic su **Protezione > Scarica richieste di firma certificato stampante**.
- 3 Utilizzare un'autorità di certificazione (CA) attendibile per firmare le richieste di firma del certificato.
- 4 Salvare i certificati firmati in un file ZIP.

**Nota:** tutti i certificati firmati devono trovarsi nella posizione radice del file ZIP. In caso contrario, MVE non potrà analizzare il file.
- 5 Nel menu Stampanti fare clic su **Elenco stampanti**.
- 6 Selezionare una o più stampanti.
- 7 Fare clic su **Configura > Distribuisci file a stampanti**.
- 8 Fare clic su **Scegli file**, quindi selezionare il file ZIP.
- 9 Nel menu Tipo file selezionare **Certificati della stampante**.
- 10 Fare clic su **Distribuisci file**.

## Rimozione di stampanti

- 1 Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2 Selezionare una o più stampanti.
- 3 Fare clic su **Stampante**.
- 4 Se necessario, per rimuovere il certificato della stampante, selezionare **Elimina certificati periferica associati**.

**Nota:** se MVE gestisce i certificati della periferica, la rimozione del certificato della stampante comporta l'eliminazione del certificato predefinito dalla stampante. La stampante genera quindi un nuovo certificato autofirmato.
- 5 Effettuare una delle seguenti operazioni:
  - Per conservare le informazioni sulla stampante, fare clic su **Ritira stampante**.
  - Per rimuovere la stampante dal sistema, fare clic su **Elimina stampante**.

# Gestione delle configurazioni

## Panoramica

MVE utilizza le configurazioni per gestire le stampanti del parco.

Una configurazione è un insieme di impostazioni che possono essere assegnate e applicate a una stampante o a un gruppo di modelli di stampante. All'interno di una configurazione, è possibile modificare le impostazioni della stampante e distribuire le applicazioni, le licenze, il firmware e i certificati delle stampanti.

È possibile creare una configurazione composta da:

- Impostazioni di base della stampante
- Impostazioni di protezione avanzate
- Autorizzazioni stampa a colori

**Nota:** questa impostazione è disponibile solo nelle configurazioni per le stampanti a colori supportate.

- Firmware delle stampanti
- Applicazioni
- Certificati CA
- File di risorse

Utilizzando le configurazioni, è possibile eseguire le seguenti operazioni per gestire le stampanti:

- Assegnare una configurazione alle stampanti.
- Applicare la configurazione alle stampanti. Le impostazioni specificate nella configurazione vengono applicate alle stampanti. Il firmware, le applicazioni, il certificato della stampante, i file dell'applicazione (.fls) e i certificati CA vengono installati.
- Controllare se le stampanti sono conformi a una configurazione. Se una stampante non è conforme, è possibile applicare la configurazione alla stampante.

**Nota:** l'applicazione della configurazione e il controllo della conformità possono essere programmati in modo che vengano eseguiti regolarmente.

- Se la stampante supporta le impostazioni di configurazione ma i valori non sono applicabili, viene visualizzata come non conforme.

## Creazione di una configurazione

Una configurazione è un insieme di impostazioni che possono essere assegnate e applicate a una stampante o a un gruppo di stampanti. All'interno di una configurazione, è possibile modificare le impostazioni della stampante e distribuire le applicazioni, le licenze, il firmware e i certificati CA alle stampanti.

- 1 Nel menu Configurazioni fare clic su **Tutte le configurazioni** > **Crea**.
- 2 Digitare un nome univoco per la configurazione e la relativa descrizione.
- 3 Nell'elenco Impostazioni, effettuare una o più delle seguenti operazioni:
  - Nella scheda Di base, selezionare una o più impostazioni, quindi specificare i valori. Se il valore è un'impostazione variabile, racchiudere l'intestazione con i simboli `${ }`. Ad esempio, `${Contact_Name}`. Per utilizzare un file delle impostazioni variabili, selezionarlo dal menu Usa file dati

delle impostazioni variabili oppure importare il file. Per ulteriori informazioni, vedere ["Informazioni sulle impostazioni delle variabili" a pagina 72](#).

Settings

Basic Advanced Security Color Print Permissions Firmware Apps Certificates Resource Files

Use variable setting data file

None Import

Show only included settings

Show settings for All models

View All settings Filter by setting name

| Setting          | Category | Value     |
|------------------|----------|-----------|
| Contact Location | General  | Demo CFCM |

- Selezionare una o più impostazioni, quindi specificare i valori. Se il valore è un'impostazione variabile, racchiudere l'intestazione con i simboli `{ }`. Ad esempio, `{Contact_Name}`. Per utilizzare un file delle impostazioni variabili, selezionarlo dal menu Usa file dati delle impostazioni variabili oppure importare il file. Per ulteriori informazioni, vedere ["Informazioni sulle impostazioni delle variabili" a pagina 72](#).

Basic Advanced Security Color Print Permissions Firmware Apps Certificates Resource Files

Use variable setting data file

ConfigVariableTest- new.csv (Imported Aug 31, 2022 2:23:39) Import

Show only included settings

Show settings for All models

View All settings Filter by setting name

| Setting          | Category | Value               |
|------------------|----------|---------------------|
| Asset Tag        | General  | S{ASSET_TAG}        |
| Contact Location | General  | S{CONTACT_LOCATION} |
| Contact Name     | General  | S{CONTACT_NAME}     |

- Se si aggiungono uno o più certificati a questa configurazione, è possibile selezionare uno dei certificati del menu a discesa **Valore**.
- Nella scheda Protezione avanzata selezionare un componente di protezione avanzata.

**Note:**

- Per creare un componente di protezione avanzata, vedere ["Creazione di un componente di protezione avanzata da una stampante" a pagina 72](#).
- È possibile gestire le impostazioni di protezione avanzata solo durante la creazione di una configurazione da una stampante selezionata. Per ulteriori informazioni, vedere ["Creazione di una configurazione da una stampante" a pagina 71](#).

- Nella scheda Autorizzazioni stampa a colori configurare le impostazioni. Per ulteriori informazioni, vedere ["Configurazione delle autorizzazioni per la stampa a colori" a pagina 73](#).

**Nota:** questa impostazione è disponibile solo nelle configurazioni per le stampanti a colori supportate.

- Nella scheda Firmware selezionare un file di firmware. Se in una configurazione sono presenti più versioni dello stesso firmware, durante la conformità e l'applicazione viene presa in considerazione solo la versione del firmware superiore. Per importare un file di firmware, vedere ["Importazione di file nella libreria delle risorse" a pagina 75](#).
- Nella scheda App selezionare una o più applicazioni da distribuire. Per ulteriori informazioni, vedere ["Creazione di un pacchetto di applicazioni" a pagina 74](#).

**Nota:** MVE non supporta la distribuzione di applicazioni con licenze di prova. È possibile distribuire solo applicazioni gratuite o applicazioni con licenze di produzione.

- Nella scheda Certificati selezionare uno o più certificati da distribuire. Per importare un file di certificato, vedere ["Importazione di file nella libreria delle risorse" a pagina 75](#).

**Nota:** selezionare **Utilizzare Markvision per gestire i certificati della periferica** affinché MVE valuti i certificati mancanti, non validi, revocati e scaduti e quindi li sostituisca automaticamente.

Selezionare una delle seguenti opzioni:

- Certificato periferica predefinito
- Certificato periferica con nome

**Nota:** per impostazione predefinita, l'utente può aggiungere 10 certificati con nome per ogni installazione MVE e 5 certificati con nome per ogni configurazione MVE.

**Nota:** Per ulteriori informazioni, vedere ["Configurazione di MVE per la gestione automatica dei certificati" a pagina 78](#).

- Nella scheda File di risorse, selezionare uno dei seguenti tipi di file da distribuire:
  - **File dell'applicazione (.fls)**
  - **Pacchetto di configurazione (.zip)**
  - **File di configurazione universale (.ucf)**

**Note:**

- Le opzioni nella scheda risorse non sono sottoposte a controllo di conformità.
- Non è consigliabile utilizzare più file UCF e pacchetti di configurazione in una singola configurazione.
- Questo metodo non è applicabile ai file UCF durante la configurazione di Acquisisci su rete sulle stampanti legacy. I file UCF devono essere distribuiti utilizzando l'azione **Distribuisci file a stampante**.

#### 4 Fare clic su **Crea configurazione**.

**Nota:** l'elenco seguente mostra la sequenza di distribuzione in una configurazione:

- **Certificati CA**
- **File dell'applicazione**
- **Pacchetti di soluzioni**
- **Protezione avanzata**
- **Certificati periferica**
- **Impostazioni di base**

- **UCF e pacchetto di configurazione**
- **Firmware**

## Creazione di una configurazione da una stampante

I seguenti componenti non sono inclusi:

- Firmware delle stampanti
- Applicazioni
- Certificati

Per aggiungere il firmware, le applicazioni e i certificati, modificare la configurazione in MVE.

- 1** Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2** Selezionare la stampante, quindi fare clic su **Configura > Crea configurazione da stampante**.
- 3** Se necessario, selezionare **Includi impostazioni di protezione avanzata** per creare un componente di protezione avanzata dalla stampante selezionata.
- 4** Se la stampante è protetta, selezionare il metodo di autenticazione, quindi immettere le credenziali.
- 5** Digitare un nome univoco per la configurazione e la relativa descrizione, quindi fare clic su **Crea configurazione**.
- 6** Nel menu Configurazioni fare clic su **Tutte le configurazioni**.
- 7** Selezionare la configurazione, quindi fare clic su **Modifica**.
- 8** Se necessario, modificare le impostazioni.
- 9** Fare clic su **Salva modifiche**.

## Scenario di esempio: clonazione di una configurazione

Quindici stampanti Lexmark MX812 sono state aggiunte al sistema dopo il rilevamento. Il personale IT deve applicare le impostazioni delle stampanti esistenti alle nuove stampanti rilevate.

**Nota:** è anche possibile clonare una configurazione da una stampante, quindi applicarla a un gruppo di modelli di stampante.

### Esempio di implementazione

- 1** Nell'elenco delle stampanti esistenti selezionare una stampante Lexmark MX812.
- 2** Creare una configurazione dalla stampante.  
**Nota:** per proteggere le stampanti, includere le impostazioni di protezione avanzata.
- 3** Assegnare e quindi applicare la configurazione alle nuove stampanti rilevate.

## Creazione di un componente di protezione avanzata da una stampante

Creare un componente di protezione avanzata da una stampante per gestire le impostazioni di protezione avanzata. MVE legge tutte le impostazioni da tale stampante, quindi crea un componente che include le impostazioni. Il componente può essere associato a più configurazioni per i modelli di stampante che hanno il medesimo framework di protezione.

- 1 Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2 Selezionare la stampante, quindi fare clic su **Configura > Crea componente di protezione avanzata dalla stampante**.
- 3 Digitare un nome univoco per il componente e la relativa descrizione.
- 4 Se la stampante è protetta, selezionare il metodo di autenticazione, quindi immettere le credenziali.
- 5 Fare clic su **Crea componente**.

**Nota:** quando si crea e si applica una configurazione con un componente di protezione avanzata che contiene account locali, gli account locali vengono aggiunti alle stampanti. Tutti gli account locali esistenti preconfigurati nella stampante vengono conservati.

## Generazione di una versione stampabile delle impostazioni di configurazione

- 1 Modificare una configurazione o un componente di protezione avanzata.
- 2 Fare clic su **Versione stampabile**.

## Informazioni sulle impostazioni dinamiche

- Queste impostazioni includono Certificato periferica 802.1x, Certificato periferica HTTPS e Certificato periferica IPsec elencate nella scheda Di base di una configurazione.
- Le opzioni per ciascuna di queste impostazioni vengono popolate con i certificati selezionati nella scheda Certificato.
- Quando si clona, esporta o importa una configurazione, i valori preselezionati di queste impostazioni vengono cancellati ed è necessario selezionare i valori manualmente.

## Informazioni sulle impostazioni delle variabili

Le impostazioni delle variabili consentono di gestire le impostazioni sul parco periferiche che sono esclusive per ciascuna stampante, ad esempio nome host o etichetta risorsa. Durante la creazione o la modifica di una configurazione, è possibile selezionare un file CSV da associare alla configurazione.

### Formato CSV di esempio:

```
IP_ADDRESS,Contact_Name,Address,Disp_Info  
1.2.3.4,John Doe,1600 Penn. Ave., Blue  
4.3.2.1,Jane Doe,1601 Penn. Ave., Red
```



```
2.3.6.5,"Joe, Jane and Douglas",1601 Penn. Ave.,Yellow  
2.3.6.7,"Joe, Jane and Douglas",1600 Penn. Ave.,He is 6'7" tall
```

Nella riga dell'intestazione del file delle variabili, la prima colonna è un token identificativo della stampante univoco. Il token deve includere una delle seguenti opzioni:

- **HOSTNAME**
- **IP\_ADDRESS**
- **SYSTEM\_NAME**
- **SERIAL\_NUMBER**

Ciascuna colonna successiva nella riga dell'intestazione del file delle variabili è un token di sostituzione definito dall'utente. Il token deve essere indicato all'interno della configurazione con il formato `${HEADER}`. Esso viene sostituito con i valori nelle righe successive quando si applica la configurazione. Verificare che i token non contengano spazi.

È possibile importare il file CSV contenente le impostazioni delle variabili durante la creazione o la modifica di una configurazione. Per ulteriori informazioni, vedere ["Creazione di una configurazione" a pagina 68](#).

## Configurazione delle autorizzazioni per la stampa a colori

MVE consente di limitare la stampa a colori per computer host e utenti specifici.

**Nota:** Questa impostazione è disponibile solo nelle configurazioni per le stampanti a colori supportate.

- 1 Nel menu Configurazioni, fare clic su **Tutte le configurazioni**.
- 2 Creare o modificare una configurazione.
- 3 Nella scheda Autorizzazioni stampa a colori, effettuare una delle seguenti operazioni:

### Configura autorizzazioni stampa a colori per i computer host

- a Nel menu Visualizza, selezionare **Computer host**, quindi **Includi autorizzazioni stampa a colori per i computer host**.
- b Fare clic su **Aggiungi**, quindi digitare il nome del computer host.
- c Per consentire la stampa a colori sul computer host, selezionare **Consenti stampa a colori**.
- d Per consentire la stampa a colori agli utenti che accedono al computer host, selezionare **Ignora autorizzazione utente**.
- e Fare clic su **Salva e aggiungi** o su **Salva**.

### Configura autorizzazioni stampa a colori per gli utenti

- a Nel menu Visualizza, selezionare **Utenti**, quindi **Includi autorizzazioni stampa a colori per gli utenti**.
- b Fare clic su **Aggiungi**, quindi digitare il nome utente.
- c Selezionare **Consenti stampa a colori**.
- d Fare clic su **Salva e aggiungi** o su **Salva**.

## Creazione di un pacchetto di applicazioni

**1** Esportare l'elenco delle stampanti da MVE utilizzando la funzione Esporta dati.

- a** Nella cartella Stampanti , fare clic su **Visualizzazioni**.
- b** Selezionare **Elenco Stampanti**, quindi fare clic su **Esporta dati**.
- c** Selezionare una ricerca salvata.
- d** Nel menu "Seleziona tipo di file per esportazione dati", selezionare **CSV**.
- e** Fare clic su **Esporta dati**.

**2** Accedere a Package Builder.

**Nota:** Se occorre accedere a Package Builder, rivolgersi al rappresentante Lexmark.

- a** Accedere al Package Builder su [cdp.lexmark.com/package-builder](http://cdp.lexmark.com/package-builder).
- b** Importare l'elenco delle stampanti, quindi fare clic su **Avanti**.
- c** Digitare la descrizione del pacchetto, quindi specificare il proprio indirizzo e-mail.
- d** Nel menu Prodotto , selezionare le applicazioni e, se necessario, aggiungere le licenze.
- e** Fare clic su **Avanti** > **Fine**. Il collegamento al download del pacchetto viene inviato all'indirizzo e-mail dell'utente.

**3** Scaricare il pacchetto.

### Note:

- MVE non supporta la distribuzione di applicazioni con licenze di prova. È possibile distribuire solo applicazioni gratuite o applicazioni con licenze di produzione. Per i codici di attivazione, contattare il rappresentante Lexmark.
- Per aggiungere le applicazioni a una configurazione, importare il pacchetto di applicazioni nella libreria delle risorse. Per ulteriori informazioni, vedere "[Importazione di file nella libreria delle risorse](#)" a [pagina 75](#).

## Importazione o esportazione di una configurazione

Prima di iniziare a importare un file di configurazione, accertarsi che venga esportato dalla stessa versione del MVE.

**1** Nel menu Configurazioni fare clic su **Tutte le configurazioni**.

**2** Effettuare una delle seguenti operazioni:

- Per importare un file di configurazione, fare clic su **Importa**, selezionare il file di configurazione e fare clic su **Importa**.
- Per esportare un file di configurazione, selezionare una configurazione, quindi fare clic su **Esporta**.

### Note:

- Durante l'esportazione di una configurazione, le password sono escluse.
- I file UCF, i pacchetti di configurazione e i file dell'applicazione non fanno parte di una configurazione esportata.

## Importazione di file nella libreria delle risorse

La libreria delle risorse è una raccolta di file di firmware, certificati CA e pacchetti di applicazioni che vengono importati in MVE. Questi file possono essere associati a una o più configurazioni.

**1** Nel menu Configurazioni fare clic su **Libreria risorse**.

**2** Fare clic su **Importa > Scegli file**, quindi selezionare il file.

**Nota:** È possibile importare solo file del firmware (.fls), file dell'applicazione (.fls), pacchetti di applicazioni o bundle di configurazione (.zip), certificati CA (.pem) e file di configurazione universale (.ucf).

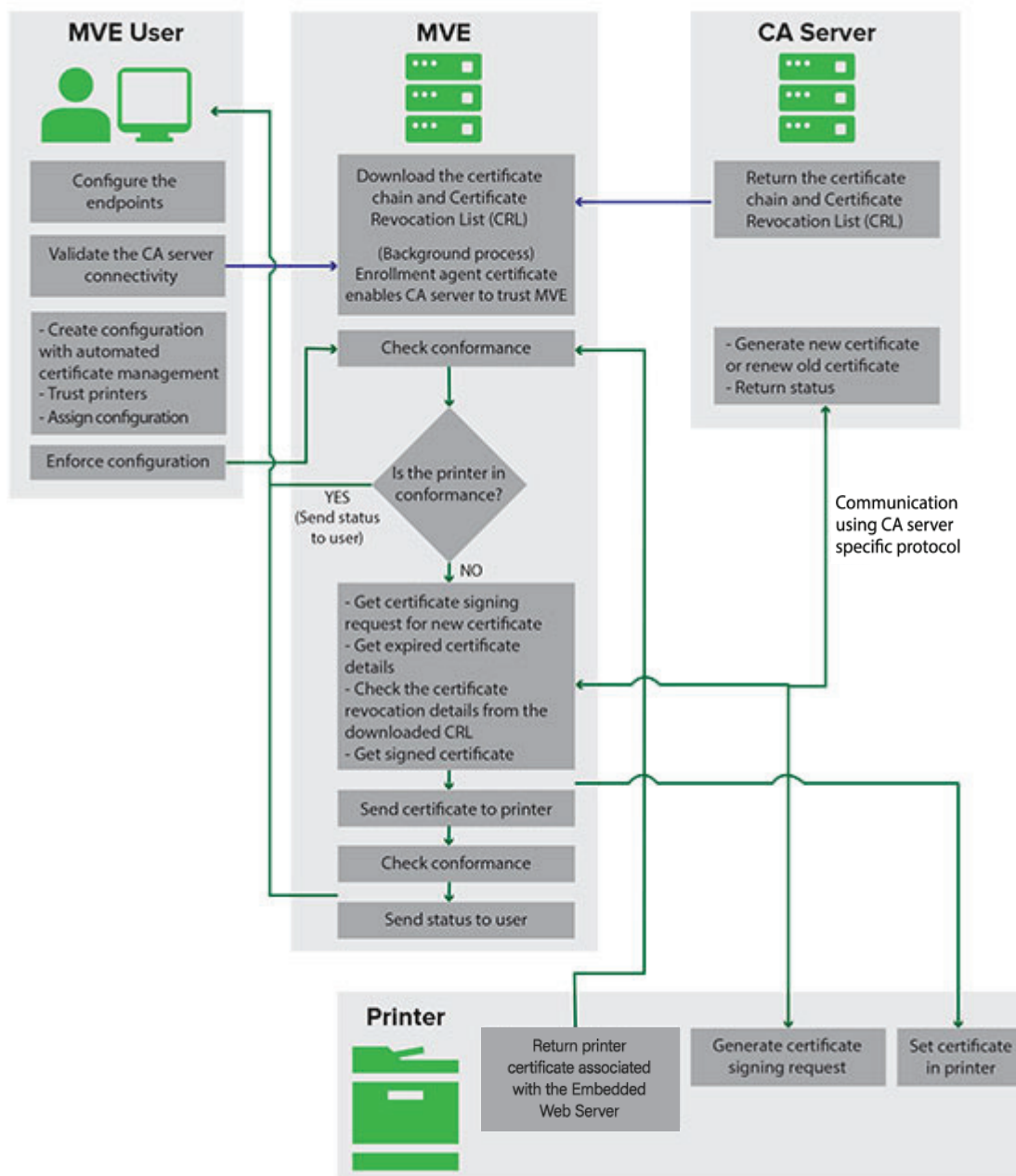
**3** Fare clic su **Importa risorsa**.

# Gestione dei certificati

## Configurazione di MVE per la gestione automatica dei certificati

### Informazioni sulla funzione di gestione automatica dei certificati

È possibile configurare MVE per gestire automaticamente i certificati delle stampanti e installarli sulle stampanti tramite applicazione della configurazione. Il seguente diagramma illustra il processo end-to-end della funzione di gestione automatica dei certificati.



Gli endpoint dell'autorità di certificazione, ad esempio il server CA e l'indirizzo del server, devono essere definiti in MVE.

Sono supportati i seguenti server CA:

- **OpenXPKI CA:** gli utenti possono utilizzare uno dei seguenti protocolli:

- SCEP (Secure Certificate Encryption Protocol)
- Connettore EST

**Note:**

- EST è il metodo consigliato per la connessione al server OpenXPKI.
- Per ulteriori informazioni sulla configurazione di OpenXPKI CA tramite il protocollo EST, vedere ["Gestione dei certificati con l'autorità di certificazione OpenXPKI tramite EST" a pagina 116](#)
- Per ulteriori informazioni sulla configurazione di OpenXPKI CA tramite il protocollo SCEP, vedere ["Gestione dei certificati con l'autorità di certificazione OpenXPKI tramite SCEP" a pagina 99](#)

- **CA Microsoft - Enterprise:** gli utenti possono utilizzare uno dei seguenti protocolli

- SCEP (Secure Certificate Encryption Protocol)
- Servizi Web di registrazione certificati Microsoft (MSCEWS)

**Note:**

- MSCEWS è il metodo consigliato per la connessione al server CA Microsoft - Enterprise.
- Per ulteriori informazioni sulla configurazione di CA Microsoft tramite il protocollo MSCEWS, vedere ["Gestione dei certificati con l'autorità di certificazione Microsoft tramite MSCEWS" a pagina 88](#)
- Per ulteriori informazioni sulla configurazione di CA Microsoft tramite il protocollo SCEP, vedere ["Gestione dei certificati con l'autorità di certificazione Microsoft tramite SCEP" a pagina 81](#)

La connessione tra MVE e i server CA deve essere convalidata. Durante la convalida, MVE comunica con il server CA per scaricare la catena di certificati e l'elenco di revoche di certificati (CRL). Viene generato anche il certificato agente o il certificato di test di registrazione. Questo certificato consente al server CA di considerare attendibile MVE.

Per ulteriori informazioni sulla definizione degli endpoint e la convalida, vedere ["Configurazione di MVE per la gestione automatica dei certificati" a pagina 78](#).

È necessario che una configurazione impostata su **Utilizzare Markvision per gestire i certificati della periferica** sia assegnata e applicata alla stampante.

Per ulteriori informazioni, vedere i seguenti argomenti:

- ["Creazione di una configurazione" a pagina 68](#)
- ["Applicazione delle configurazioni" a pagina 62](#)

Durante l'applicazione, MVE verifica la conformità della stampante.

**Per Certificato periferica predefinito**

- Il certificato viene convalidato rispetto alla catena di certificati scaricata dal server CA.
- Se la stampante non è conforme, viene richiesta una CSR, ovvero una richiesta di firma certificato, per la stampante.

**Per Certificato periferica con nome**

- Il certificato viene convalidato rispetto alla catena di certificati scaricata dal server CA.
- MVE crea un certificato periferica con nome autofirmato sul dispositivo.
- Se la stampante non è conforme, viene richiesta una CSR per la stampante.

**Note:**

- MVE comunica con il server CA tramite i protocolli configurati.
- Il server CA genera il nuovo certificato, quindi MVE invia il certificato alla stampante.
- Se nella stampante esiste un certificato con nome, non viene creato un nuovo certificato con nome, ma viene generata una CSR per la stampante.

## Configurazione di MVE per la gestione automatica dei certificati

**1** Fare clic su  nell'angolo superiore destro della pagina.

**2** Fare clic su **Autorità di certificazione > Utilizza server dell'autorità di certificazione.**

**Nota:** il pulsante Utilizza server dell'autorità di certificazione viene visualizzato solo quando si configura l'autorità di certificazione per la prima volta o quando il certificato viene eliminato.

**3** Configurare gli endpoint del server.

- **Server CA:** il server CA che genera i certificati della stampante. È possibile selezionare una delle opzioni seguenti:

- **OpenXPki CA**
- **CA Microsoft - Enterprise**

**Nota:** l'utente può anche configurare un server CA che supporta il protocollo **Enrollment over Secure Transport (EST)**.

- Il server CA deve implementare il protocollo EST come definito in RFC 7030.

**Nota:** qualsiasi deviazione dalla specifica può causare un'impostazione non valida.

- EST è il protocollo consigliato per la connessione al server OpenXPki CA.

**Nota:** il server CA Microsoft - Enterprise non supporta il protocollo EST.

- **Indirizzo del server CA:** l'indirizzo IP o il nome host del server CA. Questo campo è applicabile solo per i protocolli SCEP ed EST.

**Nota:** digitare una delle seguenti opzioni:

- Per il server MSCA (tramite SCEP): <Indirizzo IP o nome host del server>/certsrv/mscep/mscep.dll
- Per il server OpenXPki (tramite SCEP): <Indirizzo IP o nome host del server>/scep/scep
- Per EST, digitare una delle seguenti opzioni:
  - https://172.87.95.240
  - https://estserver.com
  - estserver.com

- **Etichetta server CA (opzionale):** se l'utente crea una nuova area di autenticazione, è necessario inserire in questo campo lo stesso nome dell'area di autenticazione.

- **Indirizzo server CEP:** questo campo è applicabile solo per il protocollo MSCEWS.

**Nota:** digitare una delle seguenti opzioni:

- Per l'autenticazione tramite nome utente e password:  
https://democep.com/ADPolicyProvider\_CEP\_UsernamePassword/service.svc/CEP
- Per l'autenticazione integrata di Windows:  
https://democep.com/ADPolicyProvider\_CEP\_Kerberos/service.svc/CEP

- Per l'autenticazione con certificato client:  
`https://democep.com/ADPolicyProvider_CEP_Certificate/service.svc/CEP`

- **Nome host server CA:** il nome host del server CA.

**Nota:** ad esempio, per il protocollo MSCEWS l'utente può selezionare **democa.lexmark.com**

- **Nome host server CES:** il nome host del server CES.

**Nota:** ad esempio, per il protocollo MSCEWS l'utente può selezionare **democes.lexmark.com**

- **Password di verifica:** password di verifica necessaria per l'asserzione dell'identità di MVE al server CA. Questa password è necessaria solo per OpenXPki CA. Non è supportata in CA Microsoft - Enterprise.

