Dell Data Protection | Dell Data Guardian per Mac

Guida dell'amministratore v1.2

GUID-5B8DE7B7-879F-45A4-88E0-732155904029

Messaggi di N.