**Nota:** a seconda del server CA in uso, è necessario configurare la modalità di autenticazione del server. Effettuare una delle seguenti operazioni:

- Se si seleziona il protocollo **EST**, nel menu **Modalità di autenticazione del server CA** selezionare una delle seguenti opzioni:
  - **Autenticazione tramite nome utente e password**
  - **Autenticazione certificato client**
- Se si seleziona il protocollo **MSCEWS**, nel menu **Modalità di autenticazione del server CA** selezionare una delle seguenti opzioni:
  - **Autenticazione tramite nome utente e password**
  - **Autenticazione certificato client**
  - **Autenticazione integrata di Windows**
- Il protocollo **SCEP** supporta solo la modalità di autenticazione **Password di verifica**.

**Nota:** a seconda del server CA in uso, vedere una delle seguenti sezioni:

- ["Gestione dei certificati con l'autorità di certificazione OpenXPki tramite SCEP" a pagina 99](#)
- ["Gestione dei certificati con l'autorità di certificazione Microsoft tramite SCEP" a pagina 81](#)
- ["Gestione dei certificati con l'autorità di certificazione Microsoft tramite MSCEWS" a pagina 88](#)
- ["Gestione dei certificati con l'autorità di certificazione OpenXPki tramite EST" a pagina 116](#)

#### 4 Fare clic su **Salva le modifiche e convalida** > **OK**.

##### **Note:**

- L'opzione **Rifiuta modifiche** funziona solo se le modifiche non sono ancora state salvate o salvate e convalidate.
- L'utente non può recuperare i dati da una configurazione non valida, in quanto MVE non memorizza l'ultimo stato valido di alcuna configurazione. MVE memorizza una sola configurazione di certificato alla volta, che potrebbe essere valida o non valida.

##### **Note:**

- La connessione tra MVE e i server CA deve essere convalidata. Durante la convalida, MVE comunica con il server CA per scaricare la catena di certificati e l'elenco di revoche di certificati (CRL). Viene generato anche il certificato agente o il certificato di test di registrazione. Questo certificato consente al server CA di considerare attendibile MVE.
- Quando si utilizza il protocollo MSCEWS, è possibile selezionare uno o più modelli CEP. Attenersi alla seguente procedura:

- a** Dopo aver fatto clic su **Salva le modifiche e convalida**, viene visualizzata la finestra Selezione del modello CEP.
- b** Selezionare uno o più modelli tra quelli disponibili.
  - La finestra di dialogo Utilizza server dell'autorità di certificazione recupera l'elenco di revoche di certificati.
  - Una finestra di dialogo conferma che la convalida del certificato ha avuto esito positivo.
- c** È possibile visualizzare i modelli CEP selezionati nella pagina di configurazione del server CA.

**Nota:** quando si applica questa configurazione a qualsiasi dispositivo, viene creato un certificato sulla base del modello selezionato.

- 5** Tornare alla pagina Configurazione di sistema, quindi esaminare il certificato CA.

**Nota:** è anche possibile scaricare o eliminare il certificato CA.

## Configurazione della CA Microsoft Enterprise con NDES

### Panoramica

Nel seguente scenario di distribuzione, tutte le autorizzazioni si basano sulle autorizzazioni impostate nei modelli di certificato pubblicati nel controller di dominio. Le richieste di certificato inviate alla CA si basano sui modelli di certificato.

Per questa impostazione, assicurarsi di disporre di quanto segue:

- Un computer che ospita l'autorità di certificazione subordinata
- Un computer che ospita il servizio NDES
- Un controller di dominio

### Utenti richiesti

Creare i seguenti utenti nel controller di dominio:

- Amministratore del servizio
  - Denominato **SCEPAdmin**
  - Deve essere un membro dei gruppi **local admin** ed **Enterprise Admin**
  - Deve aver effettuato l'accesso localmente quando si attiva il ruolo NDES
  - Dispone di **autorizzazione alla registrazione** per i modelli di certificato
  - Dispone di **autorizzazione all'aggiunta di modelli** per la CA
- Account di servizio
  - Denominato **SCEPSvc**
  - Deve essere un membro del gruppo **IIS\_IUSRS**
  - Deve essere un utente di dominio e disporre di autorizzazioni alla **lettura** e alla **registrazione** per i modelli configurati
  - Dispone di autorizzazione alla **richiesta** per la CA
- Amministratore CA Enterprise
  - Denominato **CAAdmin**
  - Membro del gruppo **Enterprise Admin**
  - Deve far parte del gruppo di **amministrazione locale**



## Gestione dei certificati con l'autorità di certificazione Microsoft tramite SCEP

Questa sezione fornisce istruzioni sui seguenti argomenti:

- Configurazione dell'autorità di certificazione (CA) Microsoft Enterprise con il servizio Registrazione dispositivi di rete (NDES)
- Creazione di un server CA radice

**Nota:** in questo documento, per tutte le impostazioni viene utilizzato il sistema operativo Windows Server 2016.

### Panoramica

Il server CA radice è il server CA principale in qualsiasi organizzazione ed è al vertice dell'infrastruttura PKI. La CA radice autentica il server CA subordinata. Questo server viene generalmente mantenuto in modalità offline per evitare eventuali intrusioni e per proteggere la chiave privata.

Per configurare il server CA radice, procedere come segue:

- 1 Verificare che il server CA radice sia installato. Per ulteriori informazioni, vedere ["Installazione del server CA radice" a pagina 81](#).
- 2 Configurare le impostazioni Punto di distribuzione CRL e Accesso alle informazioni dell'autorità. Per ulteriori informazioni, vedere ["Configurazione delle impostazioni Punto di distribuzione CRL e Accesso alle informazioni dell'autorità" a pagina 84](#).
- 3 Configurare l'accessibilità al CRL. Per ulteriori informazioni, vedere ["Configurazione dell'accessibilità al CRL" a pagina 85](#).

### Installazione del server CA radice

- 1 In Server Manager, fare clic su **Gestisci > Aggiungi ruoli e funzionalità**.
- 2 Fare clic su **Ruoli server**, selezionare **Servizi certificati Active Directory** e tutte le relative funzioni, quindi fare clic su **Avanti**.
- 3 Nella sezione Servizi del ruolo Servizi certificati Active Directory selezionare **Autorità di certificazione**, quindi fare clic su **Avanti > Installa**.
- 4 Dopo l'installazione, fare clic su **Configurare Servizi certificati Active Directory nel server di destinazione**.
- 5 Nella sezione Servizi ruolo selezionare **Autorità di certificazione > Avanti**.
- 6 Nella sezione Tipo di installazione selezionare **CA autonoma**, quindi fare clic su **Avanti**.
- 7 Nella sezione Tipo CA selezionare **CA radice**, quindi fare clic su **Avanti**.
- 8 Selezionare **Crea una nuova chiave privata**, quindi fare clic su **Avanti**.
- 9 Nel menu Selezionare un provider di crittografia selezionare **RSA#Microsoft Software Key Storage Provider**.
- 10 Nel menu Lunghezza chiave selezionare **4096**.
- 11 Nell'elenco degli algoritmi hash selezionare **SHA512**, quindi fare clic su **Avanti**.

**12** Nel campo Nome comune per questo CA immettere il nome del server di hosting.

**13** Nel campo Suffisso nome distinto digitare il componente del dominio.

### Configurazione del nome CA di esempio

Nome di dominio completo (FQDN) del computer: **test.dev.lexmark.com**

Nome comune (CN): **TEST**

Suffisso nome distinto: **DC=DEV, DC=LEXMARK, DC=COM**

**14** Fare clic su **Avanti**.

**15** Specificare il periodo di validità, quindi fare clic su **Avanti**.

**Nota:** in genere il periodo di validità è di 10 anni.

**16** Non modificare nulla nella finestra delle posizioni di database.

**17** Completare l'installazione.

## Configurazione della CA Microsoft Enterprise con NDES

### Panoramica

Nel seguente scenario di distribuzione, tutte le autorizzazioni si basano sulle autorizzazioni impostate nei modelli di certificato pubblicati nel controller di dominio. Le richieste di certificato inviate alla CA si basano sui modelli di certificato.

Per questa impostazione, assicurarsi di disporre di quanto segue:

- Un computer che ospita l'autorità di certificazione subordinata
- Un computer che ospita il servizio NDES
- Un controller di dominio

### Utenti richiesti

Creare i seguenti utenti nel controller di dominio:

- Amministratore del servizio
  - Denominato **SCEPAdmin**
  - Deve essere un membro dei gruppi **local admin** ed **Enterprise Admin**
  - Deve aver effettuato l'accesso localmente quando si attiva il ruolo NDES
  - Dispone di **autorizzazione alla registrazione** per i modelli di certificato
  - Dispone di **autorizzazione all'aggiunta di modelli** per la CA
- Account di servizio
  - Denominato **SCEPSvc**
  - Deve essere un membro del gruppo **IIS\_IUSRS**
  - Deve essere un utente di dominio e disporre di autorizzazioni alla **lettura** e alla **registrazione** per i modelli configurati
  - Dispone di autorizzazione alla **richiesta** per la CA

## Configurazione del server CA subordinata

### Panoramica

Il server CA subordinata è il server CA intermedia ed è sempre online. Si occupa in generale della gestione dei certificati.

Per configurare il server CA subordinata, procedere come segue:

- 1 Verificare che il server CA subordinata sia installato. Per ulteriori informazioni, vedere ["Installazione del server CA subordinata" a pagina 83](#).
- 2 Configurare le impostazioni Punto di distribuzione CRL e Accesso alle informazioni dell'autorità. Per ulteriori informazioni, vedere ["Configurazione delle impostazioni Punto di distribuzione CRL e Accesso alle informazioni dell'autorità" a pagina 84](#).
- 3 Configurare l'accessibilità al CRL. Per ulteriori informazioni, vedere ["Configurazione dell'accessibilità al CRL" a pagina 85](#).

### Installazione del server CA subordinata

- 1 Sul server, accedere come utente di dominio **CAAdmin**.
- 2 In Server Manager, fare clic su **Gestisci > Aggiungi ruoli e funzionalità**.
- 3 Fare clic su **Ruoli server**, selezionare **Servizi certificati Active Directory** e tutte le relative funzioni, quindi fare clic su **Avanti**.
- 4 Nella sezione Servizi del ruolo Servizi certificati Active Directory selezionare **Autorità di certificazione e Registrazione Web autorità di certificazione**, quindi fare clic su **Avanti**.  
**Nota:** assicurarsi che siano aggiunte tutte le funzioni di Registrazione Web autorità di certificazione.
- 5 Nella sezione Servizi ruolo server Web (IIS) conservare le impostazioni predefinite.
- 6 Dopo l'installazione, fare clic su **Configurare Servizi certificati Active Directory nel server di destinazione**.
- 7 Nella sezione Servizi ruolo selezionare **Autorità di certificazione e Registrazione Web autorità di certificazione**, quindi fare clic su **Avanti**.
- 8 Nella sezione Tipo di installazione selezionare **CA Enterprise**, quindi fare clic su **Avanti**.
- 9 Nella sezione Tipo CA selezionare **CA subordinata**, quindi fare clic su **Avanti**.
- 10 Selezionare **Crea una nuova chiave privata**, quindi fare clic su **Avanti**.
- 11 Nel menu Selezionare un provider di crittografia selezionare **RSA#Microsoft Software Key Storage Provider**.
- 12 Nel menu Lunghezza chiave selezionare **4096**.
- 13 Nell'elenco degli algoritmi hash selezionare **SHA512**, quindi fare clic su **Avanti**.
- 14 Nel campo Nome comune per questo CA immettere il nome del server host.
- 15 Nel campo Suffisso nome distinto digitare il componente del dominio.

**Configurazione del nome CA di esempio**

Nome di dominio completo (FQDN) del computer: **test.dev.lexmark.com**

Nome comune (CN): **TEST**

Suffisso nome distinto: **DC=DEV, DC=LEXMARK, DC=COM**

- 16** Nella finestra di dialogo Richiesta certificato salvare il file di richiesta, quindi fare clic su **Avanti**.
- 17** Non modificare nulla nella finestra delle posizioni di database.
- 18** Completare l'installazione.
- 19** Firmare la richiesta CA della CA radice, quindi esportare il certificato autofirmato in formato PKCS7.
- 20** Sul server CA subordinata, aprire **Autorità di certificazione**.
- 21** Nel pannello di sinistra, fare clic con il pulsante destro del mouse sulla CA, quindi scegliere **Tutte le attività > Installa certificato CA**.
- 22** Selezionare il certificato autofirmato, quindi avviare il servizio CA.

## **Configurazione delle impostazioni Punto di distribuzione CRL e Accesso alle informazioni dell'autorità**

**Nota:** configurare le impostazioni Punto di distribuzione CRL (CDP) e Accesso alle informazioni dell'autorità (AIA) per l'elenco di revoche di certificati (CRL).

- 1** In Server Manager fare clic su **Strumenti > Autorità di certificazione**.
- 2** Nel pannello di sinistra, fare clic con il pulsante destro del mouse sulla CA, quindi scegliere **Proprietà > Estensioni**.
- 3** Nel menu Seleziona estensione selezionare **Punto di distribuzione CRL**.
- 4** Nell'elenco di revoche di certificati, selezionare la voce **C:\Windows\system32\**, quindi effettuare le seguenti operazioni:
  - a** Selezionare **Pubblica CRL nel percorso specificato**.
  - b** Deselezionare **Pubblica Delta CRL in questa posizione**.
- 5** Eliminare tutte le altre voci tranne **C:\Windows\system32\**.
- 6** Fare clic su **Aggiungi**.
- 7** Nel campo Posizione aggiungere **http://serverIP/CertEnroll/<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl**, dove **serverIP** è l'indirizzo IP del server.

**Nota:** Se il server è raggiungibile tramite il nome di dominio completo (FQDN), utilizzare **<ServerDNSName>** anziché l'indirizzo IP del server.
- 8** Fare clic su **OK**.
- 9** Selezionare **Includi nell'estensione dei punti di distribuzione dei certificati emessi** per la voce creata.
- 10** Nel menu Seleziona estensione selezionare **Accesso alle informazioni dell'autorità (AIA)**.
- 11** Eliminare tutte le altre voci tranne **C:\Windows\system32\**.
- 12** Fare clic su **Aggiungi**.

- 13 Nel campo Posizione aggiungere **`http://serverIP/CertEnroll/<ServerDNSName>_<CAName><CertificateName>.crt`**, dove **serverIP** è l'indirizzo IP del server.  
  
**Nota:** Se il server è raggiungibile tramite il nome di dominio completo (FQDN), utilizzare **<ServerDNSName>** anziché l'indirizzo IP del server.
- 14 Fare clic su **OK**.
- 15 Selezionare **Includi nell'estensione AIA dei certificati emessi** per la voce creata.
- 16 Fare clic su **Applica > OK**.  
  
**Nota:** se necessario, riavviare il servizio di certificazione.
- 17 Nel pannello di sinistra, espandere la CA, fare clic con il pulsante destro del mouse su **Certificati revocati**, quindi scegliere **Proprietà**.
- 18 Specificare il valore per l'intervallo di pubblicazione CRL e per Pubblica l'intervallo di pubblicazione Delta CRL, quindi fare clic su **Applica > OK**.
- 19 Nel pannello di sinistra, fare clic con il pulsante destro del mouse su **Certificati revocati**, scegliere **Tutte le attività**, quindi pubblicare il CRL Nuovo.

## Configurazione dell'accessibilità al CRL

**Nota:** prima di iniziare, assicurarsi che Gestione Internet Information Services (IIS) sia installato.

- 1 In Gestione IIS, espandere la CA, quindi espandere **Siti**.
- 2 Fare clic con il pulsante destro del mouse su **Sito Web predefinito**, quindi scegliere **Aggiungi directory virtuale**.
- 3 Nel campo Alias digitare **CertEnroll**.
- 4 Nel campo Percorso fisico digitare **C:\Windows\System32\CertSrv\CertEnroll**.
- 5 Fare clic su **OK**.
- 6 Fare clic con il pulsante destro del mouse su **CertEnroll**, quindi scegliere **Modifica autorizzazioni**.
- 7 Nella scheda Protezione rimuovere tutti gli accessi in scrittura, tranne che per il sistema.
- 8 Fare clic su **OK**.

## Configurazione del server NDES

- 1 Sul server, accedere come utente di dominio **SCEPAdmin**.
- 2 In Server Manager, fare clic su **Gestisci > Aggiungi ruoli e funzionalità**.
- 3 Fare clic su **Ruoli server**, selezionare **Servizi certificati Active Directory** e tutte le relative funzioni, quindi fare clic su **Avanti**.
- 4 Nella sezione Servizi del ruolo Servizi certificati Active Directory deselezionare **Autorità di certificazione**.
- 5 Selezionare **Servizio Registrazione dispositivi di rete** e tutte le relative funzioni, quindi fare clic su **Avanti**.
- 6 Nella sezione Servizi ruolo server Web (IIS) conservare le impostazioni predefinite.

- 7 Dopo l'installazione, fare clic su **Configurare Servizi certificati Active Directory nel server di destinazione**.
- 8 Nella sezione Servizi ruolo selezionare **Servizio Registrazione dispositivi di rete**, quindi fare clic su **Avanti**.
- 9 Selezionare l'account di servizio **SCEPSvc**.
- 10 Nella sezione CA per NDES selezionare **Nome CA** o **Nome computer**, quindi fare clic su **Avanti**.
- 11 Nella sezione Informazioni RA specificare le informazioni, quindi fare clic su **Avanti**.
- 12 Nella sezione Crittografia per NDES effettuare le seguenti operazioni:
  - Selezionare i provider di firma e chiave di crittografia appropriati.
  - Nel menu Lunghezza chiave selezionare la stessa lunghezza chiave del server CA.
- 13 Fare clic su **Avanti**.
- 14 Completare l'installazione.

È ora possibile accedere al server NDES da un browser Web come utente SCEPSvc. Sul server NDES, è possibile visualizzare l'identificazione personale del certificato CA, la password di verifica di registrazione e il periodo di validità di tale password.

### Accesso al server NDES

Aprire un browser Web e digitare **http://NDESServerIP/certsrv/mscep\_admin**, dove **NDESServerIP** è l'indirizzo IP del server NDES.

## Configurazione di NDES per MVE

**Nota:** prima di iniziare, accertarsi che il server NDES funzioni correttamente.

### Creazione di un modello di certificato

- 1 Sul server CA subordinata (certserv), aprire **Autorità di certificazione**.
- 2 Nel pannello di sinistra, espandere la CA, fare clic con il pulsante destro del mouse su **Modelli di certificato**, quindi scegliere **Gestisci**.
- 3 In Console dei modelli di certificato, creare una copia del **Server Web**.
- 4 Nella scheda Impostazioni generali digitare **MVEWebServer** come nome del modello.
- 5 Nella scheda Protezione assegnare agli utenti **SCEPAdmin** e **SCEPSvc** le autorizzazioni appropriate.  
**Nota:** per ulteriori informazioni, vedere ["Utenti richiesti" a pagina 82](#).
- 6 Nella scheda Nome oggetto selezionare **Inserisci nella richiesta**.
- 7 Sul server CA subordinata (certserv), aprire **Autorità di certificazione**.
- 8 Nella scheda Estensioni selezionare **Criteri di applicazione > Modifica**.
- 9 Fare clic su **Aggiungi > Autenticazione client > OK**.
- 10 Nel pannello di sinistra, espandere la CA, fare clic con il pulsante destro del mouse su **Modelli di certificato**, quindi scegliere **Nuovo > Modello di certificato da rilasciare**.
- 11 Selezionare i certificati appena creati, quindi fare clic su **OK**.

È ora possibile accedere ai modelli utilizzando il portale di registrazione Web della CA.

### Accesso ai modelli

- 1 Aprire un browser Web e digitare **http://CAserverIP/certsrv/certrqxt.asp**, dove **CAserverIP** è l'indirizzo IP del server CA.
- 2 Nel menu Modello certificato visualizzare i modelli.

### Impostazione dei modelli di certificato per il servizio Registrazione dispositivi di rete (NDES)

- 1 Sul computer avviare l'editor del Registro di sistema.
- 2 Accedere a **HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Crittografia > MSCEP**.
- 3 Configurare le seguenti chiavi, quindi impostarle su **MVEWebServer**:
  - EncryptionTemplate
  - GeneralPurposeTemplate
  - SignatureTemplate
- 4 Assegnare all'utente SCEPSvc le autorizzazioni complete per MSCEP.
- 5 In Gestione IIS, espandere la CA, quindi fare clic su **Pool di applicazioni**.
- 6 Nel pannello di destra, fare clic su **Ricicla** per riavviare il pool di applicazioni SCEP.
- 7 In Gestione IIS, espandere la CA, quindi espandere **Siti > Sito Web predefinito**.
- 8 Nel pannello di destra, fare clic su **Riavvia**.

### Disabilitazione della Password di verifica nel server CA Microsoft

- 1 Sul computer avviare l'editor del Registro di sistema.
- 2 Accedere a **HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Crittografia > MSCEP**.
- 3 Impostare EnforcePassword su **0**.
- 4 In Gestione IIS, espandere la CA, fare clic su **Pool di applicazioni**, quindi selezionare **SCEP**.
- 5 Nel pannello di destra, fare clic su **Impostazioni avanzate**.
- 6 Impostare Carica profilo utente su **True**, quindi fare clic su **OK**.
- 7 Nel pannello di destra, fare clic su **Ricicla** per riavviare il pool di applicazioni SCEP.
- 8 In Gestione IIS, espandere la CA, quindi espandere **Siti > Sito Web predefinito**.
- 9 Nel pannello di destra, fare clic su **Riavvia**.

Quando si apre il servizio Registrazione dispositivi di rete (NDES) dal browser Web, ora è possibile visualizzare solo l'identificazione personale della CA.

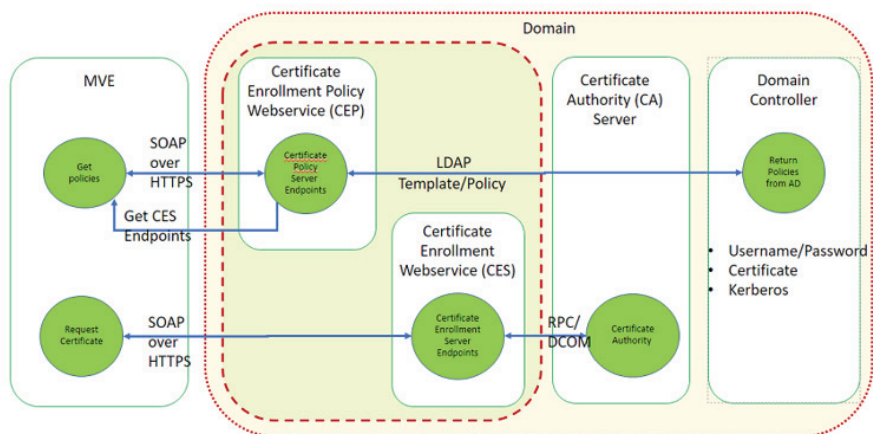
## Gestione dei certificati con l'autorità di certificazione Microsoft tramite MSCEWS

Questa sezione fornisce informazioni sulla configurazione del servizio Web di informazioni sulle registrazioni di certificati (CEP) e il servizio Web di registrazione certificati (CES). Poiché Microsoft consiglia di installare CEP e CES in due computer diversi, in questo documento si segue la stessa procedura. Questi servizi Web vengono rispettivamente elencati come server CEP e server CES.

**Nota:** l'utente deve disporre di un'autorità di certificazione (CA) Enterprise preconfigurata e di un controller di dominio.

### Requisiti di sistema

In questa sezione, per tutte le impostazioni viene utilizzato il sistema operativo Windows Server 2012 R2 e versioni successive. I seguenti requisiti e funzionalità di installazione si applicano sia al server CEP che al server CES, a meno che non sia specificato diversamente.



Creare i seguenti tipi di account nel controller di dominio:

- Amministratore del servizio: denominato **CEPAdmin** e **CESAdmin**
  - Questo utente deve far parte del **gruppo di amministrazione locale** nei rispettivi server CEP e CES.
  - Questo utente deve essere un membro del gruppo **Enterprise Admin**.
- Account di servizio: denominato **CEPSvc** e **CESSvc**
  - Questo utente deve far parte del gruppo **IIS\_IUSRS locale**.
  - Richiede l'autorizzazione **Richiedi certificati** nella CA per i rispettivi **CEPSvc** e **CESSvc**.

### Requisiti di connettività di rete

- I requisiti di connettività di rete sono una parte fondamentale della pianificazione della distribuzione, in particolare nei casi in cui i server CEP e CES siano ospitati in una rete perimetrale.
- La connettività di tutti i client a entrambi i servizi avviene all'interno di una sessione HTTPS, pertanto è consentito solo il traffico HTTPS tra il client e i servizi Web.
- Il server CEP comunica con Servizi di dominio Active Directory (AD DS), utilizzando le porte standard LDAP (Lightweight Directory Access Protocol) e LDAPS (Secure LDAP) (TCP 389 e 636 rispettivamente).
- Il server CES comunica con l'autorità di certificazione tramite DCOM (Distributed Component Object Model).



**Note:**

- Per impostazione predefinita, DCOM utilizza porte temporanee casuali.
- L'autorità di certificazione può essere configurata in modo da riservare un intervallo di porte specifico per semplificare la configurazione del firewall.

## Creazione di certificati SSL per i server CEP e CES

I server CES e CEP devono utilizzare il protocollo SSL (Secure Sockets Layer) per la comunicazione con i client (tramite HTTPS). Ogni servizio deve disporre di un certificato valido dotato di un criterio ECU (Enhanced Key Usage) per l'autenticazione del server nell'archivio certificati del computer locale.

- 1 Installare il servizio IIS nel server.
- 2 Accedere al server CEP, quindi aggiungere il Certificato CA radice nell'archivio Autorità di certificazione radice attendibile.
- 3 Avviare IIS Manager Console, quindi selezionare **Server Home**.
- 4 Nella sezione Visualizzazione principale, aprire **Certificati server**.
- 5 Fare clic su **Azioni > Crea richiesta certificato**.
- 6 Nella finestra Proprietà nome distinto, specificare le informazioni necessarie, quindi fare clic su **Avanti**.
- 7 Nella finestra Proprietà provider di servizi crittografici, selezionare la lunghezza in bit, quindi fare clic su **Avanti**.
- 8 Salvare il file.
- 9 Ottenere il file firmato dall'autorità di certificazione che si intende utilizzare per i server CEP e CES.  
**Nota:** Assicurarsi che ECU autenticazione server sia abilitato nel certificato firmato.
- 10 Copiare nuovamente il file firmato nel server CEP.
- 11 In IIS Manager Console, selezionare **Server Home**.
- 12 Nella sezione Visualizzazione principale, aprire **Certificati server**.
- 13 Fare clic su **Azioni > Completa richiesta certificato**.
- 14 Nella finestra Specifica risposta autorità di certificazione, selezionare il file firmato.
- 15 Digitare un nome, quindi nel menu Archivio certificati selezionare **Personale**.
- 16 Completare l'installazione del certificato.
- 17 In IIS Manager Console, selezionare il sito Web predefinito.
- 18 Fare clic su **Azioni > Associazioni**.
- 19 Nella finestra di dialogo Associazioni del sito, fare clic su **Aggiungi**.
- 20 Nella finestra di dialogo Aggiungi associazione del sito, impostare Tipo su **https**, quindi, dal certificato SSL, cercare il certificato appena creato.
- 21 In IIS Manager Console, selezionare **Sito Web predefinito**, quindi aprire le impostazioni SSL.
- 22 Abilitare Richiedi SSL e impostare Certificati client su **Ignora**.
- 23 Riavviare IIS.

**Nota:** Seguire la stessa procedura per il server CES.

## Creazione di modelli di certificato

L'utente deve creare un modello di certificato per la registrazione del certificato. Effettuare le seguenti operazioni per copiare da un modello di certificato esistente:

- 1 Accedere alla CA Enterprise con le credenziali di amministratore CA.
- 2 Espandere la CA, fare clic con il pulsante destro del mouse su **Modelli di certificato**, quindi scegliere **Gestisci**.
- 3 In Console dei modelli di certificato, fare clic con il pulsante destro del mouse su **Modello di certificato del server Web**, quindi fare clic su **Duplica modello**.
- 4 Nella scheda Generale del modello, assegnare un nome al modello **MVEWebServer**.
- 5 Nella scheda Protezione, concedere all'amministratore CA le autorizzazioni di **lettura, scrittura e registrazione**.
- 6 Assegnare le autorizzazioni di **lettura e registrazione** agli utenti autenticati.
- 7 Nella scheda Nome oggetto selezionare **Inserisci** nella richiesta.
- 8 Nella scheda Generale, impostare il periodo di validità del certificato.
- 9 Se si prevede di utilizzare questo modello di certificato per l'emissione di un **certificato 802.1X** per le stampanti, procedere come segue:
  - a Nella scheda **Estensioni**, selezionare **Criteri di applicazione** dall'elenco delle estensioni incluse in questo modello.
  - b Fare clic su **Modifica > Aggiungi**.
  - c Nella finestra di dialogo Aggiungi criterio applicazione, selezionare **Autenticazione client**.
  - d Fare clic su **OK**.
- 10 Nella finestra di dialogo Proprietà modello certificato, fare clic su **OK**.
- 11 Nella finestra CA, fare clic con il pulsante destro del mouse su **Modelli di certificato**, quindi fare clic su **Nuovo > modello di certificato**.
- 12 Selezionare **MVEWebServer**, quindi fare clic su **OK**.

## Informazioni sui metodi di autenticazione

I server CEP e CES supportano i seguenti metodi di autenticazione:

- Autenticazione integrata di Windows, nota anche come **autenticazione Kerberos**
- Autenticazione certificato client, nota anche come **autenticazione del certificato X.509**
- **Autenticazione tramite nome utente e password**

### Autenticazione integrata di Windows

L'autenticazione integrata di Windows utilizza Kerberos per fornire un flusso di autenticazione ininterrotto per i dispositivi connessi alla rete interna. Questo è il metodo preferito per le distribuzioni interne perché utilizza l'infrastruttura Kerberos esistente all'interno di AD DS. Richiede inoltre modifiche minime ai computer client dei certificati.

**Nota:** Utilizzare questo metodo di autenticazione se sono necessari client per accedere *solo* al servizio Web mentre si è connessi direttamente alla rete interna.

## Autenticazione certificato client

Questo è il metodo preferito rispetto all'autenticazione con nome utente e password perché è più sicuro. Non richiede una connessione diretta alla rete aziendale.

### Note:

- Utilizzare questo metodo di autenticazione se si intende fornire certificati X.509 digitali per l'autenticazione ai client.
- Questo metodo consente di abilitare i servizi Web disponibili su Internet.

## Autenticazione nome utente e password

Il metodo nome utente e password è la forma di autenticazione più semplice. Questo metodo viene in genere utilizzato per la manutenzione dei client che non direttamente connessi alla rete interna. Si tratta di un'opzione di autenticazione meno sicura rispetto all'autenticazione del certificato client, ma non richiede il provisioning di un certificato.

**Nota:** Utilizzare questo metodo di autenticazione quando è possibile accedere al servizio Web sulla rete interna o su Internet.

## Requisiti di delega

La delega consente a un servizio di impersonare l'account di un utente o un computer per accedere alle risorse in tutta la rete.

La delega è necessaria per il server CES in tutti i seguenti casi:

- CA e CES non risiedono nello stesso computer.
- Il server CES è in grado di elaborare le richieste di registrazione iniziale anziché elaborare solo le richieste di rinnovo del certificato.
- Il tipo di autenticazione è impostato su **Autenticazione integrata di Windows** o **Autenticazione certificato client**.

La delega non è necessaria per il server CES nei seguenti casi:

- CA e CES risiedono nello stesso computer.
- Il nome utente e la password sono il metodo di autenticazione.

### Note:

- Microsoft consiglia di eseguire CEP e CES come account utente di dominio.
- Gli utenti devono creare un nome principale servizio (SPN) appropriato prima di configurare la delega nell'account utente di dominio.

## Abilitazione della delega

**1** Per creare un SPN per un account utente di dominio, utilizzare il comando **setspn** come segue:

```
setspn -s http/ces.msca.com msca\CESSvc
```

**Note:**

- Il nome dell'account è CESSvc.
- Il server CES viene eseguito in un computer con un nome di dominio completo (FQDN) di **ces.msca.com** nel dominio msca.com.

**2** Aprire l'account utente di dominio CESSvc nel controller di dominio.

**3** Nella scheda Delega, selezionare **Utente attendibile per la delega solo ai servizi specificati**.

**4** Selezionare la delega appropriata in base al metodo di autenticazione.

**Note:**

- Se si seleziona l'autenticazione integrata di Windows, configurare la delega in modo da utilizzare **solo Kerberos**.
- Se il servizio utilizza l'autenticazione del certificato client, configurare la delega in modo da utilizzare qualsiasi protocollo di autenticazione.
- Se si prevede di configurare più metodi di autenticazione, configurare la delega in modo da utilizzare qualsiasi protocollo di autenticazione.

**5** Fare clic su **Aggiungi**.

**6** Nella finestra di dialogo Aggiungi servizi, selezionare **Utenti o Computer**.

**7** Digitare il nome host del server CA, quindi fare clic su **Controlla nomi**.

**8** Nella finestra di dialogo Aggiungi servizi, selezionare uno dei seguenti servizi da delegare:

- Servizio host (HOST) per il server CA specificato
- RPCSS (Remote procedure Call System Service) per il server CA specificato

**9** Chiudere la finestra di dialogo delle proprietà utente di dominio.

Per gli utenti del dominio CEP che utilizzano l'autenticazione integrata di Windows, procedere come segue:

**1** Per creare un SPN per un account utente di dominio, utilizzare il comando **setspn** come segue:

```
setspn -s http/cep.msca.com msca\CEPSvc
```

**Nota:** il nome dell'account è CESSvc.

**2** Aprire l'account utente di dominio CEPSvc nel controller di dominio.

**3** Nella scheda Delega, selezionare **Non considerare questo utente attendibile per la delega**.

## Configurazione dell'autenticazione integrata di Windows

Per installare CEP e CES, utilizzare Windows PowerShell.

### Configurazione di CEP

Il cmdlet **Install-AdcsEnrollmentPolicyWebService** configura il servizio Web dei criteri di registrazione certificato (CEP). Viene inoltre utilizzato per creare altre istanze del servizio all'interno di un'installazione esistente.

**1** Accedere al server CEP utilizzando il nome utente CEPAdmin, quindi avviare PowerShell in modalità amministrativa.

**2** Eseguire il comando **Import-Module ServerManager**.

- 3 Eseguire il comando **Add-WindowsFeature ADC-Enroll-Web-Pol**.
- 4 Eseguire il comando **Install-AdcsEnrollmentPolicyWebService -AuthenticationType Kerberos -SSLCertThumbprint "sslCertThumbPrint"**.  
**Nota:** Sostituire <sslCertThumbPrint> con l'identificazione personale del certificato SSL creato per il server CEP, dopo aver eliminato gli spazi tra i valori dell'identificazione personale.
- 5 Completare l'installazione selezionando **Y** o **A**.
- 6 Avviare IIS Manager Console.
- 7 Nel riquadro Connessioni, espandere il server Web che ospita il server CEP.
- 8 Espandere **Siti**, espandere **Sito Web predefinito**, quindi fare clic sul nome dell'applicazione virtuale di installazione appropriata, **ADPolicyProvider\_CEP\_Kerberos**.
- 9 Nell'applicazione virtuale denominata **Home**, fare doppio clic sulle impostazioni dell'applicazione, quindi fare doppio clic su **FriendlyName**.
- 10 Digitare un nome in Valore, quindi chiudere la finestra di dialogo.
- 11 Fare doppio clic su **URI**, quindi copiare il **Valore**.  
**Note:**
  - Se si desidera configurare un altro metodo di autenticazione nello stesso server CEP, è necessario modificare l'ID.
  - Questo URL viene utilizzato in MVE o in qualsiasi applicazione client.
- 12 Nel riquadro a sinistra, fare clic su **Pool di applicazioni**.
- 13 Selezionare **WSEnrollmentPolicyServer**, quindi, nel riquadro a destra, fare clic su **Azioni > Impostazioni avanzate**.
- 14 Selezionare il campo dell'identità in Modello processo.
- 15 Nella finestra di dialogo Identità pool di applicazioni, selezionare l'account personalizzato, quindi digitare **CEPSvc** come nome utente di dominio.
- 16 Chiudere tutte le finestre di dialogo, quindi riciclare IIS nel riquadro a destra di IIS Manager Console.
- 17 In PowerShell, digitare **iisreset** per riavviare IIS.

## Configurazione di CES

Il cmdlet **Install-AdcsEnrollmentWebService** configura il servizio Web di registrazione certificati (CES). Viene inoltre utilizzato per creare altre istanze del servizio all'interno di un'installazione esistente.

- 1 Accedere al server CES utilizzando **CESAdmin** come nome utente, quindi avviare PowerShell in modalità amministrativa.
- 2 Eseguire il comando **Import-Module ServerManager**.
- 3 Eseguire il comando **Add-WindowsFeature Adcs-Enroll-Web-Svc**.
- 4 Eseguire il comando **Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType Kerberos**.

**Note:**

- Sostituire `<sslCertThumbPrint>` con l'identificazione personale del certificato SSL creato per il server CES, dopo aver eliminato gli spazi tra i valori dell'identificazione personale.
- Sostituire **CA1.contoso.com** con il nome del computer CA.
- Sostituire **contoso-CA1-CA** con il nome comune CA.

- 5 Completare l'installazione selezionando **Y** o **A**.
- 6 Avviare IIS Manager Console.
- 7 Nel riquadro Connessioni, espandere il server Web che ospita il server CES.
- 8 Espandere **Siti**, espandere **Sito Web predefinito**, quindi fare clic sul nome dell'applicazione virtuale di installazione appropriata: **contoso-CA1-CA \_CES\_Kerberos**.
- 9 Nel riquadro a sinistra, fare clic su **Pool di applicazioni**.
- 10 Selezionare **WSEnrollmentServer**, quindi, nel riquadro a destra, fare clic su **Azioni > Impostazioni avanzate**.
- 11 Selezionare il campo dell'identità in Modello processo.
- 12 Nella finestra di dialogo **Identità pool di applicazioni**, selezionare l'account personalizzato, quindi digitare **CESSvc** come nome utente di dominio.
- 13 Chiudere tutte le finestre di dialogo, quindi riciclare IIS nel riquadro a destra di IIS Manager Console.
- 14 In PowerShell, digitare **iisreset** per riavviare IIS.
- 15 Per gli utenti del dominio CESSvc, abilitare la delega. Per ulteriori informazioni, vedere ["Abilitazione della delega" a pagina 91](#).

## Configurazione dell'autenticazione con certificato client

### Configurazione di CEP

Il cmdlet **Install-AdcsEnrollmentPolicyWebService** configura il server CEP. Viene inoltre utilizzato per creare altre istanze del servizio all'interno di un'installazione esistente.

- 1 Accedere al server CEP utilizzando il nome utente CEPAdmin, quindi avviare PowerShell in modalità amministrativa.
- 2 Eseguire il comando **Import-Module ServerManager**.
- 3 Eseguire il comando **Add-WindowsFeature ADC-Enroll-Web-Pol**.
- 4 Eseguire il comando **Install-AdcsEnrollmentPolicyWebService -AuthenticationType Certificate -SSLCertThumbprint "sslCertThumbPrint"**.

**Nota:** Sostituire `<sslCertThumbPrint>` con l'identificazione personale del certificato SSL creato per il server CEP, dopo aver eliminato gli spazi tra i valori dell'identificazione personale.

- 5 Completare l'installazione selezionando **Y** o **A**.
- 6 Avviare IIS Manager Console.
- 7 Nel riquadro Connessioni, espandere il server Web che ospita il server CEP.
- 8 Espandere **Siti**, espandere **Sito Web predefinito**, quindi fare clic sul nome dell'applicazione virtuale di installazione appropriata, **ADPolicyProvider\_CEP\_Certificate**.

- 9 Nell'applicazione virtuale denominata **Home**, fare doppio clic sulle impostazioni dell'applicazione, quindi fare doppio clic su **FriendlyName**.
- 10 Digitare un nome in Valore, quindi chiudere la finestra di dialogo.
- 11 Fare doppio clic su **URI**, quindi copiare il **Valore**.  
**Note:**
  - Se si desidera configurare un altro metodo di autenticazione nello stesso server CEP, è necessario modificare l'ID.
  - Questo URL viene utilizzato in MVE o in qualsiasi applicazione client.
- 12 Nel riquadro a sinistra, fare clic su **Pool di applicazioni**.
- 13 Selezionare **WSEnrollmentPolicyServer**, quindi, nel riquadro a destra, fare clic su **Azioni > Impostazioni avanzate**.
- 14 Selezionare il campo dell'identità in Modello processo.
- 15 Nella finestra di dialogo Identità pool di applicazioni, selezionare l'account personalizzato, quindi digitare **CEPSvc** come nome utente di dominio.
- 16 Chiudere tutte le finestre di dialogo, quindi riciclare IIS nel riquadro a destra di IIS Manager Console.
- 17 In PowerShell, digitare **iisreset** per riavviare IIS.

## Configurazione di CES

Il cmdlet **Install-AdcsEnrollmentWebService** configura il servizio Web di registrazione certificati (CES). Viene inoltre utilizzato per creare altre istanze del servizio all'interno di un'installazione esistente.

- 1 Accedere al server CES utilizzando **CESAdmin** come nome utente, quindi avviare PowerShell in modalità amministrativa.
- 2 Eseguire il comando **Import-Module ServerManager**.
- 3 Eseguire il comando **Add-WindowsFeature Adcs-Enroll-Web-Svc**.
- 4 Eseguire il comando **Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType Certificate**.

**Note:**

- Sostituire *<sslCertThumbPrint>* con l'identificazione personale del certificato SSL creato per il server CES, dopo aver eliminato gli spazi tra i valori dell'identificazione personale.
  - Sostituire **CA1.contoso.com** con il nome del computer CA.
  - Sostituire **contoso-CA1-CA** con il nome comune CA.
  - Se è già stato configurato un metodo di autenticazione nell'host, rimuovere **ApplicationPoolIdentity** dal comando.
- 5 Completare l'installazione selezionando **Y** o **A**.
  - 6 Avviare IIS Manager Console.
  - 7 Nel riquadro Connessioni, espandere il server Web che ospita il server CEP.

- 8 Espandere **Siti**, espandere **Sito Web predefinito**, quindi fare clic sul nome dell'applicazione virtuale di installazione appropriata: **contoso-CA1-CA\_CES\_Certificate**.
- 9 Nel riquadro a sinistra, fare clic su **Pool di applicazioni**.
- 10 Selezionare **WSEnrollmentServer**, quindi, nel riquadro a destra, fare clic su **Azioni > Impostazioni avanzate**.
- 11 Selezionare il campo dell'identità in Modello processo.
- 12 Nella finestra di dialogo Identità pool di applicazioni, selezionare l'account personalizzato, quindi digitare **CESSvc** come nome utente di dominio.
- 13 Chiudere tutte le finestre di dialogo, quindi riciclare IIS nel riquadro a destra di IIS Manager Console.
- 14 In PowerShell, digitare **iisreset** per riavviare IIS.
- 15 Per l'utente del dominio CESSvc, abilitare la delega. Per ulteriori informazioni, vedere ["Abilitazione della delega" a pagina 91](#).

## Creazione di un certificato client

- 1 Da qualsiasi account utente di dominio, aprire **certlm.msc**.
- 2 Fare clic su **Certificati > Personali > Certificati > Tutte le attività > Richiedi nuovo certificato**.
- 3 Fare clic su **Avanti**.
- 4 Fare clic su **Registrazione Active Directory > Accesso client**.  
**Nota:** se non si desidera utilizzare le opzioni **Registrazione Active Directory**, effettuare le seguenti operazioni:
  - a Fare clic su **Configurato da te > Aggiungi nuovo**.
  - b Immettere l'URI del server dei criteri di registrazione come indirizzo del server CEP per l'autenticazione Username\_Password o Kerberos.
  - c Selezionare il tipo di autenticazione come **Integrata di Windows**.
  - d Fare clic su **Convalida server**.
  - e Dopo aver eseguito correttamente la convalida, fare clic su **Aggiungi**.
  - f Fare clic su **Avanti**.
  - g Selezionare un modello qualsiasi.
- 5 Fare clic su **Dettagli > Proprietà**.
- 6 Fare clic su **Registra**.
- 7 Nella scheda Oggetto, fornire un nome di dominio completo (FQDN).
- 8 Nella scheda Chiave privata, selezionare **Consenti esportazione chiave privata**.
- 9 Fare clic su **Applica > Registra**.

Dopo aver registrato il certificato client, procedere come segue per esportarlo in formato PFX.

- 1 Fare clic su **Certificato > Tutte le attività > Esporta**.
- 2 Fare clic su **Avanti > Sì, esporta la chiave privata**.
- 3 Fare clic su **Avanti**.



- 4 Digitare la password fornita dal client.
- 5 Fare clic su **Avanti**.
- 6 Specificare il nome del file nella finestra di dialogo Esportazione certificati.
- 7 Fare clic su **Avanti** > **Fine**.

## Configurazione dell'autenticazione con nome utente-password

### Configurazione di CEP

Il cmdlet **Install-AdcsEnrollmentPolicyWebService** configura il servizio Web dei criteri di registrazione certificato (CEP). Viene inoltre utilizzato per creare altre istanze del servizio all'interno di un'installazione esistente.

- 1 Accedere al server CEP utilizzando il nome utente CEPAdmin, quindi avviare PowerShell in modalità amministrativa.
  - 2 Eseguire il comando **Import-Module ServerManager**.
  - 3 Eseguire il comando **Add-WindowsFeature ADC-Enroll-Web-Pol**.
  - 4 Eseguire il comando **Install-AdcsEnrollmentPolicyWebService -AuthenticationType UserName -SSLCertThumbprint "sslCertThumbPrint"**.
- Nota:** Sostituire `<sslCertThumbPrint>` con l'identificazione personale del certificato SSL creato per il server CEP, dopo aver eliminato gli spazi tra i valori dell'identificazione personale.
- 5 Completare l'installazione selezionando **Y** o **A**.
  - 6 Avviare IIS Manager Console.
  - 7 Nel riquadro Connessioni, espandere il server Web che ospita il server CEP.
  - 8 Espandere **Siti**, espandere **Sito Web predefinito**, quindi fare clic sul nome dell'applicazione virtuale di installazione appropriata: **ADPolicyProvider\_CEP\_UsernamePassword**.
  - 9 Nell'applicazione virtuale denominata **Home**, fare doppio clic sulle impostazioni dell'applicazione, quindi fare doppio clic su **FriendlyName**.
  - 10 Digitare un nome in **Valore**, quindi chiudere la finestra di dialogo.
  - 11 Fare doppio clic su **URI**, quindi copiare il **Valore**.

**Note:**

- Se si desidera configurare un altro metodo di autenticazione nello stesso server CEP, è necessario modificare l'ID.
- Questo URL viene utilizzato in MVE o in qualsiasi applicazione client.

- 12 Nel riquadro a sinistra, fare clic su **Pool di applicazioni**.
- 13 Selezionare **WSEnrollmentPolicyServer**, quindi, nel riquadro a destra, fare clic su **Azioni** > **Impostazioni avanzate**.
- 14 Selezionare il campo dell'identità in Modello processo.
- 15 Nella finestra di dialogo Identità pool di applicazioni, selezionare l'account personalizzato, quindi digitare **CEPSvc**.

- 16 Chiudere tutte le finestre di dialogo, quindi riciclare IIS nel riquadro a destra di IIS Manager Console.
- 17 In PowerShell, digitare **iisreset** per riavviare IIS.

## Configurazione di CES

Il cmdlet **Install-AdcsEnrollmentWebService** configura il servizio Web di registrazione certificati (CES). Viene inoltre utilizzato per creare altre istanze del servizio all'interno di un'installazione esistente.

- 1 Accedere al server CES utilizzando **CESAdmin** come nome utente, quindi avviare PowerShell in modalità amministrativa.
- 2 Eseguire il comando **Import-Module ServerManager**.
- 3 Eseguire il comando **Add-WindowsFeature Adcs-Enroll-Web-Svc**.
- 4 Eseguire il comando **Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType UserName**.

### Note:

- Sostituire *<sslCertThumbprint>* con l'identificazione personale del certificato SSL creato per il server CES, dopo aver eliminato gli spazi tra i valori dell'identificazione personale.
  - Sostituire **CA1.contoso.com** con il nome del computer CA.
  - Sostituire **contoso-CA1-CA** con il nome comune CA.
  - Se è già stato configurato un metodo di autenticazione nell'host, rimuovere **ApplicationPoolIdentity** dal comando.
- 5 Completare l'installazione selezionando **Y** o **A**.
  - 6 Avviare IIS Manager Console.
  - 7 Nel riquadro Connessioni, espandere il server Web che ospita il server CES.
  - 8 Espandere **Siti**, espandere **Sito Web predefinito**, quindi fare clic sul nome dell'applicazione virtuale di installazione appropriata: **contoso-CA1-CA\_CES\_UsernamePassword**.
  - 9 Nel riquadro a sinistra, fare clic su **Pool di applicazioni**.
  - 10 Selezionare **WSEnrollmentServer**, quindi, nel riquadro a destra, fare clic su **Azioni > Impostazioni avanzate** sotto Azioni.
  - 11 Selezionare il campo dell'identità in Modello processo.
  - 12 Nella finestra di dialogo Identità pool di applicazioni, selezionare l'account personalizzato, quindi digitare **CESSvc** come nome utente di dominio.
  - 13 Chiudere tutte le finestre di dialogo, quindi riciclare IIS nel riquadro a destra di IIS Manager Console.
  - 14 In PowerShell, digitare **iisreset** per riavviare IIS.

# Gestione dei certificati con l'autorità di certificazione OpenXPki tramite SCEP

Questa sezione fornisce istruzioni su come configurare OpenXPki CA versione 2.5.x mediante il protocollo SCEP (Simple Certificate Enrollment Protocol).

## Note:

- Assicurarsi di utilizzare il sistema operativo Debian 8 Jessie.
- Per ulteriori informazioni su OpenXPki, visitare il sito [www.openxpki.org](http://www.openxpki.org).

## Configurazione di OpenXPki CA

### Installazione di OpenXPki CA

- 1 Collegare il computer utilizzando PuTTY o un altro client.
- 2 Dal client, eseguire il comando **sudo su** - per passare all'utente root.
- 3 Immettere la password root.
- 4 In **nano /etc/apt/sources.list**, modificare l'origine per installare gli aggiornamenti.
- 5 Aggiornare il file. Ad esempio:

```
#  
  
# deb cdrom:[Debian GNU/Linux 8.11.1 _Jessie_ - Official amd64 CD Binary-1  
20190211-02:10]/ jessie local main  
# deb cdrom:[Debian GNU/Linux 8.11.1 _Jessie_ - Official amd64 CD Binary-1  
20190211-02:10]/ jessie local main  
  
deb http://security.debian.org/ jessie/updates main  
deb-src http://security.debian.org/ jessie/updates main  
  
# jessie-updates, previously known as 'volatile'  
# A network mirror was not selected during install. The following entries  
# are provided as examples, but you should amend them as appropriate  
# for your mirror of choice.  
#  
deb http://ftp.debian.org/debian/jessie-updates main  
deb-src http://ftp.debian.org/debian/jessie-updates main  
deb http://ftp.us.debian.org/debian/jessie main
```
- 6 Salvare il file.
- 7 Eseguire questi comandi:
  - **apt-get update**
  - **apt-get upgrade**
- 8 Aggiornare gli elenchi dei certificati CA nel server utilizzando **apt-get install ca-certificates**.
- 9 Installare le impostazioni locali **en\_US.utf8** utilizzando **dpkg-reconfigure locales**.
- 10 Selezionare le impostazioni locali **en\_US.UTF-8 UTF-8**, quindi impostarle come predefinite per il sistema.

**Nota:** utilizzare il tasto Tab e la barra spaziatrice per selezionare e navigare all'interno del menu.

- 11 Controllare le impostazioni locali generate utilizzando **locale -a**.

### Output di esempio

```
C
C.UTF-8
en_IN
en_IN.utf8
en_US.utf8
POSIX
```

- 12 Copiare l'impronta digitale del pacchetto OpenXPki utilizzando **nano /home/Release.key**. Per questo esempio, copiare la chiave in **/home**.
- 13 Digitare **9B156AD0 F0E6A6C7 86FABE7A D8363C4E 1611A2BE 2B251336 01D1CDB4 6C24BEF3** come valore.
- 14 Eseguire questo comando:
- ```
gpg --print-md sha256 /home/Release.key
```
- 15 Aggiungere il pacchetto utilizzando il comando **wget https://packages.openxpki.org/v2/debian/Release.key -O - | apt-key add -**.
- 16 Aggiungere il repository all'elenco di origini (jessie) utilizzando **echo "deb http://packages.openxpki.org/v2/debian/jessie release" > /etc/apt/sources.list.d/openxpki.list**, quindi **aptitude update**.
- 17 Installare l'associazione MySQL e Perl MySQL utilizzando **aptitude install mysql-server libdbd-mysql-perl**.
- 18 Installare apache2.2-common utilizzando **aptitude install apache2.2-common**.
- 19 In **nano /etc/apt/sources.list**, installare il modulo fastcgi per velocizzare l'interfaccia utente.
- Nota:** si consiglia di utilizzare **mod-fcgid**.
- 20 Aggiungere la riga **deb http://http.us.debian.org/debian/jessie main** nel file, quindi salvarlo.
- 21 Eseguire questi comandi:
- ```
apt-get update
aptitude install libapache2-mod-fcgid
```
- 22 Abilitare il modulo fastcgi utilizzando **a2enmod fcgid**.
- 23 Installare il pacchetto di base OpenXPki utilizzando **aptitude install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n**.
- 24 Riavviare il server Apache® utilizzando **service apache2 restart**.
- 25 Controllare se l'installazione è avvenuta correttamente utilizzando **openxpkiadm version**.
- Nota:** se l'installazione è riuscita, il sistema mostra la versione di OpenXPki installata. Ad esempio, **Version (core): 2.5.5**.
- 26 Creare il database vuoto, quindi assegnare l'utente del database utilizzando **mysql -u root -p**.

**Note:**

- Questo comando deve essere digitato nel client. In caso contrario, non è possibile immettere la password.

- Digitare la password per MySQL. Per questo esempio, **root** è l'utente MySQL.
- **openxpki** è l'utente su cui è installato OpenXPki.

```
CREATE DATABASE openxpki CHARSET utf8;
CREATE USER 'openxpki'@'localhost' IDENTIFIED BY 'openxpki';
GRANT ALL ON openxpki.* TO 'openxpki'@'localhost';
flush privileges;
```

Se il servizio MySQL non è in esecuzione, eseguire **/etc/init.d/mysql start** per avviarlo.

**27** Digitare **quit** per uscire da MySQL.

**28** Memorizzare le credenziali usate in **/etc/openxpki/config.d/system/database.yaml**.

### Contenuto del file di esempio

```
debug: 0
type: MySQL
name: openxpki
host: localhost
port: 3306
user: openxpki
passwd: openxpki
```

**Nota:** modificare **user** e **passwd** in modo che corrispondano al nome utente e alla password MySQL.

**29** Salvare il file.

**30** Per uno schema di database vuoto, eseguire **zcat /usr/share/doc/libopenxpki-perl/examples/schema-mysql.sql.gz | \mysql -u root --password --database openxpki** dal file di schema fornito.

**31** Immettere la password per il database.

### Configurazione di OpenXPki CA mediante lo script predefinito

**Nota:** lo script predefinito configura solo l'area di autenticazione predefinita, ovvero **ca-one**. CDP e CRL non sono configurati.

- 1** Decomprimere lo script di esempio per installare il certificato utilizzando **gunzip -k /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh.gz**.
- 2** Eseguire lo script utilizzando **bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh**.
- 3** Confermare le impostazioni utilizzando **openxpkiadm alias --realm ca-one**.

### Output di esempio

```
=== functional token ===
scep (scep):
Alias      : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

vault (datasafe):
Alias      : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40
```

```
ca-signer (certsign):
Alias       : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEhbtI9pE
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2018-01-29 20:44:40
```

```
=== root ca ===
current root ca:
Alias       : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore  : 2015-01-30 20:44:39
NotAfter   : 2020-01-30 20:44:39
```

```
upcoming root ca:
not set
```

**4** Controllare se l'installazione è avvenuta correttamente utilizzando **openxpkictl start**.

### Output di esempio

```
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

**5** Effettuare le seguenti operazioni per accedere al server OpenXPki:

- a** Nel browser Web, digitare **http://ipaddress/openxpki/**.
- b** Eseguire l'accesso come **Operatore**. La password predefinita è **openxpki**.

**Nota:** l'accesso Operatore dispone di due account operatore preconfigurati: **raop** e **raop2**.

**6** Creare una richiesta di certificato, quindi testarla.

## Configurazione manuale di OpenXPki CA

### Panoramica

**Nota:** prima di iniziare, assicurarsi di disporre di una conoscenza di base sulla creazione di certificati OpenSSL.

Per configurare manualmente OpenXPki CA, creare i seguenti certificati:

- 1** Certificato CA radice. Per ulteriori informazioni, vedere ["Creazione di un certificato CA radice" a pagina 104](#).
- 2** Certificato del firmatario CA, firmato dalla CA radice. Per ulteriori informazioni, vedere ["Creazione di un certificato del firmatario" a pagina 104](#).
- 3** Certificato del vault di dati, autofirmato. Per ulteriori informazioni, vedere ["Creazione di un certificato del vault" a pagina 105](#).
- 4** Certificato SCEP, firmato dal certificato del firmatario.

### Note:

- Quando si seleziona l'hash della firma, utilizzare SHA256 o SHA512.
- La modifica della dimensione della chiave pubblica è opzionale.

In questo esempio, utilizziamo la directory **/etc/certs/openxpki\_ca-one/** per la generazione dei certificati. Tuttavia, è possibile utilizzare qualsiasi directory.

## Creazione di un file di configurazione OpenSSL

1 Eseguire questo comando:

```
nano /etc/certs/openxpki_ca-one/openssl.conf
```

**Nota:** Se il server è raggiungibile tramite il nome di dominio completo (FQDN), utilizzare il DNS del server anziché il suo indirizzo IP.

### File di esempio

```
# x509_extensions          = v3_ca_extensions
# x509_extensions          = v3_issuing_extensions
# x509_extensions          = v3_datavault_extensions
# x509_extensions          = v3_scep_extensions
# x509_extensions          = v3_web_extensions
# x509_extensions          = v3_ca_reqexts # not for root self-signed, only for issuing
## x509_extensions         = v3_datavault_reqexts # not required self-signed
# x509_extensions          = v3_scep_reqexts
# x509_extensions          = v3_web_reqexts

[ req ]
default_bits              = 4096
distinguished_name        = req_distinguished_name

[ req_distinguished_name ]
domainComponent           = Domain Component
commonName                = Common Name

[ v3_ca_reqexts ]
subjectKeyIdentifier       = hash
keyUsage                  = digitalSignature, keyCertSign, cRLSign

[ v3_datavault_reqexts ]
subjectKeyIdentifier       = hash
keyUsage                  = keyEncipherment
extendedKeyUsage           = emailProtection

[ v3_scep_reqexts ]
subjectKeyIdentifier       = hash

[ v3_web_reqexts ]
subjectKeyIdentifier       = hash
keyUsage                  = critical, digitalSignature, keyEncipherment
extendedKeyUsage           = serverAuth, clientAuth

[ v3_ca_extensions ]
subjectKeyIdentifier       = hash
keyUsage                  = digitalSignature, keyCertSign, cRLSign
basicConstraints           = critical,CA:TRUE
authorityKeyIdentifier     = keyid:always,issuer

[ v3_issuing_extensions ]
subjectKeyIdentifier       = hash
keyUsage                  = digitalSignature, keyCertSign, cRLSign
basicConstraints           = critical,CA:TRUE
authorityKeyIdentifier     = keyid:always,issuer:always
crlDistributionPoints       = URI:http://FQDN of the server/CertEnroll/MYOPENXPKI.crl
authorityInfoAccess        = caIssuers;URI:http://FQDN of the server/CertEnroll/MYOPENXPKI.crt

[ v3_datavault_extensions ]
subjectKeyIdentifier       = hash
keyUsage                  = keyEncipherment
extendedKeyUsage           = emailProtection
basicConstraints           = CA:FALSE
authorityKeyIdentifier     = keyid:always,issuer

[ v3_scep_extensions ]
subjectKeyIdentifier       = hash
basicConstraints           = CA:FALSE
authorityKeyIdentifier     = keyid,issuer
```

```
[ v3_web_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = critical, digitalSignature, keyEncipherment
extendedKeyUsage        = serverAuth, clientAuth
basicConstraints        = critical, CA:FALSE
subjectAltName          = DNS:stloopenxpki.lexmark.com
crlDistributionPoints   = URI:http://FQDN of the server/CertEnroll/MYOPENXPKI_ISSUINGCA.crl
authorityInfoAccess     = caIssuers;URI:http://FQDN of the
server/CertEnroll/MYOPENXPKI_ISSUINGCA.crt
```

- 2 Modificare l'indirizzo IP e il nome del certificato CA in base alle informazioni delle proprie impostazioni.
- 3 Salvare il file.

## Creazione di un file di password per le chiavi dei certificati

- 1 Eseguire questo comando:  

```
nano /etc/certs/openxpki_ca-one/pd.pass
```
- 2 Digitare la propria password.
- 3 Salvare il file.

## Creazione di un certificato CA radice

**Nota:** è possibile creare un-certificato CA radice autofirmato o generare una richiesta di certificato e quindi ottenerne la firma dalla CA radice.

Eseguire questi comandi:

**Nota:** sostituire la lunghezza della chiave, l'algoritmo di firma e il nome del certificato con i valori appropriati.

- 1 **openssl genrsa -out /etc/certs/openxpki\_ca-one/ca-root-1.key -passout file:/etc/certs/openxpki\_ca-one/pd.pass 4096**
- 2 **openssl req -new -key /etc/certs/openxpki\_ca-one/ca-root-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI\_ROOTCA -out /etc/certs/openxpki\_ca-one/ca-root-1.csr**
- 3 **openssl req -config /etc/certs/openxpki\_ca-one/openssl.conf -extensions v3\_ca\_extensions -x509 -days 3560 -in /etc/certs/openxpki\_ca-one/ca-root-1.csr -key /etc/certs/openxpki\_ca-one/ca-root-1.key -out /etc/certs/openxpki\_ca-one/ca-root-1.crt -sha256**

## Creazione di un certificato del firmatario

**Nota:** sostituire la lunghezza della chiave, l'algoritmo di firma e il nome del certificato con i valori appropriati.

- 1 Eseguire questo comando:  

```
openssl genrsa -out /etc/certs/openxpki_ca-one/ca-signer-1.key -passout file:/etc/certs/openxpki_ca-one/pd.pass 4096
```
- 2 Modificare l'oggetto della richiesta con le informazioni della propria CA utilizzando **openssl req -config /etc/certs/openxpki\_ca-one/openssl.conf -reqexts v3\_ca\_reqexts -new -key /etc/certs/openxpki\_ca-one/ca-signer-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI\_ISSUINGCA -out /etc/certs/openxpki\_ca-one/ca-signer-1.csr.**



- 3 Ottenere il certificato firmato dalla CA radice utilizzando `openssl x509 -req -extfile /etc/certs/openxpki_ca-one/openssl.conf -extensions v3_issuing_extensions -days 3650 -in /etc/certs/openxpki_ca-one/ca-signer-1.csr -CA /etc/certs/openxpki_ca-one/ca-root-1.crt -CAkey /etc/certs/openxpki_ca-one/ca-root-1.key -CAcreateserial -out /etc/certs/openxpki_ca-one/ca-signer-1.crt -sha256`.

## Creazione di un certificato del vault

### Note:

- Il certificato del vault è autofirmato.
- Sostituire la lunghezza della chiave, l'algoritmo di firma e il nome del certificato con i valori appropriati.

- 1 Eseguire questo comando:

```
openssl genrsa -out /etc/certs/openxpki_ca-one/vault-1.key -passout  
file:/etc/certs/openxpki_ca-one/pd.pass 4096
```

- 2 Modificare l'oggetto della richiesta con le informazioni della propria CA utilizzando `openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_datavault_reqexts -new -key /etc/certs/openxpki_ca-one/vault-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/DC=STLOPENXPKI_INTERNAL/CN=MYOPENXPKI_DATAVAULT -out /etc/certs/openxpki_ca-one/vault-1.csr`.

- 3 Eseguire questo comando:

```
openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -extensions  
v3_datavault_extensions -x509 -days 3560 -in /etc/certs/openxpki_ca-  
one/vault-1.csr -key /etc/certs/openxpki_ca-one/vault-1.key -  
out /etc/certs/openxpki_ca-one/vault-1.crt
```

## Creazione di un certificato SCEP

**Nota:** il certificato SCEP è firmato dal certificato del firmatario.

Eseguire questi comandi:

**Nota:** sostituire la lunghezza della chiave, l'algoritmo di firma e il nome del certificato con i valori appropriati.

- 1 `openssl genrsa -out /etc/certs/openxpki_ca-one/scep-1.key -passout file:/etc/certs/openxpki_ca-one/pd.pass 4096`
- 2 `openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_scep_reqexts -new -key /etc/certs/openxpki_ca-one/scep-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_SCEPCA -out /etc/certs/openxpki_ca-one/scep-1.csr`
- 3 `openssl x509 -req -extfile /etc/certs/openxpki_ca-one/openssl.conf -extensions v3_scep_extensions -days 900 -in /etc/certs/openxpki_ca-one/scep-1.csr -CA /etc/certs/openxpki_ca-one/ca-signer-1.crt -CAkey /etc/certs/openxpki_ca-one/ca-signer-1.key -CAcreateserial -out /etc/certs/openxpki_ca-one/scep-1.crt -sha256`

## Copia del file di chiave e creazione di un collegamento simbolico

### 1 Copiare i file di chiave in `/etc/openxpki/ca/ca-one`.

**Nota:** i file di chiave devono essere leggibili da OpenXPki.

```
cp /etc/certs/openxpki_ca-one/ca-signer-1.key /etc/openxpki/ca/ca-one/
cp /etc/certs/openxpki_ca-one/vault-1.key /etc/openxpki/ca/ca-one/
cp /etc/certs/openxpki_ca-one/scep-1.key /etc/openxpki/ca/ca-one/
```

### 2 Creare il collegamento simbolico.

**Nota:** i collegamenti simbolici sono alias utilizzati dalla configurazione predefinita.

```
ln -s /etc/openxpki/ca/ca-one/ca-signer-1.key /etc/openxpki/ca/ca-one/ca-signer-1.pem
ln -s /etc/openxpki/ca/ca-one/scep-1.key /etc/openxpki/ca/ca-one/scep-1.pem
ln -s /etc/openxpki/ca/ca-one/vault-1.key /etc/openxpki/ca/ca-one/vault-1.pem
```

## Importazione dei certificati

Importare il certificato radice, il certificato del firmatario, il certificato del vault e il certificato SCEP nel database con i token appropriati.

Eseguire questi comandi:

- 1 **openxpkiadm certificate import --file /etc/certs/openxpki\_ca-one/ca-root-1.crt**
- 2 **openxpkiadm certificate import --file /etc/certs/openxpki\_ca-one/ca-signer-1.crt --realm ca-one --token certsign**
- 3 **openxpkiadm certificate import --file /etc/certs/openxpki\_ca-one/scep-1.crt --realm ca-one --token scep**
- 4 **openxpkiadm certificate import --file /etc/certs/openxpki\_ca-one/vault-1.crt --realm ca-one --token datasafe**
- 5 Controllare se l'importazione è avvenuta correttamente utilizzando **openxpkiadm alias --realm ca-one**.

## Output di esempio

```
=== functional token ===
scep (scep):
Alias      : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

vault (datasafe):
Alias      : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

ca-signer (certsign):
Alias      : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEdhbtI9pE
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2018-01-29 20:44:40

=== root ca ===
```

```
current root ca:
Alias      : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore  : 2015-01-30 20:44:39
NotAfter   : 2020-01-30 20:44:39

upcoming root ca:
not set
```

## Avvio di OpenXPki

- 1 Eseguire il comando **openxpkictl start**.

### Output di esempio

```
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

- 2 Effettuare le seguenti operazioni per accedere al server OpenXPki:

- a Nel browser Web, digitare **http://ipaddress/openxpki/**.

**Nota:** Invece di **ipaddress**, è possibile utilizzare anche il nome di dominio completo (FQDN) del server.

- b Eseguire l'accesso come **Operatore**. La password predefinita è **openxpki**.

**Nota:** l'accesso Operatore dispone di due account operatore preconfigurati: **raop** e **raop2**.

- 3 Creare una richiesta di certificato, quindi testarla.

## Generazione delle informazioni del CRL

**Nota:** se il server è raggiungibile tramite il nome di dominio completo (FQDN), utilizzare il DNS del server anziché il suo indirizzo IP.

- 1 Arrestare il servizio OpenXPki utilizzando **Openxpkictl stop**.
- 2 In **nano /etc/openxpki/config.d/realm/ca-one/publishing.yaml**, aggiornare la sezione **connectors: cdp** come segue:

```
class: Connector::Builtin::File::Path
LOCATION: /var/www/openxpki/CertEnroll/
file: "[% ARGS.0 %].crl"
content: "[% pem %]"
```

- a In **nano /etc/openxpki/config.d/realm/ca-one/profile/default.yaml**, aggiornare quanto segue:

- **Sezione `crl_distribution_points`:** sezione

```
critical: 0
uri:
  - http://FQDN of the server/CertEnroll/[% ISSUER.CN.0 %].crl
  - ldap://localhost/[% ISSUER.DN %]
```

- **Sezione `authority_info_access`:** sezione

```
critical: 0
ca_issuers: http://FQDN of the server/CertEnroll/MYOPENXPki.crt
ocsp: http://ocsp.openxpki.org/
```

Modificare l'indirizzo IP e il nome del certificato CA in base al proprio server CA.

**b** In **nano /etc/openxpki/config.d/realm/ca-one/crl/default.yaml**, effettuare le seguenti operazioni:

- Se necessario, aggiornare **nextupdate** e **renewal**.
- Aggiungere **ca\_issuers** alla seguente sezione:

```
extensions:
  authority_info_access:
    critical: 0
    # ca_issuers and ocsp can be scalar or list
    ca_issuers: http://FQDN of the server/CertEnroll/MYOPENXPKI.crt
    #ocsp: http://ocsp.openxpki.org/
```

Modificare l'indirizzo IP e il nome del certificato CA in base al proprio server CA.

**3** Avviare il servizio OpenXPki utilizzando **Openxpkictl start**.

## Configurazione dell'accessibilità al CRL

**1** Arrestare il servizio Apache utilizzando **service apache2 stop**.

**2** Creare una directory **CertEnroll** per **crl** nella directory **/var/www/openxpki/**.

**3** Impostare **openxpki** come proprietario di questa directory, quindi configurare le autorizzazioni per consentire ad Apache la lettura e l'esecuzione e agli altri servizi la sola lettura.

```
chown openxpki /var/www/openxpki/CertEnroll
```

```
chmod 755 /var/www/openxpki/CertEnroll
```

**4** Aggiungere un riferimento al file Apache **alias.conf** utilizzando **nano /etc/apache2/mods-enabled/alias.conf**.

**5** Dopo la sezione **<Directory "/usr/share/apache2/icons">**, aggiungere quanto segue:

```
Alias /CertEnroll/ "/var/www/openxpki/CertEnroll/"
<Directory "/var/www/openxpki/CertEnroll">
  Options FollowSymlinks
  AllowOverride None
  Require all granted
</Directory>
```

**6** Aggiungere un riferimento nel file **apache2.conf** utilizzando **nano /etc/apache2/apache2.conf**.

**7** Aggiungere quanto segue nella sezione **Apache2 HTTPD server**:

```
<Directory /var/www/openxpki/CertEnroll>
  Options FollowSymlinks
  AllowOverride None
  Allow from all
</Directory>
```

**8** Avviare il servizio Apache utilizzando **service apache2 start**.

## Abilitazione del servizio SCEP

**1** Arrestare il servizio OpenXPki utilizzando **openxpkictl stop**.

**2** Installare il pacchetto **openca-tools** utilizzando **aptitude install openca-tools**.

**3** Avviare il servizio OpenXPki utilizzando **openxpkictl start**.

Testare il servizio utilizzando un qualsiasi client, ad esempio **certnanny** con **SSCEP**.

**Nota:** SSCEP è un client della riga di comando per SCEP. È possibile scaricare SSCEP da <https://github.com/cernanny/sscep>.

## Abilitazione del certificato del "firmatario per conto di" (agente di registrazione)

Per le richieste automatiche di certificati, stiamo utilizzando la funzione del "firmatario per conto di" di OpenXPki.

- 1 Arrestare il servizio OpenXPki utilizzando **openxpkictl stop**.
- 2 In **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml**, nella sezione **authorized\_signer:**, aggiungere una regola per il nome dell'oggetto del certificato del firmatario.

```
rule1:
    # Full DN
    subject: CN=Markvision_.*
```

### Note:

- In questa regola, qualsiasi CN di certificato che inizia con **Markvision\_** è il certificato del "firmatario per conto di".
- Il nome dell'oggetto è impostato in MVE per generare il certificato del "firmatario per conto di".
- Esaminare lo spazio e il rientro nel file script.
- Se il CN viene modificato in MVE, aggiungere il CN aggiornato in OpenXPki.
- È possibile specificare un solo certificato del "firmatario per conto di", quindi specificare il CN completo.

- 3 Salvare il file.

- 4 Avviare il servizio OpenXPki utilizzando **openxpkictl start**.

## Abilitazione dell'approvazione automatica delle richieste di certificato in OpenXPki CA

- 1 Arrestare il servizio OpenXPki utilizzando **openxpkictl stop**.
- 2 In **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml**, aggiornare la sezione **eligible:** come segue:

### Precedente contenuto

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
    args: "[% context.cert_subject_parts.CN.0 %]"
    expect:
      - Build
      - New
```

### Nuovo contenuto

```
eligible:
  initial:
    value: 1
    # value@: connector:scep.generic.connector.initial
    # args: "[% context.cert_subject_parts.CN.0 %]"
```

```
# expect:
#   - Build
#   - New
```

**Note:**

- Esaminare lo spazio e il rientro nel file script.
- Per approvare manualmente i certificati, inserire un commento per **value: 1**, quindi rimuovere il commento dalle altre righe in cui era stato in precedenza inserito.

**3** Salvare il file.

**4** Avviare il servizio OpenXPKI utilizzando **openxpkictl start**.

## Creazione di una seconda area di autenticazione

In OpenXPKI è possibile configurare più strutture PKI sullo stesso sistema. I seguenti argomenti illustrano come creare un'altra area di autenticazione per MVE denominata **ca-two**.

### Copia e impostazione della directory

**1** Copiare la struttura di directory di esempio **/etc/openxpki/config.d/realm/ca-one** in una nuova directory (**cp -avr /etc/openxpki/config.d/realm/ca-one /etc/openxpki/config.d/realm/ca-two**) all'interno della directory dell'area di autenticazione.

**2** In **/etc/openxpki/config.d/system/realms.yaml**, aggiornare la seguente sezione:

#### Precedente contenuto

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

ca-one:
  label: Verbose name of this realm
  baseurl: https://pki.example.com/openxpki/

#ca-two:
#   label: Verbose name of this realm
#   baseurl: https://pki.acme.org/openxpki/
```

#### Nuovo contenuto

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

ca-one:
  label: CA-ONE
  baseurl: https://pki.example.com/openxpki/

ca-two:
  label: CA-TWO
  baseurl: https://pki.example.com/openxpki/
```

**3** Salvare il file.

## Creazione dei certificati

Le seguenti istruzioni mostrano come generare il certificato del firmatario, il certificato del vault e il certificato SCEP. La CA radice firma il certificato del firmatario, quindi il certificato del firmatario firma il certificato SCEP. Il certificato del vault è autofirmato.

- 1 Generare e quindi firmare i certificati. Per ulteriori informazioni, vedere ["Configurazione manuale di OpenXPki CA" a pagina 102](#).

**Nota:** modificare il nome comune del certificato in modo che l'utente possa distinguere facilmente tra i diversi certificati per le diverse aree di autenticazione. Si può modificare **DC=CA-ONE** in **DC=CA-TWO**. I file di certificato vengono creati nella **/etc/certs/openxpki\_ca-two/**.

- 2 Copiare i file di chiave in **/etc/openxpki/ca/ca-two/**.

**Nota:** i file di chiave devono essere leggibili da OpenXPki.

```
cp /etc/certs/openxpki_ca-two/ca-signer-1.key /etc/openxpki/ca/ca-two/
```

```
cp /etc/certs/openxpki_ca-two/vault-1.key /etc/openxpki/ca/ca-two/
```

```
cp /etc/certs/openxpki_ca-two/scep-1.key /etc/openxpki/ca/ca-two/
```

- 3 Creare il collegamento simbolico. Creare anche un collegamento simbolico per il certificato CA radice.

**Nota:** i collegamenti simbolici sono alias utilizzati dalla configurazione predefinita.

```
ln -s /etc/openxpki/ca/ca-one/ca-root-1.crt /etc/openxpki/ca/ca-two/ca-root-1.crt
```

```
ln -s /etc/openxpki/ca/ca-two/ca-signer-1.key /etc/openxpki/ca/ca-two/ca-signer-1.pem
```

```
ln -s /etc/openxpki/ca/ca-two/scep-1.key /etc/openxpki/ca/ca-two/scep-1.pem
```

```
ln -s /etc/openxpki/ca/ca-two/vault-1.key /etc/openxpki/ca/ca-two/vault-1.pem
```

- 4 Importare il certificato del firmatario, il certificato del vault e il certificato SCEP nel database con i token appropriati per **ca-two**.

```
openxpkiadm certificate import --file /etc/certs/openxpki_ca-two/ca-signer-1.crt --realm ca-two --issuer /etc/openxpki/ca/ca-two/ca-one-1.crt --token certsign
```

```
openxpkiadm certificate import --file /etc/certs/openxpki_ca-two/scep-1.crt --realm ca-two --token scep
```

```
openxpkiadm certificate import --file /etc/certs/openxpki_ca-two/vault-1.crt --realm ca-two --token datasafe
```

- 5 Controllare se l'importazione è avvenuta correttamente utilizzando **openxpkiadm alias --realm ca-two**.

## Output di esempio

```
=== functional token ===
scep (scep):
Alias      : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

vault (datasafe):
Alias      : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

ca-signer (certsign):
Alias      : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEhbtI9pE
```

```
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias      : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore : 2015-01-30 20:44:39
NotAfter  : 2020-01-30 20:44:39

upcoming root ca:
not set
```

In questo caso, le informazioni relative alla CA radice sono le stesse per **ca-one** e **ca-two**.

- 6 Se la password della chiave del certificato è stata modificata durante la creazione del certificato, aggiornare **nano /etc/openxpki/config.d/realm/ca-two/crypto.yaml**.
- 7 Generare i CRL per questa area di autenticazione. Per ulteriori informazioni, vedere ["Generazione delle informazioni del CRL" a pagina 107](#).
- 8 Pubblicare i CRL per questa area di autenticazione. Per ulteriori informazioni, vedere ["Configurazione dell'accessibilità al CRL" a pagina 108](#).
- 9 Riavviare il servizio OpenXPki utilizzando **openxpkictl restart**.

### Output di esempio

```
Stopping OpenXPki
Stopping gracefully, 3 (sub)processes remaining...
DONE.
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

- 10 Effettuare le seguenti operazioni per accedere al server OpenXPki:

- a Nel browser Web, digitare **http://ipaddress/openxpki/**.
- b Eseguire l'accesso come **Operatore**. La password predefinita è **openxpki**.

**Nota:** l'accesso Operatore dispone di due account operatore preconfigurati: **raop** e **raop2**.

### Configurazione dell'endpoint SCEP per più aree di autenticazione

L'endpoint SCEP dell'area di autenticazione predefinita è **http://<ipaddress>/scep/scep**. Se si dispone di più aree di autenticazione, configurare un endpoint SCEP univoco (file di configurazione diverso) per ogni area di autenticazione. Nelle seguenti istruzioni, utilizziamo due aree di autenticazione PKI, ovvero **ca-one** e **ca-two**.

- 1 Copiare il file di configurazione predefinito in **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-one.conf**.

**Nota:** assegnare al file il nome **ca-one.conf**.

- 2 In **nano /etc/openxpki/scep/ca-one.conf**, modificare il valore dell'area di autenticazione in **realm=ca-one**.
- 3 Creare un altro file di configurazione in **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-two.conf**.

**Nota:** assegnare al file il nome **ca-two.conf**.

- 4 In **nano /etc/openxpki/scep/ca-two.conf**, modificare il valore dell'area di autenticazione in **realm=ca-two**.
- 5 Riavviare il servizio OpenXPki utilizzando **openxpkictl restart**.



Gli endpoint SCEP sono i seguenti:

- **ca-one:** `http://ipaddress/scep/ca-one`
- **ca-two:** `http://ipaddress/scep/ca-two`

Se si desidera differenziare tra le credenziali di accesso e i modelli di certificato predefiniti per aree di autenticazione PKI diverse, potrebbe essere necessaria una configurazione avanzata.

## Abilitazione della presenza contemporanea di più certificati attivi

Per impostazione predefinita, in OpenXPki può essere attivo un solo certificato con lo stesso nome oggetto alla volta. Tuttavia, quando si applicano più certificati con nome, devono essere presenti più certificati attivi con lo stesso nome oggetto alla volta.

- 1 In `etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml`, nella sezione **policy**, modificare il valore di **max\_active\_certs** da 1 a 0.

**Note:**

- REAL NAME è il nome dell'area di autenticazione. Ad esempio, **ca-one**.
- Esaminare lo spazio e il rientro nel file script.

- 2 Riavviare il servizio OpenXPki utilizzando `openxpkictl restart`.

## Impostazione del numero di porta predefinito per OpenXPki CA

Per impostazione predefinita, Apache è in ascolto sulla porta numero 80. Impostare il numero di porta predefinito per OpenXPki CA per evitare conflitti.

- 1 In `/etc/apache2/ports.conf`, aggiungere o modificare una porta. Ad esempio, **Listen 8080**.
- 2 In `/etc/apache2/sites-enabled/000-default.conf`, aggiungere o modificare la sezione **VirtualHost** per associare la nuova porta. Ad esempio, **<VirtualHost \*:8080>**.
- 3 Riavviare il server Apache utilizzando `systemctl restart apache2`.

Per verificare lo stato, eseguire `netstat -tlnp | grep apache`. L'URL SCEP di OpenXPki è ora `http://ipaddress:8080/scep/ca-one`, mentre l'URL Web è `http://ip address:8080/openxpki`.

## Rifiuto delle richieste di certificati senza password di verifica in OpenXPki CA

Per impostazione predefinita, OpenXPki accetta le richieste senza controllare la password di verifica. La richiesta di certificato non viene rifiutata e la CA e l'amministratore CA stabiliscono se approvare o rifiutare la richiesta. Per evitare potenziali problemi di sicurezza, disabilitare questa funzione in modo che tutte le richieste di certificato che contengono password non valide vengano rifiutate immediatamente. In MVE, la Password di verifica è obbligatoria solo quando viene generato il certificato agente di registrazione.

- 1 In `etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml`, nella sezione **policy**, modificare il valore di **allow\_man\_authn** da 1 a 0.

**Note:**

- REAL NAME è il nome dell'area di autenticazione. Ad esempio, **ca-one**.

- Esaminare lo spazio e il rientro nel file script.

**2** Riavviare il servizio OpenXPki utilizzando **openxpkictl restart**.

## Aggiunta dell'EKU di autenticazione client nei certificati

**1** In **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N\_OPENXPki\_PROFILE\_TLS\_SERVER.yaml**, nella sezione **extended\_key\_usage:**, modificare il valore di **client\_auth:** in **1**.

**Note:**

- REAL NAME è il nome dell'area di autenticazione. Ad esempio, **ca-one**.
- Esaminare lo spazio e il rientro nel file script.

**2** Riavviare il servizio OpenXPki utilizzando **openxpkictl restart**.

## Recupero dell'oggetto del certificato completo quando si effettua la richiesta tramite SCEP

Per impostazione predefinita, OpenXPki legge solo il nome comune CN dell'oggetto del certificato richiesto. Il resto delle informazioni, quali il paese, la località e dominio DC, è hardcoded. Ad esempio, se l'oggetto di un certificato è **C=US, ST=KY, L=Lexington, O=Lexmark, OU=ISS,**

**CN=ET0021B7C34AEC.dhcp.dev.lexmark.com**, dopo la firma del certificato tramite SCEP, l'oggetto viene modificato in **DC=Test Deployment, DC= OpenXPki, CN=ET0021B7C34AEC.dhcp.dev.lexmark.com**.

**Nota:** REAL NAME è il nome dell'area di autenticazione. Ad esempio, **ca-one**.

**1** In **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N\_OPENXPki\_PROFILE\_TLS\_SERVER.yaml**, nella sezione **enroll**, modificare il valore di **dn** come segue:

```
CN=[% CN.0 %][% IF OU %][% FOREACH entry = OU %],OU=[% entry %][% END %][% END %][% IF O
%][% FOREACH entry = O %],O=[% entry %][% END %][% END %][% IF L %],L=[% L.0 %][% END %]
[% IF ST %],ST=[% ST.0 %][% END %][% IF C %],C=[% C.0 %][% END %][% IF DC %][% FOREACH
entry = DC %],DC=[% entry %][% END %][% END %][% IF EMAIL %][% FOREACH entry = EMAIL
%],EMAIL=[% entry %][% END %][% END %]
```

**2** Salvare il file.

**3** Creare un file denominato **l.yaml** nella directory **/etc/openxpki/config.d/realm/REALM NAME/profile/template**.

**4** Aggiungere quanto segue:

```
id: L
label: L
description: I18N_OPENXPki_UI_PROFILE_L_DESC
preset: L
type: freetext
width: 60
placeholder: Kolkata
```

**5** Salvare il file.

**6** Creare un file denominato **st.yaml** nella directory **/etc/openxpki/config.d/realm/REALM NAME/profile/template**.

**7** Aggiungere quanto segue:

```
id: ST
label: ST
description: I18N_OPENXPki_UI_PROFILE_ST_DESC
```

```
preset: ST
type: freetext
width: 60
placeholder: WB
```

**8** Salvare il file.

**Nota:** OpenXPki deve contenere entrambi i file e deve essere leggibile, scrivibile e eseguibile.

**9** Riavviare il servizio OpenXPki utilizzando **openxpkictl restart**.

## Revoca dei certificati e pubblicazione del CRL

**1** Accedere al server OpenXPki.

**a** Nel browser Web, digitare **http://ipaddress/openxpki/**.

**b** Eseguire l'accesso come **Operatore**. La password predefinita è **openxpki**.

**Nota:** l'accesso Operatore dispone di due account operatore preconfigurati: **raop** e **raop2**.

**2** Fare clic su **Cerca flusso di lavoro > Cerca ora**.

**3** Fare clic su un certificato da revocare, quindi sul collegamento del certificato.

**4** Nella sezione Azione fare clic su **richiesta di revoca**.

**5** Digitare i valori appropriati, quindi fare clic su **Continua > Invia richiesta**.

**6** Nella pagina successiva approvare la richiesta. La revoca del certificato è in attesa della successiva pubblicazione del CRL.

**7** Nella sezione Funzionamento PKI fare clic su **Emettere un elenco di revoche di certificati (CRL)**.

**8** Fare clic su **Applica creazione di elenchi di revoche > Continua**.

**9** Nella sezione Funzionamento PKI fare clic su **Pubblica CA/CRL**.

**10** Fare clic su **Cerca flusso di lavoro > Cerca ora**.

**11** Fare clic sul certificato revocato con un tipo **certificate\_revocation\_request\_v2**.

**12** Fare clic su **Applica riattivazione**.

Nel nuovo CRL è possibile trovare il numero di serie e il motivo di revoca del certificato revocato.

# Gestione dei certificati con l'autorità di certificazione OpenXPki tramite EST

Questa sezione aiuta l'utente a configurare la OpenXPki CA versione 3.x.x tramite il protocollo EST.

## Note:

- Assicurarsi di utilizzare il sistema operativo Debian 10 Buster.
- Per ulteriori informazioni su OpenXPki, visitare il sito [www.openxpki.org](http://www.openxpki.org).

## Configurazione di OpenXPki CA

### Installazione di OpenXPki CA

- 1 Collegare il computer utilizzando PuTTY o un altro client.
- 2 Dal client, eseguire il comando **sudo su** - per passare all'utente root.
- 3 Immettere la password root.
- 4 In **nano /etc/apt/sources.list**, modificare l'origine per installare gli aggiornamenti.
- 5 Aggiornare il file. Ad esempio:

```
#  
  
# deb cdrom:[Debian GNU/Linux testing _Buster_ - Official Snapshot amd64 DVD Binary-1  
20190527-04:04]/ buster contrib main  
# deb cdrom:[Debian GNU/Linux testing _Buster_ - Official Snapshot amd64 DVD Binary-1  
20190527-04:04]/ buster contrib main  
  
deb http://security.debian.org/debian-security buster/updates main contrib  
deb-src http://security.debian.org/debian-security buster/updates main contrib  
  
# buster-updates, previously known as 'volatile'  
# A network mirror was not selected during install. The following entries  
# are provided as examples, but you should amend them as appropriate  
# for your mirror of choice.  
#  
deb http://ftp.debian.org/debian/ buster-updates main  
deb-src http://ftp.debian.org/debian/ buster-updates main  
deb http://ftp.us.debian.org/debian/ buster main
```
- 6 Salvare il file.
- 7 Eseguire questi comandi:
  - **apt-get update**
  - **apt-get upgrade**
- 8 Aggiornare gli elenchi dei certificati CA nel server utilizzando **apt-get install ca-certificates**.
- 9 Installare le impostazioni locali **en\_US.utf8** utilizzando **dpkg-reconfigure locales**.
- 10 Selezionare le impostazioni locali **en\_US.UTF-8 UTF-8**, quindi impostarle come predefinite per il sistema.

**Nota:** utilizzare il tasto Tab e la barra spaziatrice per selezionare e navigare all'interno del menu.

- 11 Controllare le impostazioni locali generate utilizzando **locale -a**.

### Output di esempio

```
C
C.UTF-8
en_IN
en_IN.utf8
en_US.utf8
POSIX
```

- 12 Copiare l'impronta digitale del pacchetto OpenXPki utilizzando **nano /home/Release.key**. Per questo esempio, copiare la chiave in **/home**.
- 13 Digitare **55D89776 006F632B E0196E3E D2495509 BAFDDC74 22FEAAD2 F055074E 0FE3A724** come valore.
- 14 Eseguire questo comando:
- ```
gpg --print-md sha256 /home/Release.key
```
- 15 Aggiungere il pacchetto utilizzando il comando **wget https://packages.openxpki.org/v3/debian/Release.key -O - | apt-key add -**.
- 16 Aggiungere il repository all'elenco di origini (buster) utilizzando **echo " deb http://packages.openxpki.org/v3/debian/ buster release"**  
> **/etc/apt/sources.list.d/openxpki.list**, quindi **apt update**.
- 17 Installare l'associazione MySQL e Perl MySQL utilizzando **apt install mariadb-server libdbd-mariadb-perl**.
- 18 Installare apache2.2-common utilizzando **apt install apache2**.
- 19 In **nano /etc/apt/sources.list**, installare il modulo fastcgi per velocizzare l'interfaccia utente.
- Nota:** si consiglia di utilizzare **mod-fcgid**.
- 20 Aggiungere la riga **deb http://http.us.debian.org/debian/ buster main** nel file, quindi salvarlo.
- 21 Eseguire questi comandi:
- ```
apt-get update
apt install libapache2-mod-fcgid
```
- 22 Abilitare il modulo fastcgi utilizzando **a2enmod fcgid**.
- 23 Installare il pacchetto di base OpenXPki utilizzando **apt install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n**.
- 24 Riavviare il server Apache utilizzando **service apache2 restart**.
- 25 Controllare se l'installazione è avvenuta correttamente utilizzando **openxpkiadm version**.
- Nota:** se l'installazione è riuscita, il sistema mostra la versione di OpenXPki installata. Ad esempio, **Version (core): 3.18.2**.
- 26 Creare il database vuoto, quindi assegnare l'utente del database utilizzando **mariadb -u root -p**.

**Note:**

- Questo comando deve essere digitato nel client. In caso contrario, non è possibile immettere la password.

- Digitare la password per MySQL. Per questo esempio, **root** è l'utente MySQL.
- **openxpki** è l'utente su cui è installato OpenXPki.

```
CREATE DATABASE openxpki CHARSET utf8;
CREATE USER 'openxpki'@'localhost' IDENTIFIED BY 'openxpki';
GRANT ALL ON openxpki.* TO 'openxpki'@'localhost';
flush privileges;
```

Se il servizio MySQL non è in esecuzione, eseguire **/etc/init.d/mysql start** per avviarlo.

**27** Digitare **quit** per uscire da MySQL.

**28** Memorizzare le credenziali usate in **/etc/openxpki/config.d/system/database.yaml**.

### Contenuto del file di esempio

```
main:
debug: 0
type: MariaDB
name: openxpki
host: localhost
port: 3306
user: openxpki
passwd: openxpki
```

**Nota:** modificare **user** e **passwd** in modo che corrispondano al nome utente e alla password per MariaDB.

**29** Salvare il file.

**30** Per uno schema di database vuoto, eseguire **zcat /usr/share/doc/libopenxpki-perl/examples/schema-mariadb.sql.gz | \ mysql -u root --password --database openxpki** dal file di schema fornito.

**31** Digitare la password per il database.

### Configurazione di OpenXPki CA mediante lo script predefinito

**Nota:** lo script predefinito configura solo l'area di autenticazione predefinita, ovvero **ca-one**. CDP e CRL non sono configurati.

**1** Eseguire lo script utilizzando **bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh**.

**2** Confermare le impostazioni utilizzando **openxpkiadm alias --realm democa**.

### Output di esempio

```
=== functional token ===
scep (scep):
Alias      : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

vault (datasafe):
Alias      : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

ca-signer (certsign):
```

```
Alias      : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEhbtI9pE
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2018-01-29 20:44:40
```

```
=== root ca ===
current root ca:
Alias      : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore  : 2015-01-30 20:44:39
NotAfter   : 2020-01-30 20:44:39
```

```
upcoming root ca:
  not set
```

**3** Controllare se l'installazione è avvenuta correttamente utilizzando **openxpkictl start**.

## Output di esempio

```
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

**4** Effettuare le seguenti operazioni per accedere al server OpenXPki:

- a** Nel browser Web, digitare **http://ipaddress/openxpki/**.
- b** Aggiungere il nome utente e le password corrispondenti in un file **userdb.yaml**. Per aggiungere il nome utente e la password, procedere come segue:
  - Eseguire il check-out a **/home/pkiadm** e quindi **nano userdb.yaml**.
  - Incollare quanto segue:

```
estRA:
  digest: "{ssh256}somePassword"
  role: RA Operator
```

**Nota:** in questo caso estRA si riferisce al nome utente. Per generare la password, digitare **openxpkiadm hashpwd**. Quando viene visualizzato un messaggio che richiede la password e appare una password crittografata ssh256, copiarla e incollarla nel digest di qualsiasi utente.

**Nota:** i ruoli disponibili nell'accesso Operatore sono RA Operator CA Operator e User.

**5** Immettere il nome utente e la password.

**6** Creare una richiesta di certificato, quindi testarla.

## Configurazione manuale di OpenXPki CA

### Panoramica

**Nota:** prima di iniziare, assicurarsi di disporre di una conoscenza di base sulla creazione di certificati OpenSSL.

Per configurare manualmente OpenXPki CA, creare i seguenti certificati:

- 1** Certificato CA radice. Per ulteriori informazioni, vedere ["Creazione di un certificato CA radice" a pagina 104](#).
- 2** Certificato del firmatario CA, firmato dalla CA radice. Per ulteriori informazioni, vedere ["Creazione di un certificato del firmatario" a pagina 104](#).

- 3** Certificato del vault di dati, autofirmato. Per ulteriori informazioni, vedere ["Creazione di un certificato del vault" a pagina 105](#).
- 4** Certificato Web, firmato dal certificato del firmatario. Per ulteriori informazioni, vedere ["Configurazione del server Web" a pagina 123](#).

**Note:**

- Quando si seleziona l'hash della firma, utilizzare SHA256 o SHA512.
- La modifica della dimensione della chiave pubblica è opzionale.

Per la versione 3.10 o successiva, è possibile gestire le chiavi direttamente utilizzando il comando `openxpkiadm alias`:

- Eseguire `mkdir -p /etc/openxpki/local/key` per creare la directory. La posizione predefinita della directory è `/etc/openxpki/local/keys`.
- Eseguire `openxpkictl start` per avviare il server.

In questo esempio, utilizziamo la directory `/etc/certs/openxpki_democa/` per la generazione dei certificati. Tuttavia, è possibile utilizzare qualsiasi directory.

## Creazione di un file di configurazione OpenSSL

Il file di configurazione OpenSSL contiene le estensioni X.509 per la generazione e la firma delle richieste di certificato.

- 1** Eseguire questo comando:

```
nano /etc/certs/openxpki_democa/openssl.conf
```

**Nota:** se il server è raggiungibile tramite il nome di dominio completo (FQDN), utilizzare il DNS del server anziché il suo indirizzo IP.

### File di esempio

```
# x509_extensions          = v3_ca_extensions
# x509_extensions          = v3_issuing_extensions
# x509_extensions          = v3_datavault_extensions
# x509_extensions          = v3_scep_extensions
# x509_extensions          = v3_web_extensions
# x509_extensions          = v3_ca_reqexts # not for root self-signed, only for issuing
## x509_extensions         = v3_datavault_reqexts # not required self-signed
# x509_extensions          = v3_scep_reqexts
# x509_extensions          = v3_web_reqexts

[ req ]
default_bits               = 4096
distinguished_name         = req_distinguished_name

[ req_distinguished_name ]
domainComponent            = Domain Component
commonName                 = Common Name

[ v3_ca_reqexts ]
subjectKeyIdentifier       = hash
keyUsage                   = digitalSignature, keyCertSign, cRLSign

[ v3_datavault_reqexts ]
subjectKeyIdentifier       = hash
keyUsage                   = keyEncipherment
extendedKeyUsage           = emailProtection

[ v3_scep_reqexts ]
subjectKeyIdentifier       = hash
```



```

[ v3_web_reqexts ]
subjectKeyIdentifier    = hash
keyUsage                = critical, digitalSignature, keyEncipherment
extendedKeyUsage        = serverAuth, clientAuth

[ v3_ca_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = digitalSignature, keyCertSign, cRLSign
basicConstraints        = critical,CA:TRUE
authorityKeyIdentifier  = keyid:always,issuer

[ v3_issuing_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = digitalSignature, keyCertSign, cRLSign
basicConstraints        = critical,CA:TRUE
authorityKeyIdentifier  = keyid:always,issuer:always
crlDistributionPoints    = URI:https://FQDN of your system/openxpki/CertEnroll/MYOPENXPki.crl
authorityInfoAccess     = caIssuers;URI:https://FQDN of your system/download/MYOPENXPki.crt

[ v3_datavault_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = keyEncipherment
extendedKeyUsage        = emailProtection
basicConstraints        = CA:FALSE
authorityKeyIdentifier  = keyid:always,issuer

[ v3_scep_extensions ]
subjectKeyIdentifier    = hash
basicConstraints        = CA:FALSE
authorityKeyIdentifier  = keyid,issuer

[ v3_web_extensions ]
subjectKeyIdentifier    = hash
keyUsage                = critical, digitalSignature, keyEncipherment
extendedKeyUsage        = serverAuth, clientAuth
basicConstraints        = critical,CA:FALSE
subjectAltName          = DNS:FQDN of est server
crlDistributionPoints    = URI:https://FQDN of your
system/openxpki/CertEnroll/MYOPENXPki_ISSUINGCA.cr
authorityInfoAccess     = caIssuers;URI:https://FQDN of your
system/download/MYOPENXPki_ISSUINGCA.crt

```

**2** Sostituire l'indirizzo IP e il nome del certificato CA in base alle informazioni delle proprie impostazioni.

**3** Salvare il file.

## Creazione di un file di password per le chiavi dei certificati

**1** Eseguire questo comando:

```
nano /etc/certs/openxpki_democa/pd.pass
```

**2** Digitare la propria password.

**3** Salvare il file.

## Creazione di un certificato CA radice

È possibile creare un certificato CA radice autofirmato o generare una richiesta di certificato e quindi ottenerne la firma dalla CA radice.

**Nota:** sostituire la lunghezza della chiave, l'algoritmo di firma e il nome del certificato con i valori appropriati.

**1** Eseguire questo comando:

```
openssl genrsa -out /etc/certs/openxpki_democa/ca-root-1.key -passout
file:/etc/certs/openxpki_democa/pd.pass 4096
```

- 2 Sostituire il soggetto della richiesta con le informazioni della propria CA utilizzando **openssl req -new -key /etc/certs/openxpki\_democa/ca-root-1.key -out /etc/certs/openxpki\_democa/ca-root-1.csr**.
- 3 Ottenere il certificato firmato dalla CA radice utilizzando **openssl req -config /etc/certs/openxpki\_democa/openssl.conf -extensions v3\_ca\_extensions -x509 -days 3560 -in /etc/certs/openxpki\_democa/ca-root-1.csr -key /etc/certs/openxpki\_democa/ca-root-1.key -out /etc/certs/openxpki\_democa/ca-root-1.crt -sha256**.
- 4 Accedere a **/etc/certs/openxpki\_democa/** in cui è salvato **ca-root-1.crt**.
- 5 Eseguire questo comando:  
**openxpkiadm certificate import --file ca-root-1.crt**

## Creazione di un certificato del firmatario

**Nota:** sostituire la lunghezza della chiave, l'algoritmo di firma e il nome del certificato con i valori appropriati.

- 1 Eseguire questo comando:  
**openssl genrsa -out /etc/certs/openxpki\_democa/ca-signer-1.key -passout file:/etc/certs/openxpki\_democa/pd.pass 4096**
- 2 Modificare l'oggetto della richiesta con le informazioni della propria CA utilizzando **openssl req -config /etc/certs/openxpki\_democa/openssl.conf -reqexts v3\_ca\_reqexts -new -key /etc/certs/openxpki\_democa/ca-signer-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI\_ISSUINGCA -out /etc/certs/openxpki\_democa/ca-signer-1.csr**.
- 3 Ottenere il certificato firmato dalla CA radice utilizzando **openssl x509 -req -extfile /etc/certs/openxpki\_democa/openssl.conf -extensions v3\_issuing\_extensions -days 3650 -in /etc/certs/openxpki\_democa/ca-signer-1.csr -CA /etc/certs/openxpki\_democa/ca-root-1.crt -CAkey /etc/certs/openxpki\_democa/ca-root-1.key -CAcreateserial -out /etc/certs/openxpki\_democa/ca-signer-1.crt -sha256**.
- 4 Eseguire questo comando:  
**openxpkiadm alias --realm democa --token certsign --file ca-signer-1.crt --key ca-signer-1.key**

## Creazione di un certificato del vault

**Note:**

- Il certificato del vault è autofirmato.
- sostituire la lunghezza della chiave, l'algoritmo di firma e il nome del certificato con i valori appropriati.

- 1 Eseguire questo comando:  
**openssl req -new -x509 -keyout vault.key -out vault.crt -days 1100 -config /etc/certs/openxpki\_democa/openssl.conf**
- 2 Modificare l'oggetto della richiesta con le informazioni della propria CA utilizzando **openxpkiadm certificate import --file vault.crt**.

3 Eseguire questo comando:

```
openxpkiadm alias --realm democa --token datasafe --file vault.crt --key
vault.key
```

**Nota:** fornire i valori necessari, ma mantenere **/CN=DataVault** come oggetto.

## Creazione di un certificato Web

1 Eseguire questo comando:

```
openssl genrsa -out /etc/certs/openxpki_democa/web-1.key -passout
file:/etc/certs/openxpki_democa/pd.pass 4096
```

2 Modificare l'oggetto della richiesta con le informazioni della propria CA utilizzando **openssl req -config /etc/certs/openxpki\_democa/openssl.conf -reqexts v3\_web\_reqexts -new -key /etc/certs/openxpki\_democa/web-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=FQDN of your system -out /etc/certs/openxpki\_democa/web-1.csr**.

3 Eseguire questo comando:

```
openssl x509 -req -extfile /etc/certs/openxpki_democa/openssl.conf -
extensions v3_web_extensions -days 900 -
in /etc/certs/openxpki_democa/web-1.csr -CA /etc/certs/openxpki_democa/ca-
signer-1.crt -CAkey /etc/certs/openxpki_democa/ca-signer-1.key -
CAcreateserial -out /etc/certs/openxpki_democa/web-1.crt -sha256
```

## Configurazione del server Web

1 Eseguire questi comandi:

```
a2enmod ssl rewrite headers
a2ensite openxpki
a2disssite 000-default default-ssl
mkdir -m755 -p /etc/openxpki/tls/chain
cp /etc/certs/openxpki_democa/ca-root-1.crt /etc/openxpki/tls/chain/
cp /etc/certs/openxpki_democa/ca-signer-1.crt /etc/openxpki/tls/chain/
c_rehash /etc/openxpki/tls/chain/
mkdir -m755 -p /etc/openxpki/tls/entidentity
mkdir -m700 -p /etc/openxpki/tls/private
cp /etc/certs/openxpki_democa/web-1.crt /etc/openxpki/tls/entidentity/openxp
ki.crt
cat /etc/certs/openxpki_democa/ca-signer-1.crt
>> /etc/openxpki/tls/entidentity/openxpki.crt
openssl rsa -in /etc/certs/openxpki_democa/web-1.key -passin
file:/etc/certs/openxpki_democa/pd.pass -
out /etc/openxpki/tls/private/openxpki.pem
chmod 400 /etc/openxpki/tls/private/openxpki.pem
```

2 Riavviare il servizio OpenXPki utilizzando **apache2 restart**.

**3** Eseguire questo comando per verificare che l'importazione dei file abbia avuto esito positivo:

```
openxpkiadm alias --realm democa
```

### Output di esempio

```
=== functional token ===
ca-signer (certsign):
  Alias       : ca-signer-2
  Identifier: XjC6MPbsnyfLZkI9Poi9vm4Z5rk
  NotBefore  : 2022-04-06 10:03:01
  NotAfter   : 2032-04-03 10:03:01

vault (datasafe):
  Alias       : vault-2
  Identifier: G8ekluAsskGVC0N-jZhB2n9kvdM
  NotBefore  : 2022-04-06 09:53:57
  NotAfter   : 2025-04-10 09:53:57

scep (scep):
  not set

ratoken (cmcra):
  not set

=== root ca ===
current root ca:
  Alias       : root-2
  Identifier: prTHU5vCfcJuCnQWyb5wUknvXQM
  NotBefore  : 2022-04-06 09:40:27
  NotAfter   : 2032-01-04 09:40:27
```

## Rendere la password della chiave del certificato disponibile per OpenXPki

- 1 Modificare il valore nel file **nano /etc/openxpki/config.d/system/crypto.yaml**.
- 2 Rimuovere il commento dalla cache: **daemon under secret: default:**

```
secret:
  default:
    label: Global Secret group
    export: 0
    method: literal
    value: root
    cache: daemon
```

## Avvio di OpenXPki

- 1 Eseguire il comando **openxpkictl start**.

### Output di esempio

```
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

- 2 Accedere al server OpenXPki:

- a Nel browser Web, digitare **http://ipaddress/openxpki/**.
- b Aggiungere i nomi utente e le password corrispondenti in un file **userdb.yaml**:

- Eseguire il check-out a **/home/pkiadm** e quindi **nano userdb.yaml**.
- Incollare quanto segue:

```
estRA:
  digest: "{ssh256}somePassword"
  role: RA Operator
```

**Nota:** qui estRA si riferisce al nome utente.

- Per generare la password, digitare **openxpkiadm hashpwd**. Viene visualizzato un messaggio che mostra la password e una password crittografata ssh256.
- Copiare la password, quindi incollarla nel digest di qualsiasi utente.

**Nota:** l'accesso Operatore ha due ruoli disponibili preconfigurati: RA Operator, CA Operator e User.

**3** Digitare il nome utente e la password.

**4** Creare una richiesta di certificato, quindi testarla.

## Generazione delle informazioni del CRL

**Nota:** se il server è raggiungibile tramite il nome di dominio completo (FQDN), utilizzare il DNS del server anziché il suo indirizzo IP.

**1** Arrestare il servizio OpenXPki utilizzando **openxpkictl stop**.

**2** In **nano /etc/openxpki/config.d/realm/democa/publishing.yaml**, aggiornare la sezione **connectors:** **cdp** come segue:

```
class: Connector::Builtin::File::Path
LOCATION: /var/www/openxpki/CertEnroll/
file: "[% ARGS.0 %].crl"
content: "[% pem %]"
```

**a** In **nano /etc/openxpki/config.d/realm/democa/profile/default.yaml**, aggiornare quanto segue:

- **Sezione `crl_distribution_points`:** sezione

```
critical: 0
uri:
  - https://FQDN of the est/openxpki/CenrtEnroll/[% ISSUER.CN.0 %].crl
  - ldap://localhost/[% ISSUER.DN %]
```

- **Sezione `authority_info_access`:** sezione

```
critical: 0
ca_issuers: http://FQDN of the est/download/MYOPENXPki.crt
ocsp: http://ocsp.openxpki.org/
```

Modificare l'indirizzo IP e il nome del certificato CA in base al proprio server CA.

**Nota:** il percorso `authority_info_access` (AIA) viene salvato nella cartella Download, ma è possibile impostare la posizione in base alle proprie preferenze.

**b** In **nano /etc/openxpki/config.d/realm/democa/crl/default.yaml**, effettuare le seguenti operazioni:

- Se necessario, aggiornare **nextupdate** e **renewal**.
- Aggiungere **ca\_issuers** alla seguente sezione:

```
extensions:
  authority_info_access:
    critical: 0
    # ca_issuers and ocsp can be scalar or list
    ca_issuers: https://FQDN of the est/download/MYOPENXPki.crt
    #ocsp: http://ocsp.openxpki.org/
```

Modificare l'indirizzo IP e il nome del certificato CA in base al proprio server CA.

**3** Avviare il servizio OpenXPki utilizzando **openxpkictl start**.

## Publicazione delle informazioni CRL

Dopo aver creato i CRL, è necessario pubblicarli affinché tutti possano accedervi.

- 1 Arrestare il servizio Apache utilizzando **service apache2 stop**.
- 2 Creare una directory **CertEnroll** per il CRL nella directory **/var/www/openxpi/**.
- 3 Impostare **openxpi** come proprietario di questa directory, quindi configurare le autorizzazioni per consentire ad Apache la lettura e l'esecuzione e agli altri servizi la sola lettura.  
**chown openxpi /var/www/openxpi/CertEnroll**  
**chmod 755 /var/www/openxpi/CertEnroll**
- 4 Aggiungere un riferimento al file Apache alias.conf utilizzando **nano /etc/apache2/mods-enabled/alias.conf**.
- 5 Dopo la sezione **<Directory "/usr/share/apache2/icons">**, aggiungere quanto segue:

```
Alias /CertEnroll/ "/var/www/openxpi/CertEnroll/"
<Directory "/var/www/openxpi/CertEnroll">
    Options FollowSymlinks
    AllowOverride None
    Require all granted
</Directory>
```

- 6 Aggiungere un riferimento nel file apache2.conf utilizzando **nano /etc/apache2/apache2.conf**.
- 7 Aggiungere quanto segue nella sezione **Apache2 HTTPD server**:

```
<Directory /var/www/openxpi/CertEnroll>
    Options FollowSymlinks
    AllowOverride None
    Allow from all
</Directory>
```

- 8 Avviare il servizio Apache utilizzando **service apache2 start**.

## Abilitazione dell'approvazione automatica delle richieste di certificato in OpenXPki CA

- 1 Arrestare il servizio OpenXPki utilizzando **openxpkictl stop**.
- 2 In **/etc/openxpi/config.d/realm/democa/est/default.yaml**, aggiornare la sezione **eligible**: come segue:

### Precedente contenuto

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
    args: "[% context.cert_subject_parts.CN.0 %]"
    expect:
      - Build
      - New
```

### Nuovo contenuto

```
eligible:
  initial:
    value: 1
    # value@: connector:scep.generic.connector.initial
    # args: "[% context.cert_subject_parts.CN.0 %]"
    # expect:
    #   - Build
    #   - New
```

**Note:**

- Esaminare lo spazio e il rientro nel file script.
- Per approvare manualmente i certificati, inserire un commento per **value: 1**, quindi rimuovere il commento dalle altre righe in cui era stato in precedenza inserito.

**3** Salvare il file.

**4** Avviare il servizio OpenXPki utilizzando **openxpkictl start**.

## Modifica dei dettagli per abilitare il download di ca-certs

**1** Eseguire questo comando:

```
nano /usr/lib/cgi-bin/est.fcgi
```

**2** Sostituire **my \$mime = "application/pkcs7-mime; smime-type=certs-only";** con **my \$mime = "application/pkcs7-mime";**.

**3** Avviare il servizio OpenXPki utilizzando **openxpkictl**.

## Creazione di una seconda area di autenticazione

In OpenXPki è possibile configurare più strutture PKI sullo stesso sistema. I seguenti argomenti illustrano come creare un'altra area di autenticazione per MVE denominata **democa-two**.

### Copia e impostazione della directory

**1** Creare una directory, ossia **democa2**, per la seconda area di autenticazione all'interno di **/etc/openxpki/config.d/realm**.

**2** Copiare la struttura di directory di esempio **/etc/openxpki/config.d/realm/ca-one** in una nuova directory (**cp -r /etc/openxpki/config.d/realm.tpl/\* /etc/openxpki/config.d/realm/democa2**) all'interno della directory dell'area di autenticazione.

**3** In **/etc/openxpki/config.d/system/realms.yaml**, aggiornare la seguente sezione:

#### Precedente contenuto

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

democa:
  label: Verbose name of this realm
  baseurl: https://pki.example.com/openxpki/

#democa2:
#   label: Verbose name of this realm
#   baseurl: https://pki.acme.org/openxpki/
```

#### Nuovo contenuto

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

democa:
  label: Example.org Demo CA
  baseurl: https://pki.example.com/openxpki/

democa2:
```

```
label: Example.org Demo CA2
baseurl: https://pki.example.com/openxpki/
```

#### 4 Salvare il file.

### Configurazione dell'endpoint EST per più aree di autenticazione

È possibile configurare l'endpoint EST con una tupla composta dalla parte dell'URI relativa all'autorità dall'etichetta opzionale (ad esempio `www.example.com:80` e `arbitraryLabel1`). Nelle seguenti istruzioni utilizziamo due aree di autenticazione PKI, ovvero **democa** e **democa2**.

#### 1 Copiare il file di configurazione predefinito in

**cp /etc/openxpki/est/default.conf /etc/openxpki/est/democa.conf.**

**Nota:** assegnare al file il nome **democa.conf**.

#### 2 In **nano /etc/openxpki/est/democa.conf**, modificare il valore dell'area di autenticazione in **realm=democa**.

**Nota:** In base alle esigenze, potrebbe essere necessario rimuovere i commenti dalle righe corrispondenti per le sezioni **simpleenroll**, **simplereenroll**, **csrattrs** e **cacerts**. Mantenere i commenti delle sezioni relative all'ambiente. Eseguire la stessa operazione per **default.conf**.

#### 3 Creare un altro file di configurazione in

**cp /etc/openxpki/est/default.conf /etc/openxpki/est/democa2.conf.**

**Nota:** assegnare al file il nome **democa2.conf**.

#### 4 In **nano /etc/openxpki/est/democa2.conf**, modificare il valore dell'area di autenticazione in **realm=democa2**.

**Nota:** In base alle esigenze, potrebbe essere necessario rimuovere i commenti dalle righe corrispondenti per le sezioni **simpleenroll**, **simplereenroll**, **csrattrs** e **cacerts**. Mantenere i commenti delle sezioni relative all'ambiente.

#### 5 Copiare il file **default.yaml** nelle seguenti posizioni:

- **cp /etc/openxpki/config.d/realm/democa/est/default.yaml**
- **/etc/openxpki/config.d/realm/democa/est/democa.yaml**

**Nota:** assegnare al file il nome **democa.yaml**.

#### 6 Copiare il file **default.yaml** nelle seguenti posizioni:

- **cp /etc/openxpki/config.d/realm/democa2/est/default.yaml**
- **/etc/openxpki/config.d/realm/democa2/est/democa2.yaml**

**Nota:** assegnare al file il nome **democa2.yaml**.

#### 7 Riavviare il servizio OpenXPki utilizzando **openxpkictl restart**.

Selezionare i seguenti URL per aprire il server EST corrispondente a un'area di autenticazione tramite un browser Web:

- **democa:** **http://ipaddress/est/democa**
- **democa2:** **http://ipaddress/est/democa2**

Se si desidera differenziare tra le credenziali di accesso e i modelli di certificato predefiniti per aree di autenticazione PKI diverse, potrebbe essere necessaria una configurazione avanzata.



## Creazione di un certificato del firmatario

Le seguenti istruzioni mostrano come generare un certificato del firmatario nella seconda area di autenticazione. È possibile utilizzare gli stessi certificati radice e del vault presenti nella prima area di autenticazione.

- 1 Creare un file di configurazione OpenSSL in **nano /etc/certs/openxpki\_democa2/openssl.conf**.

**Nota:** modificare il nome comune del certificato in modo che l'utente possa distinguere facilmente tra i diversi certificati per le diverse aree di autenticazione. I file di certificato vengono creati nella directory **/etc/certs/openxpki\_democa2/**.

- 2 Accedere alla directory del certificato del vault nella prima area di autenticazione, quindi importare il certificato dalla prima area di autenticazione.

- 3 Eseguire questo codice:

```
openxpkiadm alias --realm democa2 --token datasafe --file vault.crt
```

## Creazione di un file di password per le chiavi dei certificati

- 1 Eseguire questo comando:

```
nano /etc/certs/openxpki_democa2/pd.pass
```

- 2 Digitare la propria password.

- 3 Creare un certificato del firmatario. Per ulteriori informazioni, vedere ["Creazione di un certificato del firmatario" a pagina 104](#).

- 4 Controllare se l'importazione è avvenuta correttamente utilizzando **openxpkiadm alias --realm democa2**.

**Nota:** se la password della chiave del certificato è stata modificata durante la creazione del certificato, aggiornare **nano /etc/openxpki/config.d/realm/democa2/crypto.yaml**.

- 5 Generare i CRL per la seconda area di autenticazione. Per ulteriori informazioni, vedere ["Generazione delle informazioni del CRL" a pagina 107](#).

**Nota:** assicurarsi di utilizzare il nome del certificato CA corretto in base all'area di autenticazione.

- 6 Pubblicare i CRL per questa area di autenticazione. Per ulteriori informazioni, vedere ["Pubblicazione delle informazioni CRL" a pagina 126](#).

- 7 Riavviare il servizio OpenXPki utilizzando **openxpkictl restart**.

## Output di esempio

```
Stopping OpenXPki
Stopping gracefully, 3 (sub)processes remaining...
DONE.
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

## Abilitazione della presenza contemporanea di più certificati attivi con lo stesso oggetto

Per impostazione predefinita, in OpenXPki può essere attivo un solo certificato con lo stesso nome oggetto alla volta. Tuttavia, quando si applicano più certificati con nome, devono essere presenti più certificati attivi con lo stesso nome oggetto alla volta.

- 1 In `/etc/openxpki/config.d/realm/REALM NAME/est/< REALM NAME >.yaml`, nella sezione **policy**, modificare il valore di **max\_active\_certs** da 1 a 0.

### Note:

- REAL NAME è il nome dell'area di autenticazione. Ad esempio, **ca-one**.
- Esaminare lo spazio e il rientro nel file script.

- 2 Riavviare il servizio OpenXPki utilizzando **openxpkictl restart**.

## Impostazione del numero di porta predefinito per OpenXPki CA

Per impostazione predefinita, Apache è in ascolto sulla porta numero 443 per https. Impostare il numero di porta predefinito per OpenXPki CA per evitare conflitti.

- 1 In `/etc/apache2/ports.conf`, modificare la porta 443 impostando su una qualsiasi altra porta. Ad esempio:

### Precedente contenuto

```
Listen 80

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>
```

### Nuovo contenuto

```
Listen 80

<IfModule ssl_module>
    Listen 9443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 9443
</IfModule>
```

- 2 In `/etc/apache2/sites-available/openxpki.conf`, aggiungere o modificare la sezione **VirtualHost** per associare una nuova porta. Ad esempio, **<VirtualHost \*:443>** in **<Virtualhost \*:9443>**.
- 3 In `/etc/apache2/sites-available/default-ssl.conf`, aggiungere o modificare la sezione **VirtualHost\_default** per associare una nuova porta. Ad esempio, modificare **<VirtualHost \*:443>** in **<Virtualhost \*:9443>**.
- 4 Riavviare il server Apache utilizzando **systemctl restart apache2**.

**Nota:** se viene richiesta la passphrase **SSL/TLS**, digitare la password quando si aggiunge il certificato del server Web TLS nel server EST.

- 5 In **tinddopenxpkiweb01.dhcp.dev.lexmark.com:9443 (RSA):**, immettere la passphrase per le chiavi **SSL/TLS**.

Per verificare lo stato, eseguire **netstat -tlnp | grep apache**. L'URL SCEP di OpenXPki è ora **https://ipaddress**, mentre l'URL Web è **FQDN:9443/openxpki**.

## Abilitazione dell'autenticazione di base

1 Eseguire questo comando:

```
apt -y install apache2-utils
```

2 Creare un account utente che abbia accesso al server. Immettere i seguenti dettagli:

```
htpasswd -c /etc/apache2/.htpasswd <username>
New password:
Re-type new password:
Adding password for user <username>
```

3 Passare alla directory **cd /etc/apache2/sites-enabled/**.

4 In **nano openxpki.conf**, aggiungere le seguenti righe in **<Virtualhost \*: 443 block>**:

```
#HTTPS BASIC AUTH FOR LABELS
Location /.well-known/est/*/simpleenroll
    AuthType Basic
    AuthName "estrealm"
    AuthUserFile /etc/apache2/.htpasswd
    require valid-user
</Location>
#HTTPS BASIC AUTH FOR NO LABEL
<Location /.well-known/est/simpleenroll>
    AuthType Basic
    AuthName "estrealm"
    AuthUserFile /etc/apache2/.htpasswd
    require valid-user
</Location>
```

5 Aggiungere **ErrorDocument 401%{unescape:%00}** prima di **SSLEngine** nello stesso blocco host virtuale.

## Esempio

```
ServerAlias *
DocumentRoot /var/www/
ErrorDocument 401 %{unescape:%00}
SSLEngine On
```

6 Riavviare il **servizio apache2** utilizzando **service apache2 restart**.

**Nota:** l'autenticazione di base funziona utilizzando il nome utente e la password indicati sopra.

## Abilitazione dell'autenticazione con certificato client

1 Passare alla seguente directory: **cd /etc/apache2/sites-enabled/**.

2 Per l'host richiesto in **nano openxpki.conf**, aggiungere **SSLVerifyClient require**.

Ad esempio, se si utilizza la porta 443, modificare la sezione **Virtualhost** in:

```
<VirtualHost *:443>
SSLVerifyClient require
</VirtualHost>
```

3 Rimuovere il comando **SSLVerifyClient opzional\_no\_ca**.

4 Salvare il file, quindi digitare **quit** per uscire da MySQL.

5 Passare alla seguente directory: **cd /etc/openxpki/config.d/realm/democa/est**.

**6** Aprire **default.yaml** e **democa.yaml**.

**Nota:** Se l'etichetta è diversa, modificare il file YAML.

**7** Eseguire questo comando:

```
vi default.yaml
```

**8** Nella sezione **authorized\_signer**, aggiungere quanto segue:

```
authorized_signer:
rule2:
    subject: CN=, .
```

Ad esempio, se il nome dell'oggetto del certificato client è **test123**, aggiungere quanto segue nella sezione **authorized\_signer**:

```
authorized_signer:
rule1:
    # Full DN
    subject: CN=.:pkiclient, .
rule2:
    subject: CN=test123, .*
```

**9** Salvare il file, quindi digitare **quit** per uscire da MySQL.**10** Riavviare il servizio OpenXPki utilizzando **openxpkictl restart**.**11** Avviare il servizio Apache utilizzando **service apache2 restart**.

### Che cosa causa dell'errore di SAN non corrispondente che impedisce al sistema di recuperare il CRL?

L'errore di SAN non corrispondente può verificarsi quando si abilitano le informazioni CRL. Questo errore indica che l'IP o il nome host non corrispondono al valore della SAN nel certificato Web. Per evitare di ricevere questo errore, utilizzare il nome di dominio completo (FQDN) nel percorso del CRL anziché l'IP. È anche possibile configurare il certificato Web e utilizzare l'FQDN del sistema nel campo SAN.

### Perché i token ca-signer-1 e vault-1 sono offline?

Se nella pagina Stato sistema risulta che i token ca-signer-1 e vault-1 sono offline, procedere come segue:

**1** In **/etc/openxpki/config.d/realm/realm name/crypto.yaml**, modificare il valore della chiave corrispondente.

**2** Riavviare il servizio OpenXPki.

## Gestione degli avvisi della stampante

# Panoramica

Gli avvisi vengono attivati quando una stampante richiede un intervento. Le azioni consentono di inviare e-mail personalizzate o di eseguire script quando viene emesso un avviso. Gli eventi definiscono quali azioni vengono eseguite quando sono attivi avvisi specifici. Per effettuare la registrazione per gli avvisi da una stampante, creare azioni, quindi associarle a un evento. Assegnare l'evento alle stampanti da monitorare.

**Nota:** questa funzione non è applicabile alle stampanti protette.

## Creazione di un'azione

Un'azione è una notifica e-mail o un registro di visualizzazione eventi. Le azioni assegnate agli eventi vengono attivate quando viene emesso un avviso della stampante.

- 1 Nel menu Stampanti fare clic su **Eventi e azioni** > **Azioni** > **Crea**.
- 2 Digitare un nome univoco per l'azione e la relativa descrizione.
- 3 Selezionare un tipo di azione.

## E-mail

**Nota:** prima di iniziare, accertarsi che le impostazioni e-mail siano configurate. Per ulteriori informazioni, vedere ["Configurazione delle impostazioni e-mail"](#) a pagina 145.

- a** Nel menu Tipo selezionare **E-mail**.
- b** Immettere i valori appropriati nei relativi campi. È anche possibile utilizzare i segnaposto disponibili per una parte o per tutto il titolo dell'oggetto, o come parte di un messaggio e-mail. Per ulteriori informazioni, vedere ["Comprensione segnaposto azione" a pagina 134](#).

Type

E-mail

From (Optional)

admin@mycompany.com

To

scott.summers@mycompany.com

CC (Optional)

Subject (Optional)

\$ {alert.type}

alert.type

Body

\$ {alert.type}\$ {alert.location}\$ {alert.name}

alert.name

Create Action

Cancel

- c** Fare clic su **Crea azione**.

## Registro eventi

- a Nel menu Tipo selezionare **Registro eventi**.
- b Digitare i parametri dell'evento. È inoltre possibile utilizzare i segnaposto nel menu a discesa. Per ulteriori informazioni, vedere ["Comprensione segnaposto azione" a pagina 134](#).

- c Fare clic su **Crea azione**.

## Comprensione segnaposto azione

Utilizzare i segnaposto disponibili nel titolo dell'oggetto o nel messaggio e-mail. I segnaposto rappresentano degli elementi variabili e vengono sostituiti con i valori effettivi una volta utilizzati.

- **\$(eventHandler.timestamp)**: la data e l'ora di elaborazione dell'evento in MVE. Ad esempio, **Mar 14, 2017 1:42:24 PM**.
- **\$(eventHandler.name)**: il nome dell'evento.
- **\$(configurationItem.name)**: il nome del sistema della stampante che ha attivato l'avviso.
- **\$(configurationItem.address)**: l'indirizzo MAC della stampante che ha attivato l'avviso.
- **\$(configurationItem.ipAddress)**: l'indirizzo IP della stampante che ha attivato l'avviso.
- **\$(configurationItem.ipHostname)**: il nome host della stampante che ha attivato l'avviso.
- **\$(configurationItem.model)**: il nome del modello della stampante che ha attivato l'avviso.
- **\$(configurationItem.serialNumber)**: il numero di serie della stampante che ha attivato l'avviso.
- **\$(configurationItem.propertyTag)**: l'etichetta della proprietà della stampante che ha attivato l'avviso.
- **\$(configurationItem.contactName)**: il nome del contatto della stampante che ha attivato l'avviso.
- **\$(configurationItem.contactLocation)**: la posizione di contatto della stampante che ha attivato l'avviso.
- **\$(configurationItem.manufacturer)**: il produttore della stampante che ha attivato l'avviso.
- **\$(alert.name)**: il nome dell'avviso attivato.
- **\$(alert.state)**: lo stato dell'avviso. Può essere attivo o cancellato.
- **\$(alert.location)**: la posizione all'interno della stampante in cui si è verificato l'avviso attivato.
- **\$(alert.type)**: la gravità dell'avviso attivato, ad esempio **Avvertenza** o **Intervento richiesto**.

## Gestione delle azioni

**1** Nel menu Stampanti, fare clic su **Eventi e azioni > Azioni**.

**2** Effettuare una delle seguenti operazioni:

### Modificare un'azione

- a** Selezionare un'azione, quindi fare clic su **Modifica**.
- b** Configurare le impostazioni.
- c** Fare clic su **Salva modifiche**.

### Eliminare le azioni

- a** Selezionare una o più azioni.
- b** Fare clic su **Elimina**, quindi confermare l'eliminazione.

### Effettuare il test di un'azione

- a** Selezionare un'azione, quindi fare clic su **Test**.
- b** Per verificare i risultati del test, vedere i registri delle attività.

#### Note:

- Per ulteriori informazioni, vedere ["visualizzazione dei registri" a pagina 141](#).
- Se si sta effettuando il test di un'azione e-mail, verificare se l'e-mail è stata inviata al destinatario.

## Creazione di un evento

È possibile controllare gli avvisi nel parco periferiche. Creare un evento, quindi impostare l'esecuzione di un'azione quando si verificano gli avvisi specificati. Gli eventi non sono supportati sulle stampanti protette.

**1** Nel menu Stampanti, fare clic su **Eventi e azioni > Eventi > Crea**.

**2** Digitare un nome univoco per l'evento e la relativa descrizione.

**3** Nella sezione Avvisi, selezionare uno o più eventi. Per ulteriori informazioni, vedere ["Informazioni sugli avvisi della stampante" a pagina 136](#).

**4** Nella sezione Azioni, selezionare una o più azioni da eseguire quando sono attivi gli avvisi selezionati.

**Nota:** Per ulteriori informazioni, vedere ["Creazione di un'azione" a pagina 133](#).

**5** Consentire al sistema di eseguire azioni specifiche quando vengono cancellati gli avvisi sulla stampante.

**6** Impostare un periodo di tolleranza prima dell'esecuzione delle azioni selezionate.

**Nota:** Se l'avviso viene cancellato durante il periodo di tolleranza, l'azione non viene eseguita.

**7** Fare clic su **Crea evento**.

## Informazioni sugli avvisi della stampante

Gli avvisi vengono attivati quando una stampante richiede un intervento. I seguenti avvisi possono essere associati a un evento in MVE:

- **Inceppamento alimentatore automatico documenti (ADF):** un documento è inceppato nell'ADF e deve essere rimosso fisicamente.
  - Scanner: Inceppamento uscita ADF
  - Scanner: Inceppamento carta ADF
  - Scanner: Inceppamento inversione ADF
  - Scanner: Carta inceppata nell'ADF rimossa
  - Scanner: Carta ADF mancante
  - Scanner: Inceppamento preregistrazione ADF
  - Scanner: Inceppamento registrazione ADF
  - Avviso scanner: sostituire tutti gli originali in caso di riavvio del processo
- **Sportello o coperchio aperto:** uno sportello della stampante è aperto e deve essere chiuso.
  - Controlla coperchio/sportello - Mailbox
  - Sportello aperto
  - Avviso coperchio
  - Coperchio chiuso
  - Coperchio aperto
  - Coperchio aperto o cartuccia mancante
  - Coperchio fronte/retro aperto
  - Coperchio ADF scanner aperto
  - Coperchio di accesso inceppamento scanner aperto
- **Dimensione o tipo di supporto errato:** un processo è in fase di stampa e richiede il caricamento di alcuni documenti in un vassoio.
  - Dimensioni busta errate
  - Alimentazione manuale errata
  - Supporto errato
  - Dimensioni supporto errate
  - Carica supporti
- **Memoria piena o errore:** la memoria della stampante è quasi esaurita ed è necessario applicare delle modifiche.
  - Pagina complessa
  - I file verranno eliminati
  - Memoria insufficiente per fascicolazione
  - Memoria deframmentazione insufficiente
  - Memoria fax insufficiente
  - Memoria insufficiente
  - Memoria insufficiente - Possibile perdita processi in attesa
  - Memoria insufficiente per la funzione Salva risorse
  - Memoria piena



- Memoria PS insufficiente
- Scanner: Troppe pagine. Scansione annullata
- Riduzione risoluzione
- **Malfunzionamento opzione:** un'opzione collegata alla stampante è in stato di errore. Le opzioni comprendono opzioni di input, opzioni di stampa, schede font, schede di memoria flash utente, dischi e fascicolatori.
  - Verifica allineamento/connessione
  - Verifica connessione unità fronte/retro
  - Verifica installazione fascicolatore/mailbox
  - Verifica alimentazione
  - Opzione danneggiata
  - Opzione difettosa
  - Scollega periferica
  - Avviso fronte/retro
  - Vassoio fronte/retro mancante
  - Adattatore di rete esterno assente
  - Avviso fascicolatore
  - Blocco o sportello fascicolatore aperto
  - Pannello carta fascicolatore aperto
  - Periferica fronte/retro non compatibile
  - Periferica di alimentazione non compatibile
  - Periferica di uscita non compatibile
  - Periferica sconosciuta non compatibile
  - Installazione opzione errata
  - Avviso alimentazione
  - Errore di configurazione alimentazione
  - Avviso opzione
  - Raccoglitore di uscita pieno
  - Raccoglitore di uscita quasi pieno
  - Errore di configurazione uscita
  - Opzione piena
  - Opzione mancante
  - Meccanismo di alimentazione carta mancante
  - Processi di stampa su opzione
  - Ricollega periferica
  - Ricollega periferica di uscita
  - Troppi vassoi di alimentazione installati
  - Troppe opzioni installate
  - Troppi vassoi di uscita installati
  - Vassoio mancante
  - Vassoio mancante durante accensione

- Errore di rilevamento vassoio
- Vassoio di alimentazione non calibrato
- Opzione non formattata
- Opzione non supportata
- Ricollega periferica di alimentazione
- **Inceppamento carta:** un documento è inceppato nella stampante e deve essere rimosso fisicamente.
  - Inceppamento carta interno
  - Avviso inceppamento
  - Inceppamento carta
- **Errore scanner:** problema relativo allo scanner.
  - Scanner: Cavo posteriore non collegato
  - Carrello scanner bloccato
  - Scanner: Pulire striscia di supporto/vetro superficie piana
  - Scanner: Disabilitato
  - Scanner: Coperchio superficie piana aperto
  - Scanner: Cavo anteriore non collegato
  - Scanner: Registrazione scanner non valida
- **Errore mat. consumo:** problema relativo a un materiale di consumo della stampante.
  - Materiale di consumo anomalo
  - Regione cartuccia non corrispondente
  - Materiale di consumo difettoso
  - Rullo di patinatura o unità di fusione mancante
  - Cartuccia sinistra non valida o mancante
  - Cartuccia destra non valida o mancante
  - Materiale di consumo non valido
  - Attivazione non riuscita
  - Avviso materiali di consumo
  - Inceppamento materiale di consumo
  - Materiale di consumo mancante
  - Maniglia di espulsione cartuccia di toner tirata
  - Cartuccia di toner non installata in modo corretto
  - Materiale di consumo non calibrato
  - Materiale di consumo senza licenza
  - Materiale di consumo non supportato
- **Materiali di consumo mancanti:** un materiale di consumo della stampante deve essere sostituito.
  - Alimentatore vuoto
  - Esaurito
  - Stampante pronta per manutenzione
  - Manutenzione programmata
  - Materiale di consumo vuoto

- Materiale di consumo pieno
- Materiale di consumo pieno o mancante

**Nota:** La stampante invia l'avviso sotto forma di errore o avvertenza. Se viene attivato uno di questi avvisi, l'azione associata si verifica due volte.

- **Materiali di consumo in esaurimento:** un materiale di consumo della stampante è in esaurimento.
  - Avviso preventivo
  - Primo basso
  - Alimentatore basso
  - In esaurimento
  - Quasi vuoto
  - Quasi basso
  - Materiale di consumo basso
  - Materiale di consumo quasi pieno
- **Condizione o avviso non classificato**
  - Errore di calibrazione colore
  - Errore trasmissione dati
  - Errore CRC motore
  - Avviso esterno
  - Connessione fax interrotta
  - Ventola bloccata
  - Esadecimale attivo
  - Inserire pagina fronte/retro e premere Vai
  - Avviso interno
  - Assistenza richiesta su adattatore di rete interno
  - Avviso unità logica
  - Offline
  - Prompt Fuori linea per avvertenza
  - Operazione non riuscita
  - Avviso intervento operatore
  - Errore pagina
  - Avviso porta
  - Errore di comunicazione porta
  - Porta disabilitata
  - risparmio energia
  - Spegnimento
  - Timeout processo PS
  - Timeout manuale PS
  - Installazione richiesta
  - Errore checksum SIMM
  - Calibrazione materiali di consumo
  - Rilevamento patch toner non riuscito

- Condizione di avviso sconosciuta
- Configurazione sconosciuta
- Condizione avviso scanner sconosciuta
- Utenti bloccati
- Notifica di avvertenza

## Gestione degli eventi

**1** Nel menu Stampanti, fare clic su **Eventi e azioni > Eventi**.

**2** Effettuare una delle seguenti operazioni:

### Modificare un evento

- a** Selezionare un evento, quindi fare clic su **Modifica**.
- b** Configurare le impostazioni.
- c** Fare clic su **Salva modifiche**.

### Elimina eventi

- a** Selezionare uno o più eventi.
- b** Fare clic su **Elimina**, quindi confermare l'eliminazione.

# Visualizzazione della cronologia e dello stato delle attività

## Panoramica

Le attività sono le attività di gestione delle stampanti eseguite in MVE, quali rilevamento delle stampanti, controllo e applicazione delle configurazioni. La pagina Stato mostra lo stato di tutte le attività attualmente in esecuzione e delle attività eseguite nelle ultime 72 ore. Le informazioni sulle attività attualmente in esecuzione sono inserite nel registro. Le attività anteriori a 72 ore si possono visualizzare solo come voci di registro singole nella pagina Registro e si possono ricercare utilizzando gli ID corrispondenti.

## Visualizzazione dello stato delle attività

Nel menu Attività, fare clic su **Stato**.

**Nota:** Lo stato dell'attività viene aggiornato in tempo reale.

## Interruzione delle attività

- 1 Nel menu Attività, fare clic su **Stato**.
- 2 Nella sezione Attività attualmente in esecuzione, selezionare una o più attività.
- 3 Fare clic su **Interrompi**.

## visualizzazione dei registri

- 1 Nel menu Attività, fare clic su **Registri**.
- 2 Selezionare le categorie e i tipo di attività o un intervallo di tempo.

**Note:**

- Utilizzare il campo di ricerca per cercare più ID attività. Utilizzare le virgole per separare più ID attività o un trattino per indicare un intervallo. Ad esempio, **11, 23, 30-35**.
- Per esportare i risultati di ricerca, fare clic su **Esporta su CSV**.

## Eliminazione dei registri

- 1 Nel menu Attività, fare clic su **Registro**.
- 2 Fare clic su **Elimina registro**, quindi selezionare una data.
- 3 Fare clic su **Elimina registro**.

## Esportazione dei registri

- 1** Nella cartella Attività , fare clic su **Registro**.
- 2** Selezionare le categorie e i tipo di attività o un intervallo di tempo.
- 3** Fare clic su **Esporta a CSV**.

# Programmazione delle attività

## Creazione di un programma

- 1 Nel menu Attività fare clic su **Programma > Crea**.
- 2 Nella sezione Impostazioni generali digitare un nome univoco per le attività programmate e la relativa descrizione.
- 3 Nella sezione Attività effettuare una delle seguenti operazioni:

### Programmare un controllo

- a Selezionare **Controllo**.
- b Selezionare una ricerca salvata.

### Programmare un controllo di conformità

- a Selezionare **Conformità**.
- b Selezionare una ricerca salvata.

### Programmare un controllo dello stato della stampante

- a Selezionare **Stato attuale**.
- b Selezionare una ricerca salvata.
- c Selezionare un'azione.

### Programmare una distribuzione di configurazione

- a Selezionare **Distribuisci file**.
- b Selezionare una ricerca salvata.
- c Selezionare il file, quindi scegliere il tipo di file.
- d Se necessario, selezionare un protocollo o metodo di distribuzione.

### Pianificare un rilevamento

- a Selezionare **Ricerca**.
- b Selezionare un profilo di ricerca.

### Programmare un'applicazione della configurazione

- a Selezionare **Applicazione**.
- b Selezionare una ricerca salvata.

### Pianificare una convalida del certificato

Selezionare **Convalida certificato**.

**Nota:** durante la convalida, MVE comunica con il server CA per scaricare la catena di certificati e l'elenco di revoche di certificati (CRL). Viene generato anche il certificato agente di registrazione. Questo certificato consente al server CA di considerare attendibile MVE.

### Programmare un'esportazione di visualizzazione

- a** Selezionare **Esporta visualizzazione**.
  - b** Selezionare una ricerca salvata.
  - c** Selezionare un modello di visualizzazione.
  - d** Digitare l'elenco di indirizzi e-mail in cui vengono inviati i file esportati.
- 4** Nella sezione Programma impostare la data, l'ora e la frequenza dell'attività.
- 5** Fare clic su **Crea attività programmata**.

## Gestione delle attività programmate

- 1** Nella cartella Attività , fare clic su **Pianifica**.
- 2** Effettuare una delle seguenti operazioni:

### Modificare un'attività programmata

- a** Selezionare un'attività, quindi fare clic su **Modifica**.
- b** Configurare le impostazioni.
- c** Fare clic su **Modifica attività programmata**.

**Nota:** Le informazioni su Ultima esecuzione vengono rimosse quando viene modificata un'attività programmata.

### Eliminare un'attività programmata

- a** Selezionare un'attività, quindi fare clic su **Elimina**.
- b** Fare clic su **Elimina attività programmata**.



# Esecuzione di altre attività amministrative

## Configurazione delle impostazioni generali

- 1 Fare clic su  nell'angolo superiore destro della pagina.
- 2 Fare clic su **Generale**, quindi selezionare un'origine di nome host.
  - **Stampante**: il sistema recupera il nome host dalla stampante.
  - **Ricerca DNS inversa**: il sistema recupera il nome host dalla tabella DNS utilizzando l'indirizzo IP.
- 3 Impostare la frequenza delle nuove registrazioni degli avvisi.

**Nota:** Quando si effettuano modifiche, come il riavvio o l'aggiornamento del firmware, le stampanti possono perdere lo stato di registrazione degli avvisi. MVE tenta di ripristinare automaticamente lo stato sull'intervallo successivo impostato nella frequenza della nuova registrazione degli avvisi.

- 4 Fare clic su **Salva modifiche**.

## Configurazione delle impostazioni e-mail

Abilitare la configurazione SMTP per consentire a MVE di inviare tramite e-mail i file di esportazione dei dati e le notifiche degli eventi.

- 1 Fare clic su  nell'angolo superiore destro della pagina.
- 2 Fare clic su **E-mail**, quindi selezionare **Abilita configurazione SMTP e-mail**.
- 3 Digitare la porta e il server di posta SMTP.
- 4 Selezionare la crittografia appropriata.

**Note:**

- Per la crittografia SSL, selezionare la porta 465.
- Per la crittografia TLS/STARTTLS, selezionare la porta 587.

- 5 Digitare l'indirizzo e-mail del mittente.
- 6 Se un utente deve effettuare l'accesso prima della comunicazione e-mail, selezionare **Connessione richiesta**, quindi digitare le credenziali dell'utente.
- 7 Fare clic su **Salva modifiche**.

## Aggiunta di una dichiarazione di responsabilità prima dell'accesso

È possibile configurare una dichiarazione di responsabilità per l'accesso che verrà visualizzata all'accesso degli utenti a una nuova sessione. Gli utenti devono accettare la dichiarazione di responsabilità per poter accedere a MVE.

- 1 Fare clic su  nell'angolo superiore destro della pagina.
- 2 Fare clic su **Dichiarazione di responsabilità**, quindi selezionare **Abilita dichiarazione di responsabilità prima dell'accesso**.
- 3 Digitare il testo della dichiarazione di responsabilità.
- 4 Fare clic su **Salva modifiche**.

## Firma del certificato MVE

SSL (Secure Socket Layer) o TLS (Transport Layer Security) è un protocollo di sicurezza che utilizza la crittografia e l'autenticazione del certificato per proteggere la comunicazione tra server e client. In MVE, viene utilizzato il protocollo TLS per proteggere le informazioni riservate condivise tra il server MVE e il browser Web. Le informazioni protette possono essere password della stampante, criteri di sicurezza, credenziali utente MVE o informazioni di autenticazione della stampante, come LDAP o Kerberos.

TLS permette al server MVE e al browser Web di crittografare i dati prima dell'invio, quindi di decrittografarli dopo la ricezione. SSL richiede inoltre al server di inviare al browser Web un certificato che dimostri l'identità del server. Questo certificato è autofirmato o firmato mediante un'autorità di certificazione (CA) attendibile di terze parti. Per impostazione predefinita, MVE è configurato per l'uso di un certificato autofirmato.

- 1 Scaricare la richiesta di firma del certificato.
  - a Fare clic su  nell'angolo superiore destro della pagina.
  - b Fare clic su **TLS > Download**.
  - c Selezionare **Richiesta di firma certificato**.
- 2 Utilizzare un'autorità di certificazione (CA) attendibile per firmare la richiesta di firma del certificato.
- 3 Installare il certificato firmato tramite CA.
  - a Fare clic su  nell'angolo superiore destro della pagina.
  - b Fare clic su **TLS > Installa certificato firmato**.
  - c Caricare il certificato firmato tramite CA, quindi fare clic su **Installa certificato**.
  - d Fare clic su **Riavvia servizio MVE**.

**Nota:** il riavvio del servizio MVE determina il riavvio del sistema, per cui il server potrebbe non essere disponibile per alcuni minuti. Prima di riavviare il servizio, assicurarsi che non vi siano attività in esecuzione.

## Rimozione di informazioni e riferimenti dell'utente

MVE è conforme alle normative sulla protezione dei dati enunciate nel Regolamento generale sulla protezione dei dati (General Data Protection Regulation, GDPR). MVE si può configurare in modo da applicare il diritto di essere dimenticati e rimuovere i dati personali dell'utente dal sistema.

### Rimozione di utenti

- 1 Fare clic su  nell'angolo superiore destro della pagina.
- 2 Fare clic su **Utente**, quindi selezionare uno o più utenti.
- 3 Fare clic su **Elimina** > **Elimina utenti**.

### Rimozione dei riferimenti dell'utente in LDAP

- 1 Fare clic su  nell'angolo superiore destro della pagina.
- 2 Fare clic su **LDAP**.
- 3 Rimuovere le informazioni relative all'utente nei filtri di ricerca e nelle impostazioni di binding.

### Rimozione dei riferimenti dell'utente dal server e-mail

- 1 Fare clic su  nell'angolo superiore destro della pagina.
- 2 Fare clic su **E-mail**.
- 3 Rimuovere le eventuali informazioni relative all'utente, ad esempio le credenziali utilizzate dall'utente per l'autenticazione sul server e-mail.

### Rimozione dei riferimenti dell'utente dai registri delle attività

Per ulteriori informazioni, vedere ["Eliminazione dei registri" a pagina 141](#).

### Rimozione dei riferimenti di un utente da una configurazione

- 1 Nel menu Configurazioni fare clic su **Tutte le configurazioni**.
- 2 Fare clic sul nome della configurazione.
- 3 Nella scheda Di base rimuovere eventuali valori correlati all'utente dalle impostazioni della stampante, con il nome del contatto e la posizione del contatto.

### Rimozione dei riferimenti dell'utente in un componente di protezione avanzata

- 1 Nel menu Configurazioni fare clic su **Tutti i componenti di protezione avanzata**.
- 2 Fare clic sul nome del componente.
- 3 Nella sezione Impostazioni di protezione avanzate, rimuovere i valori relativi all'utente.

### Rimozione dei riferimenti dell'utente dalle ricerche salvate

- 1 Nel menu Stampanti fare clic su **Ricerche salvate**.
- 2 Fare clic su una ricerca salvata.

- 
- 
- 3** Rimuovere le eventuali regole di ricerca che utilizzano valori relativi all'utente, come il nome del contatto e la posizione del contatto.

### **Rimozione dei riferimenti dell'utente nelle parole chiave**

- 1** Nel menu Stampanti fare clic su **Elenco stampanti**.
- 2** Annullamento dell'assegnazione di parole chiave correlate all'utente dalle stampanti.
- 3** Nel menu Stampanti fare clic su **Parole chiave**.
- 4** Rimuovere le parole chiave che utilizzano informazioni relative all'utente.

### **Rimozione dei riferimenti dell'utente in eventi e azioni**

- 1** Nel menu Stampanti fare clic su **Eventi e azioni**.
- 2** Rimuovere le eventuali azioni che contengono riferimenti e-mail agli utenti.

## Domande frequenti

### Domande frequenti su Markvision Enterprise

#### Perché non è possibile selezionare più stampanti nell'elenco dei modelli supportati durante la creazione di una configurazione?

Le impostazioni e i comandi di configurazione variano a seconda del modello di stampante.

#### Altri utenti possono accedere alle mie ricerche salvate?

Sì. Tutti gli utenti possono accedere alle ricerche salvate.

#### Dove è possibile trovare i file di registro?

I file del registro di installazione sono nella directory nascosta dell'utente che ha installato MVE. Ad esempio, **C:\Utenti\Administrator\AppData\Local\Temp\mveLexmark-install.log**.

È possibile trovare i file del registro dell'applicazione \*.log nella cartella **installation\_dir\Lexmark\Markvision Enterprise\tomcat\logs**, dove **installation\_dir** indica la cartella di installazione di MVE.

#### Qual è la differenza tra ricerca DNS inversa e nome host?

Un nome host è un nome univoco assegnato a una stampante in rete. A ciascun nome host corrisponde un indirizzo IP. La ricerca DNS inversa viene usata per determinare il nome host e il nome di dominio designato di un determinato indirizzo IP.

#### Dove è disponibile la ricerca DNS inversa in MVE?

La ricerca DNS inversa si trova nelle impostazioni generali. Per ulteriori informazioni, vedere ["Configurazione delle impostazioni generali" a pagina 145](#).

#### In che modo è possibile aggiungere manualmente regole a Windows Firewall?

Eseguire il prompt dei comandi come amministratore, quindi digitare quanto segue:

```
firewall add allowedprogram "installation_dir/Lexmark/Markvision  
Enterprise/tomcat/bin/tomcat9.exe" "Markvision Enterprise Tomcat"  
firewall add portopening UDP 9187 "Markvision Enterprise NPA UDP"  
firewall add portopening UDP 6100 "Markvision Enterprise LST UDP"
```

Dove **installation\_dir** indica la cartella di installazione di MVE.

## In che modo è possibile configurare MVE per utilizzare una porta diversa dalla 443?

1 Arrestare il servizio Markvision Enterprise.

a Aprire la finestra di dialogo Esegui, quindi digitare **services.msc**.

b Fare clic con il pulsante destro del mouse su **Markvision Enterprise**, quindi fare clic su **Arresta**.

2 Aprire il file **installation\_dir\Lexmark\Markvision Enterprise\tomcat\conf\server.xml**.

Dove **installation\_dir** indica la cartella di installazione di MVE.

3 Modificare il valore **Connector port** con quello di un'altra porta inutilizzata.

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEImplementation"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
compression="on" compressableMimeType="text/html,text/xml,text/plain,text/css,
text/javascript,application/javascript,application/json" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" enableLookups="false"
acceptCount="100" connectionTimeout="120000" disableUploadTimeout="true"
URIEncoding="UTF-8" server="Apache" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
sslProtocol="TLS" keystoreFile="C:/Program Files/Lexmark/Markvision Enterprise/
../mve_truststore.p12" keystorePass="markvision" keyAlias="mve" keyPass="markvision"
keystoreType="PKCS12" ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA"/>
```

4 Modificare il valore **redirectPort** sullo stesso numero di porta utilizzato come porta del connettore.

```
<Connector port="9788" maxHttpHeaderSize="16384" maxThreads="150" minSpareThreads="25"
enableLookups="false" redirectPort="443" acceptCount="100" connectionTimeout="120000"
disableUploadTimeout="true" compression="on" compressableMimeType="text/html,text/xml,
text/plain,text/css,text/javascript,application/javascript,application/json"
URIEncoding="UTF-8" server="Apache"/>
```

5 Riavviare il servizio Markvision Enterprise.

a Aprire la finestra di dialogo Esegui, quindi digitare **services.msc**.

b Fare clic con il pulsante destro del mouse su **Markvision Enterprise**, quindi fare clic su **Riavvia**.

6 Accedere a MVE utilizzando la nuova porta.

Ad esempio, aprire un browser Web e digitare **https://MVE\_SERVER:port/mve**.

Dove **MVE\_SERVER** è il nome host o l'indirizzo IP del server su cui è installato MVE e **port** è il numero di porta del connettore.

## In che modo è possibile personalizzare le crittografie e le versioni TLS utilizzate da MVE?

1 Arrestare il servizio Markvision Enterprise.

a Aprire la finestra di dialogo Esegui, quindi digitare **services.msc**.

b Fare clic con il pulsante destro del mouse su **Markvision Enterprise**, quindi fare clic su **Arresta**.

2 Aprire il file **installation\_dir\Lexmark\Markvision Enterprise\tomcat\conf\server.xml**.

Dove **installation\_dir** indica la cartella di installazione di MVE.

### 3 Configurare le crittografie e le versioni TLS.

Per ulteriori informazioni sulla configurazione, vedere le [istruzioni di configurazione di Apache Tomcat SSL/TLS](#).

Per ulteriori informazioni sui protocolli e i valori delle crittografie, vedere la [documentazione relativa alle informazioni di supporto di Apache Tomcat SSL](#).

### 4 Riavviare il servizio Markvision Enterprise.

- a Aprire la finestra di dialogo Esegui, quindi digitare **services.msc**.
- b Fare clic con il pulsante destro del mouse su **Markvision Enterprise**, quindi fare clic su **Riavvia**.

## Come si gestiscono i file CRL quando si utilizza una CA Microsoft Enterprise?

### 1 Ottenere il file CRL dal server CA.

#### Note:

- Per la CA Microsoft Enterprise, il CRL non viene scaricato automaticamente tramite SCEP.
- Per ulteriori informazioni, vedere la *Guida alla configurazione dell'autorità di certificazione Microsoft*.

### 2 Salvare il file CRL nella cartella installation\_dir Lexmark/Markvision Enterprise/apps/library/crl, dove **installation\_dir** è la cartella di installazione di MVE.

### 3 Configurare l'autorità di certificazione in MVE.

**Nota:** Questo processo è applicabile solo al protocollo SCEP.

## Risoluzione dei problemi

### L'utente ha dimenticato la password

#### Reimpostare la password utente

È necessario disporre dei privilegi di amministratore per reimpostare la password.

- 1 Fare clic su  nell'angolo superiore destro della pagina.
- 2 Fare clic su **Utente**, quindi selezionare un utente.
- 3 Fare clic su **Modifica**, quindi modificare la password.
- 4 Fare clic su **Salva modifiche**.

Se si è dimenticata la password, effettuare una delle seguenti operazioni:

- Contattare un altro utente amministratore per reimpostare la password.
- Contattare il Centro di assistenza clienti Lexmark.

### L'utente amministratore ha dimenticato la password

#### Creare un altro utente amministratore, quindi eliminare l'account precedente

È possibile utilizzare Markvision Enterprise Password Utility per creare un altro utente amministratore.

- 1 Selezionare la cartella in cui è installato Markvision Enterprise.  
Ad esempio, **C:\Programmi\**
- 2 Avviare il file **mvepwdutility-windows.exe** nella cartella Lexmark\Markvision Enterprise\.
- 3 Selezionare una lingua, quindi fare clic su **OK > Avanti**.
- 4 Selezionare **Aggiungi account utente > Avanti**.
- 5 Immettere le credenziali utente.
- 6 Fare clic su **Avanti**.
- 7 Accedere a MVE, quindi eliminare il precedente utente amministratore.

**Nota:** Per ulteriori informazioni, vedere ["Gestione degli utenti" a pagina 30](#).



## La pagina non viene caricata

Questo problema può verificarsi se il browser Web è stato chiuso senza disconnettersi.

Provare una o più di una delle seguenti soluzioni:

**Cancellare la cache ed eliminare i cookie nel browser Web**

**Andare alla pagina di accesso a MVE, quindi effettuare l'accesso utilizzando le proprie credenziali**

Aprire un browser Web e digitare **`https://MVE_SERVER/mve/login`**, in cui **`MVE_SERVER`** corrisponde al nome host o all'indirizzo IP del server che ospita MVE.

## Impossibile rilevare una stampante di rete

Provare una o più delle seguenti soluzioni:

**Verificare che la stampante sia accesa.**

**Assicurarsi che il cavo di alimentazione sia collegato saldamente alla stampante e a una presa elettrica dotata di messa a terra.**

**Verificare che la stampante sia collegata alla rete**

**Riavviare la stampante**

**Accertarsi che il protocollo TCP/IP sia abilitato sulla stampante**

**Accertarsi che le porte utilizzate da MVE siano aperte e che i protocolli SNMP e mDNS siano abilitati**

Per ulteriori informazioni, vedere ["Informazioni su porte e protocolli" a pagina 158](#).

**Contattare il rappresentante Lexmark**

## Informazioni stampante errate

**Eseguire un controllo**

Per ulteriori informazioni, vedere ["Controllo delle stampanti" a pagina 61](#).

## MVE non riconosce una stampante come stampante protetta

### Come verificare che la stampante sia protetta

Per ulteriori informazioni sulla protezione delle stampanti, consultare il documento *MarkVision Enterprise e protezione della stampante*.

### Come accertarsi che mDNS sia attivato e che non si sia bloccato

### Come eliminare la stampante, quindi eseguire di nuovo la ricerca della stampante

Per ulteriori informazioni, vedere ["Rilevamento delle stampanti" a pagina 34](#).

## L'applicazione di configurazioni con più applicazioni non riesce al primo tentativo ma riesce con i tentativi successivi

### Aumentare il timeout

- 1 Selezionare la cartella in cui è installato Markvision Enterprise.

Ad esempio, **C:\Programmi\**

- 2 Passare alla cartella Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes.

- 3 Utilizzando un editor di testo, aprire il file *platform.properties*.

- 4 Modificare il valore **cdcl.ws.readTimeout**.

**Nota:** Il valore è espresso in millisecondi. Ad esempio, 90000 millisecondi è pari a 90 secondi.

- 5 Utilizzando un editor di testo, aprire il file *devCom.properties*.

- 6 Modificare i valori **1st.responseTimeoutsRetries**.

**Nota:** Il valore è espresso in millisecondi. Ad esempio, 10000 millisecondi è pari a 10 secondi.

Ad esempio, **1st.responseTimeoutsRetries=10000 15000 20000**. Il primo tentativo di riconnessione avviene dopo 10 secondi, il secondo tentativo di riconnessione avviene dopo 15 secondi e il terzo dopo 20 secondi.

- 7 Se necessario, quando si utilizza LDAP GSSAPI, creare un file *parameters.properties*.

Aggiungere l'impostazione seguente: **1st.negotiation.timeout=400**

**Nota:** Il valore è espresso in secondi.

- 8 Salvare le modifiche.

## L'applicazione di configurazioni con il certificato della stampante non riesce

A volte non viene rilasciato alcun nuovo certificato durante l'applicazione.

### Aumentare il numero di tentativi di registrazione

Aggiungere la seguente chiave nel file **platform.properties**:

```
enrol.maxEnrolmentRetry=10
```

Il valore dei tentativi deve essere maggiore di cinque.

## Autorità di certificazione OpenXPki

### Rilascio del certificato non riuscito con il server OpenXPki CA

**Assicurarsi che la chiave del "firmatario per conto di" in MVE corrisponda alla chiave del firmatario autorizzato nel server CA**

Ad esempio:

Se la seguente è la chiave **ca.onBehalf.cn** nel file **platform.properties** in MVE,

```
ca.onBehalf.cn=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

la seguente deve essere la chiave **authorized\_signer** nel file **generic.yaml** nel server CA.

```
rule1:
    # Full DN
    Subject: CN=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

Per ulteriori informazioni sulla configurazione del server OpenXPki CA, consultare la *Guida alla configurazione dell'autorità di certificazione OpenXPki*.

### Si verifica un errore interno del server

#### Installare le impostazioni locali en\_US.utf8

- 1 Eseguire il comando **dpkg-reconfigure locales**.
- 2 Installare le impostazioni locali **en\_US.utf8** (locale -a | grep en\_US).

## La richiesta di accesso non viene visualizzata

Quando si accede a **http://yourhost/openxpki/**, viene visualizzato solo il banner Open Source TrustCenter, senza una richiesta di accesso.

### Abilitare `fcgid`

Eeguire questi comandi:

- 1 `a2enmod fcgid`
- 2 `service apache2 restart`

## Si verifica un errore di connettore nidificato senza classe

Viene visualizzato un errore **EXCEPTION: Nested connector without class (scep.scep-server-1.connector.initial)** alla riga 201 di `/usr/share/perl5/Connector/Multi.pm`.

### Aggiornare `scep.scep-server-1`

In `/etc/openxpki/config.d/realm/REALM/scep/general.yaml`, sostituire `scep.scep-server-1` con `scep.generic`.

**Nota:** sostituire **REALM** con il nome dell'area di autenticazione. Ad esempio, quando si utilizza l'area di autenticazione predefinita, utilizzare **ca-one**.

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
```

## Impossibile approvare manualmente i certificati

Il pulsante Approvazione manuale non viene visualizzato quando si approvano manualmente i certificati.

### Aggiornare `scep.scep-server-1`

In `/etc/openxpki/config.d/realm/REALM/scep/general.yaml`, sostituire `scep.scep-server-1` con `scep.generic`.

**Nota:** sostituire **REALM** con il nome dell'area di autenticazione. Ad esempio, quando si utilizza l'area di autenticazione predefinita, utilizzare **ca-one**.

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
```

## Si verifica un errore Perl durante l'approvazione delle richieste di registrazione

### Aggiornare `scep.scep-server-1`

In `/etc/openxpki/config.d/realm/REALM/scep/general.yaml`, sostituire `scep.scep-server-1` con `scep.generic`.

**Nota:** sostituire **REALM** con il nome dell'area di autenticazione. Ad esempio, quando si utilizza l'area di autenticazione predefinita, utilizzare **ca-one**.

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
```

## I token **ca-signer-1** e **vault-1** sono offline

Nella pagina Stato sistema risulta che i token **ca-signer-1** e **vault-1** sono offline.

Provare una o più delle soluzioni seguenti

### Modificare la password della chiave del certificato

In `/etc/openxpki/config.d/realm/ca-one/crypto.yaml`, modificare la password della chiave del certificato.

### Creare collegamenti simbolici corretti e copiare il file della chiave

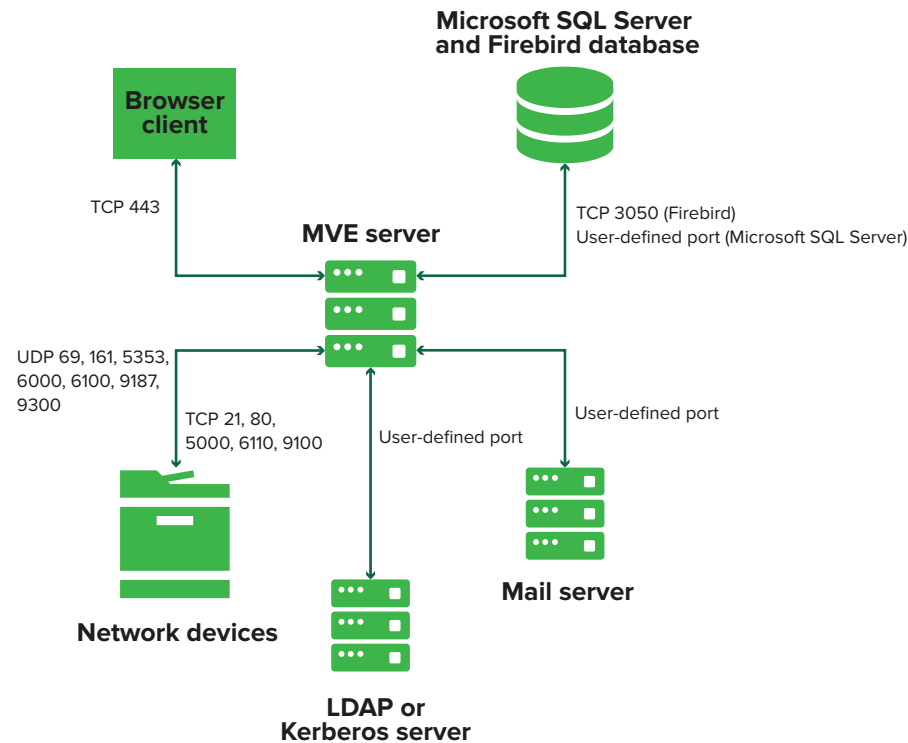
Per ulteriori informazioni, vedere ["Copia del file di chiave e creazione di un collegamento simbolico" a pagina 106](#).

### Assicurarsi che il file della chiave sia leggibile per OpenXPki

# Appendice

## Informazioni su porte e protocolli

MVE utilizza diversi protocolli e porte per i vari tipi di comunicazione di rete, come mostrato nel diagramma seguente:



**Note:**

- Le porte sono bidirezionali e devono essere aperte o attive affinché MVE funzioni correttamente. Assicurarsi che tutte le porte della stampante siano attivate.
- Alcune comunicazioni richiedono una porta temporanea, cioè un intervallo assegnato delle porte disponibili sul server. Quando un client richiede una sessione di comunicazione temporanea, il server assegna una porta dinamica al client. La porta è valida solo per una durata breve e può diventare disponibile per il riutilizzo alla scadenza della sessione precedente.

## Comunicazione da server a stampante

### Protocolli e porte utilizzati per le comunicazioni dal server MVE alle stampanti di rete

| Protocollo                                       | Server MVE | Stampante | Utilizzato per                                      |
|--------------------------------------------------|------------|-----------|-----------------------------------------------------|
| <b>NPAP (Network Printing Alliance Protocol)</b> | UDP 9187   | UDP 9300  | Comunicazioni con le stampanti di rete Lexmark.     |
| <b>XMLNT (XML Network Transport)</b>             | UDP 9187   | UDP 6000  | Comunicazioni con alcune stampanti di rete Lexmark. |

| Protocollo                                          | Server MVE                                                                     | Stampante                          | Utilizzato per                                                                                                                                                                                                             |
|-----------------------------------------------------|--------------------------------------------------------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LST (Lexmark Secure Transport)</b>               | UDP 6100<br>Porta TCP (Transmission Control Protocol) temporanea (handshaking) | UDP 6100<br>TCP 6110 (handshaking) | Comunicazioni protette con alcune stampanti di rete Lexmark.                                                                                                                                                               |
| <b>mDNS (Multicast Domain Name System)</b>          | Porta UDP (User Datagram Protocol) temporanea                                  | UDP 5353                           | Rilevamento delle stampanti di rete Lexmark e identificazione delle funzionalità di protezione delle stampanti.<br><b>Nota:</b> Questa porta è richiesta per consentire la comunicazione di MVE con le stampanti protette. |
| <b>SNMP (Simple Network Management Protocol)</b>    | Porta UDP temporanea                                                           | UDP 161                            | Rilevamento e comunicazione con le stampanti di rete Lexmark e di terze parti.                                                                                                                                             |
| <b>FTP (File Transfer Protocol)</b>                 | Porta TCP temporanea                                                           | TCP 21<br>TCP 20                   | Distribuzione dei file.                                                                                                                                                                                                    |
| <b>HTTP (Hypertext Transfer Protocol)</b>           | Porta TCP temporanea                                                           | TCP 80                             | Distribuzione dei file o applicazione delle configurazioni.                                                                                                                                                                |
|                                                     |                                                                                | TCP 443                            | Distribuzione dei file o applicazione delle configurazioni.                                                                                                                                                                |
| <b>HTTPS (Hypertext Transfer Protocol over SSL)</b> | Porta TCP temporanea                                                           | TCP 161<br>TCP 443                 | Distribuzione dei file o applicazione delle configurazioni.                                                                                                                                                                |
| <b>RAW</b>                                          | Porta TCP temporanea                                                           | TCP 9100                           | Distribuzione dei file o applicazione delle configurazioni.                                                                                                                                                                |

## Comunicazione da stampante a server

La porta e il protocollo utilizzati per le comunicazioni dalle stampanti di rete al server MVE

| Protocollo  | Stampante | Server MVE | Utilizzato per                  |
|-------------|-----------|------------|---------------------------------|
| <b>NPAP</b> | UDP 9300  | UDP 9187   | Creazione e ricezione di avvisi |

## Comunicazioni da server a database

Porte utilizzate durante la comunicazione dal server MVE ai database

| Server MVE                  | Database                                                     | Utilizzato per                            |
|-----------------------------|--------------------------------------------------------------|-------------------------------------------|
| <b>Porta TCP temporanea</b> | Porta definita dall'utente. La porta predefinita è TCP 1433. | Comunicazioni con un database SQL Server. |
| <b>Porta TCP temporanea</b> | TCP 3050                                                     | Comunicazioni con un database Firebird.   |

## Comunicazioni da client a server

La porta e il protocollo utilizzati per le comunicazioni dal client del browser al server MVE

| Protocollo                                   | Client browser | Server MVE |
|----------------------------------------------|----------------|------------|
| HTTPs (Hypertext Transfer Protocol over SSL) | Porta TCP      | TCP 443    |

## Comunicazione da server a server di posta

Porta e protocollo utilizzati per le comunicazioni dal server MVE a un server di posta

| Protocollo                           | Server MVE           | Server SMTP                                                | Utilizzato per                                                                     |
|--------------------------------------|----------------------|------------------------------------------------------------|------------------------------------------------------------------------------------|
| SMTP (Simple Mail Transfer Protocol) | Porta TCP temporanea | Porta definita dall'utente. La porta predefinita è TCP 25. | Fornire la funzionalità e-mail utilizzata per ricevere gli avvisi dalle stampanti. |

## Comunicazione da server a server LDAP

Le porte e i protocolli utilizzati per le comunicazioni dal server MVE a un server LDAP che interessano i gruppi utente e la funzionalità di autenticazione

| Protocollo                                             | Server MVE           | Server LDAP                                                 | Utilizzato per                                                 |
|--------------------------------------------------------|----------------------|-------------------------------------------------------------|----------------------------------------------------------------|
| LDAP (Lightweight Directory Access Protocol)           | Porta TCP temporanea | Porta definita dall'utente. La porta predefinita è TCP 389. | Autenticazione degli utenti MVE tramite un server LDAP.        |
| LDAPS (Lightweight Directory Access Protocol over TLS) | Porta TCP temporanea | Porta definita dall'utente. La porta predefinita è TCP 636. | Autenticazione degli utenti MVE tramite un server LDAP su TLS. |
| Kerberos                                               | Porta UDP temporanea | Porta definita dall'utente. La porta predefinita è UDP 88.  | Autenticazione degli utenti MVE tramite Kerberos.              |

## Abilitazione dell'approvazione automatica delle richieste di certificato in CA Microsoft

Per impostazione predefinita, tutti i server CA sono in modalità di attesa ed è necessario approvare manualmente ogni richiesta di certificato firmato. Poiché questo metodo non è pratico per le richieste in blocco, abilitare l'approvazione automatica dei certificati firmati.

- 1 In Server Manager fare clic su **Strumenti > Autorità di certificazione**.
- 2 Nel pannello di sinistra, fare clic con il pulsante destro del mouse sulla CA, quindi scegliere **Proprietà > Modulo criterio**.
- 3 Nella scheda gestione delle richieste fare clic su **Utilizza le impostazioni contenute nel modello di certificato.**, quindi fare clic su **OK**.

**Nota:** se l'opzione **Imposta lo stato della richiesta certificato in modo che risulti in sospeso** è selezionata, è necessario approvare manualmente il certificato.

- 4 Riavviare il servizio CA.



## Revoca di certificati

**Nota:** prima di iniziare, assicurarsi che il server CA sia configurato per i CRL e che questi siano disponibili.

- 1** Sul server CA, aprire **Autorità di certificazione**.
- 2** Nel pannello di sinistra, espandere la CA, quindi fare clic su **Certificati emessi**.
- 3** Fare clic con il pulsante destro del mouse su un certificato da revocare, quindi scegliere **Tutte le attività > Revoca certificato**.
- 4** Selezionare un codice motivo e la data e l'ora della revoca, quindi fare clic su **Sì**.
- 5** Nel pannello di sinistra, fare clic con il pulsante destro del mouse su **Certificati revocati**, quindi scegliere **Tutte le attività > Pubblica**.

**Nota:** assicurarsi che il certificato revocato si trovi in Certificati revocati.

Il numero di serie del certificato revocato è riportato nel CRL.

# Avvertenze

## Nota sull'edizione

Settembre 2022

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

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

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

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

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

Per informazioni sui materiali di consumo e sui download, visitare il sito Web [www.lexmark.com](http://www.lexmark.com).

© 2017 Lexmark International, Inc.

**Tutti i diritti riservati.**

## Marchi

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

Windows, Microsoft, Microsoft Edge, PowerShell, SQL Server e Windows Server sono marchi del gruppo di società Microsoft.

Firebird è un marchio registrato di Firebird Foundation.

Google Chrome è un marchio di Google LLC.

Apple and Safari are registered trademarks of Apple Inc.

Java è un marchio registrato di Oracle e/o delle sue consociate.

Tutti gli altri marchi appartengono ai rispettivi proprietari.

## GOVERNMENT END USERS

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

## JmDNS License

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Arthur van Hoff

avh@strangeberry.com

Rick Blair

rickblair@mac.com

\*\* JmDNS

## Informazioni sulla licenza

È possibile visualizzare tutti gli avvisi sulla licenza relativi a questo prodotto nella cartella del programma.

## Glossario

|                                  |                                                                                                                                                                                                                                                                                                             |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>azione</b>                    | Una notifica e-mail o un'operazione della riga di comando. Le azioni assegnate agli eventi vengono attivate quando viene emesso un avviso della stampante.                                                                                                                                                  |
| <b>configurazione</b>            | Insieme di impostazioni che possono essere assegnate e applicate a una stampante o a un gruppo di modelli di stampante. All'interno di una configurazione, è possibile modificare le impostazioni della stampante e distribuire le applicazioni, le licenze, il firmware e i certificati CA alle stampanti. |
| <b>controllo</b>                 | Attività di raccolta dei dati della stampante, ad esempio lo stato della stampante, i materiali di consumo e le funzionalità.                                                                                                                                                                               |
| <b>evento</b>                    | Definisce le azioni eseguite quando sono attivi avvisi specifici.                                                                                                                                                                                                                                           |
| <b>impostazioni di variabili</b> | Una serie di impostazioni della stampante che contiene valori dinamici che possono essere integrati in una configurazione.                                                                                                                                                                                  |
| <b>parola chiave</b>             | Testo personalizzato assegnato alle stampanti che è possibile utilizzare per la ricerca di queste stampanti all'interno del sistema. Quando si filtra una ricerca utilizzando una parola chiave, vengono visualizzate solo le stampanti contrassegnate con la parola chiave.                                |
| <b>profilo di ricerca</b>        | Profilo che contiene una serie di parametri utilizzati per rilevare le stampanti su una rete. Può anche contenere configurazioni predefinite che possono essere assegnate e applicate automaticamente alle stampanti durante il rilevamento.                                                                |
| <b>stampante protetta</b>        | Stampante configurata per comunicare tramite un canale crittografato e che richiede l'autenticazione per l'accesso alle relative funzioni o applicazioni.                                                                                                                                                   |
| <b>token</b>                     | Identificatore che rappresenta i valori dei dati della stampante per le impostazioni delle variabili in una configurazione.                                                                                                                                                                                 |

# Indice

## A

- abilitazione dei certificati del "firmatario per conto di" 109
- abilitazione dell'approvazione automatica delle richieste di certificato in CA Microsoft 160
- abilitazione dell'approvazione automatica delle richieste di certificato in OpenXPki CA 109
- abilitazione dell'autenticazione di base 131
- abilitazione dell'autenticazione tramite server LDAP 31
- abilitazione del servizio SCEP 108
- abilitazione di più certificati attivi stesso soggetto 113
- accessibilità al CRL
  - configurazione 85, 108
- Accesso alle informazioni dell'autorità
  - configurazione 84
- accesso a MVE 23
- aggiornamento alla versione più recente di MVE 25
- aggiornamento del firmware delle stampanti 64
- aggiornamento dello stato della stampante 61
- aggiunta dell'EKU di autenticazione client nei certificati 114
- aggiunta di una declinazione di responsabilità prima dell'accesso 146
- AIA
  - configurazione 84
- annullamento dell'assegnazione delle configurazioni 62
- applicazione delle configurazioni 62
- applicazioni
  - disinstallazione 65
- approvazione automatica delle richieste di certificato
  - abilitazione in CA Microsoft 160
  - abilitazione in OpenXPki CA 109, 126

- assegnazione di configurazioni alle stampanti 62
- assegnazione di eventi alle stampanti 65
- assegnazione di una parola chiave 65
- attività
  - interruzione 141
- autenticazione
  - certificato client 91
  - integrata di Windows 90
  - nome utente e password 91
- autenticazione certificato client 91
- autenticazione di base
  - abilitazione 131
- autenticazione integrata di Windows 90
- autenticazione nome utente e password 91
- autorizzazioni
  - informazioni 58
- autorizzazioni stampa a colori
  - configurazione 73
- avvio di OpenXPki 107
- avvisi della stampante
  - informazioni 136
- azione
  - segnaposto 134
- azione e-mail 133
- azione registro eventi 133
- azioni
  - creazione 133
  - eliminazione 135
  - gestione 135
  - modifica 135
  - test 135

## B

- backup e ripristino del database 26
- barra di ricerca
  - filtraggio delle stampanti 46
- best practice 13
- browser Web supportati 15

## C

- CA Microsoft Enterprise
  - configurazione 149
- CA Microsoft Enterprise con NDES
  - configurazione 80, 82
- caricamento pagina continuo 153
- ca-signer-1 è offline
  - risoluzione dei problemi 157
- CDP
  - configurazione 84
- CEP
  - configurazione 92, 94, 97
  - installazione 92
- certificati
  - creazione 111, 129
  - importazione 106
  - revoca 115, 161
- certificati CA radice
  - creazione 104, 121
- certificati con lo stesso oggetto
  - abilitazione 130
- certificati del "firmatario per conto di"
  - abilitazione 109
- certificati del firmatario
  - creazione 104, 122, 129
- certificati della stampante
  - configurazione manuale 66
- certificati del vault
  - creazione 105, 122
- certificati SCEP
  - creazione 105
- certificati server LDAP
  - installazione 33
- certificati SSL
  - creazione 89
- certificato client 96
- certificato MVE
  - firma 146
- certificato Web
  - creazione 123
- CES
  - configurazione 93, 95, 98
  - installazione 92
- chiavi dei certificati
  - creazione di file di password 104, 121, 129

- clonazione di configurazioni
  - scenario di esempio 71
- collegamenti simbolici
  - creazione 106
- componente di protezione avanzata
  - creazione 72
- comunicazioni della stampante
  - protezione 59
- configurazione
  - conformità 63
  - creazione 68, 71
  - esportazione 74
  - importazione 74
- configurazione degli endpoint EST per più aree di autenticazione 128
- configurazione degli endpoint SCEP per più aree di autenticazione 112
- configurazione dei server del servizio Registrazione dispositivi di rete 85
- configurazione dei server NDES 85
- configurazione del database 19
- configurazione dell'accessibilità al CRL 85, 108
- configurazione dell'accesso utente, panoramica 29
- configurazione della CA Microsoft Enterprise con NDES
  - panoramica 80, 82
- configurazione della protezione della stampante 58
- configurazione delle autorizzazioni per la stampa a colori 73
- configurazione delle impostazioni Accesso alle informazioni dell'autorità 84
- configurazione delle impostazioni e-mail 145
- configurazione delle impostazioni generali 145
- configurazione delle impostazioni Punto di distribuzione CRL 84
- configurazione del server CA radice, panoramica 81
- configurazione del server CA subordinata, panoramica 83

- configurazione del server Web 123
- configurazione di CEP 92, 94, 97
- configurazione di CES 93, 95, 98
- configurazione di MVE per la gestione automatica dei certificati 78
- configurazione di OpenXPki CA mediante lo script predefinito 101, 118
- configurazione manuale dei certificati delle stampanti 66
- configurazione manuale di OpenXPki CA 102, 119
- configurazioni
  - annullamento dell'assegnazione 62
  - applicazione 62
  - assegnazione 62
  - gestione 68
- configurazioni predefinite 56
- conformità
  - verifica 63
- controlli di accesso alle funzioni informazioni 58
- Controllo conformità periferica gestione 38
- controllo della conformità della stampante con una configurazione 63
- controllo delle stampanti 61
- copia dei file di chiave 106
- copia dei profili di ricerca 36
- copia della directory 110, 127
- copia delle ricerche salvate 53
- copia di visualizzazioni 44
- creazione dei certificati 111
- creazione dei certificati CA radice 104
- creazione dei certificati del firmatario 104
- creazione dei certificati del vault 105
- creazione dei collegamenti simbolici 106
- creazione di certificati SCEP 105
- creazione di certificati SSL server CEP e CES 89
- creazione di file di configurazione OpenSSL 103
- creazione di file di password per le chiavi dei certificati 104, 129

- creazione di modelli di certificato 86, 90
- creazione di parole chiave 47
- creazione di un'azione 133
- creazione di una configurazione 68
- creazione di una configurazione da una stampante 71
- creazione di una ricerca salvata personalizzata 49
- creazione di un certificato client 96
- creazione di un componente di protezione avanzata da una stampante 72
- creazione di un evento 135
- creazione di un pacchetto di applicazioni 74
- creazione di un profilo di ricerca 34
- creazione di un programma 143
- credenziali
  - immissione 66
- crittografia AES256
  - configurazione 149
- crittografie
  - personalizzazione 149
- CRL
  - pubblicazione 115
- cronologia delle modifiche 8
- CSV
  - impostazioni di variabili 72

## D

- dashboard
  - accesso 38
- database
  - backup 26
  - impostazione 19
  - requisiti 15
  - ripristino 26
- database Firebird 19
- database supportati 15
- dati delle stampanti
  - esportazione 44
- declinazione di responsabilità per l'accesso
  - aggiunta 146
- delega
  - abilitazione 91
  - requisiti 91

directory  
  copia e impostazione 127  
disabilitazione della Password di  
verifica nel server CA  
Microsoft 87  
disinstallazione delle applicazioni  
dalle stampanti 65  
distribuzione dei file alle  
stampanti 63  
domande frequenti 132  
download di ca-certs  
  modifica dei dettagli per  
  l'abilitazione 127

## E

EKU di autenticazione client  
  aggiunta nei certificati 114  
elenco delle stampanti  
  visualizzazione 40  
eliminazione dei registri 141  
eliminazione di azioni 135  
eliminazione di parole chiave 47  
eliminazione di profili di  
ricerca 36  
eliminazione di  
  programmazioni 144  
eliminazione di ricerche  
salvate 53  
eliminazione di visualizzazioni 44  
Embedded Web Server  
  visualizzazione 61  
endpoint EST  
  configurazione per più aree di  
  autenticazione 128  
endpoint SCEP  
  configurazione per più aree di  
  autenticazione 112  
errore di connettore nidificato  
senza classe 156  
errore interno del server 155  
errore Perl 156  
esecuzione dei profili di  
ricerca 36  
esecuzione di una ricerca  
salvata 49  
esportazione dei registri 142  
esportazione di CSV  
  impostazioni di variabili 72  
esportazione di dati delle  
stampanti 44  
eventi  
  assegnazione 65

eliminazione 140  
gestione 140  
modifica 140  
evento  
  creazione 135

## F

FAQ 132  
file  
  distribuzione 63  
file di chiave  
  copia 106  
file di configurazione OpenSSL  
  creazione 103, 120  
file di password per le chiavi dei  
certificati  
  creazione 104, 121, 129  
file di registro  
  individuazione 149  
file di registro dell'applicazione  
  individuazione 149  
file di registro di installazione  
  individuazione 149  
filtraggio delle stampanti dalla  
barra di ricerca 46  
firma del certificato MVE 146  
firmware delle stampanti  
  aggiornamento 64  
funzione di gestione automatica  
dei certificati 76

## G

generazione delle informazioni  
del CRL 107  
gestione automatica dei  
certificati  
  configurazione 78  
gestione certificati 76  
gestione degli avvisi della  
stampante, panoramica 133  
gestione degli eventi 140  
gestione degli utenti 30  
gestione dei profili di ricerca 36  
gestione delle azioni 135  
gestione delle configurazioni 68  
gestione delle parole chiave 47  
gestione delle  
  programmazioni 144  
gestione delle ricerche  
salvate 53  
gestione delle visualizzazioni 44

## I

immissione delle credenziali per  
le stampanti protette 66  
importazione dei certificati 106  
importazione di CSV  
  impostazioni di variabili 72  
importazione di file nella libreria  
delle risorse 75  
importazione o esportazione di  
una configurazione 74  
impossibile approvare  
manualmente i certificati 156  
impossibile rilevare una  
stampante di rete 153  
impostazione dei modelli di  
certificato per il servizio  
Registrazione dispositivi di rete  
(NDES) 87  
impostazione dei numeri di porta  
predefiniti per OpenXPki CA 113  
impostazione della  
directory 110, 127  
impostazione dello stato della  
stampante 62  
impostazione di una  
visualizzazione predefinita 44  
impostazione MVE come utente  
RunAs 20  
impostazioni delle regole di  
ricerca  
  informazioni 50  
impostazioni del programma di  
installazione  
  modifica 28  
impostazioni di configurazione  
  versione stampabile 72  
impostazioni dinamiche  
  informazioni 72  
impostazioni di variabili  
  informazioni 72  
impostazioni e-mail  
  configurazione 145  
impostazioni generali  
  configurazione 145  
informazioni CRL  
  generazione 107, 125  
  pubblicazione 126  
informazioni relative alla  
stampante  
  visualizzazione 43

informazioni stampante errate 153  
informazioni sugli avvisi della stampante 136  
informazioni sugli stati del ciclo di vita delle stampanti 47  
informazioni sui ruoli utente 29  
informazioni sui segnaposto azione 134  
Informazioni sulla protezione della periferica gestione 38  
informazioni utente rimozione 147  
installazione dei certificati del server LDAP 33  
installazione di MVE 21  
installazione di MVE invisibile all'utente 21  
installazione di OpenXPki CA 99, 116  
installazione di server CA radice 81  
installazione di server CA subordinata 83  
installazione invisibile all'utente MVE 21  
interruzione delle attività 141

## L

l'applicazione di configurazioni con il certificato della stampante non riesce 155  
l'applicazione di configurazioni con più applicazioni non riesce al primo tentativo ma riesce con i tentativi successivi 154  
l'utente amministratore ha dimenticato la password 152  
l'utente ha dimenticato la password 152  
la richiesta di accesso non viene visualizzata 156  
libreria delle risorse importazione di file in 75  
lingua modifica 24  
lingue supportate 16  
lingue supportate 16

## M

Markvision Enterprise informazioni 12  
metodi di autenticazione 90  
Microsoft SQL Server 19  
modelli di certificato 90 creazione 86  
modelli di certificato per il servizio Registrazione dispositivi di rete (NDES) impostazione 87  
modelli di stampante supportati 16  
modelli supportati configurazione 149  
modifica della lingua 24  
modifica della password 24  
modifica della visualizzazione dell'elenco stampanti 46  
modifica delle impostazioni del programma di installazione dopo l'installazione 28  
modifica di azioni 135  
modifica di parole chiave 47  
modifica di profili di ricerca 36  
modifica di programmazioni 144  
modifica di ricerche salvate 53  
modifica di visualizzazioni 44  
monitoraggio delle stampanti 53  
MVE accesso 23  
aggiornamento 25  
installazione 21  
MVE, installazione invisibile all'utente 21  
MVE non riconosce una stampante come stampante protetta 154

## N

numeri di porta predefiniti impostazione per OpenXPki CA 113  
modifica per OpenXPki CA 130  
numeri di porta predefiniti per OpenXPki CA modifica 130

## O

OpenXPki avvio 107, 124

OpenXPki CA configurazione manuale 102, 119  
configurazione mediante lo script predefinito 101, 118  
installazione 99, 116

## P

pacchetto applicazioni creazione 74  
panoramica configurazione dell'accesso utente 29  
configurazione del server CA radice 81  
configurazione del server CA subordinata 83  
dashboard di protezione 38  
gestione degli avvisi della stampante 133  
gestione delle configurazioni 68  
Markvision Enterprise 12  
visualizzazione della cronologia e dello stato delle attività 141  
parola chiave assegnazione 65  
parole chiave creazione 47  
eliminazione 47  
gestione 47  
modifica 47  
password modifica 24  
reimpostazione 152  
password della chiave del certificato rendere disponibile per openXPki 124  
Password di verifica disabilitazione nel server CA Microsoft 87  
più certificati attivi con lo stesso oggetto abilitazione 130  
porte configurazione 149  
informazioni 158  
profili di ricerca copia 36  
eliminazione 36  
esecuzione 36



- gestione 36
- modifica 36
- profilo di ricerca
  - creazione 34
- programma
  - creazione 143
- programmazioni
  - eliminazione 144
  - gestione 144
  - modifica 144
- protezione delle comunicazioni della stampante nel parco dispositivi 59
- protezione delle stampanti 60
  - configurazione 58
- protezione delle stampanti mediante le configurazioni predefinite 56
- protocolli
  - informazioni 158
- pubblicazione del CRL 115
- Punto di distribuzione CRL
  - configurazione 84

## R

- recupero dei soggetti dei certificati completi quando si effettua la richiesta tramite SCEP 114
- registri
  - eliminazione 141
  - esportazione 142
  - visualizzazione 141
- regole di ricerca
  - operatori 50
  - parametri 50
- requisiti
  - connettività di rete 88
  - sistema 88
- requisiti del database 15
- requisiti del server Web 15
- requisiti di connettività 88
- requisiti di connettività di rete 88
- requisiti di delega 91
- requisiti di sistema 88
- requisiti di sistema dell'utente 15
- revoca di certificati 115, 161
- riavvio della stampante 61
- ricerca DNS inversa 149
- ricerca nome host
  - ricerca inversa 149

- ricerca salvata personalizzata
  - creazione 49
- ricerche salvate
  - accesso 149
  - copia 53
  - eliminazione 53
  - esecuzione 49
  - gestione 53
  - modifica 53
- richieste di certificati senza password di verifica
  - rifiuto in OpenXPki CA 113
- richieste di certificato in CA Microsoft
  - approvazione automatica 160
- richieste di certificato in OpenXPki CA
  - approvazione automatica 109, 126
- rifiuto delle richieste di certificati senza password di verifica in OpenXPki CA 113
- rilascio del certificato non riuscito con il server OpenXPki CA 155
- rilevamento delle stampanti 37
- rimozione di informazioni e riferimenti dell'utente 147
- rimozione di stampanti 67
- risoluzione dei problemi
  - caricamento pagina continuo 153
  - ca-signer-1 è offline 157
  - errore di connettore nidificato senza classe 156
  - errore interno del server 155
  - errore Perl 156
  - impossibile approvare manualmente i certificati 156
  - impossibile rilevare una stampante di rete 153
  - informazioni stampante errate 153
- l'applicazione di configurazioni con il certificato della stampante non riesce 155
- l'applicazione di configurazioni con più applicazioni non riesce al primo tentativo ma riesce con i tentativi successivi 154
- l'utente amministratore ha dimenticato la password 152

- l'utente ha dimenticato la password 152
- la richiesta di accesso non viene visualizzata 156
- MVE non riconosce una stampante come stampante protetta 154
- rilascio del certificato non riuscito con il server OpenXPki CA 155
- vault-1 è offline 157
- ruoli utente
  - informazioni 29

## S

- scenario di esempio per la clonazione di configurazioni 71
- segnaposto 133
- segnaposto azione
  - informazioni 134
- server CA radice
  - installazione 81
- server CA subordinata
  - installazione 83
- server CEP e CES
  - creazione di certificati SSL 89
- server del servizio Registrazione
- dispositivi di rete
  - configurazione 85
- server LDAP
  - abilitazione dell'autenticazione 31
- server NDES
  - configurazione 85
- server supportati 15
- server Web
  - impostazione 123
  - requisiti 15
- servizio SCEP
  - abilitazione 108
- Simple Certificate Enrollment Protocol
  - abilitazione 108
- sistema utente
  - requisiti 15
- sistemi operativi supportati 15
- soggetti dei certificati completi
  - richiesta tramite SCEP 114
- stampante
  - conformità 63
  - riavvio 61

- stampanti
  - controllo 61
  - distribuzione di file 63
  - eventi 65
  - filtraggio 46
  - protezione 56, 60
  - rilevamento 37
  - rimozione 67
- stampanti protette
  - autenticazione 66
- stati del ciclo di vita delle stampanti
  - informazioni 47
- stati di protezione della stampante
  - informazioni 55
- stato della stampante
  - impostazione 62
- stato delle attività
  - visualizzazione 141
- stato stampante
  - aggiornamento 61

## T

- test delle azioni 135

## U

- utente RunAs
  - impostazione 20
- utenti
  - aggiunta 30
  - eliminazione 30
  - gestione 30
  - modifica 30

## V

- vault-1 è offline
  - risoluzione dei problemi 157
- versioni TLS
  - personalizzazione 149
- visualizzazione dei registri 141
- visualizzazione dell'elenco delle stampanti
  - modifica 46
- visualizzazione dell'elenco stampanti 40
- visualizzazione della cronologia e dello stato delle attività, panoramica 141
- visualizzazione delle informazioni della stampante 43

- visualizzazione dello stato delle attività 141
- visualizzazione di Embedded Web Server della stampante 61
- visualizzazioni
  - copia 44
  - eliminazione 44
  - gestione 44
  - modifica 44

## W

- Windows Firewall
  - aggiunta di regole 149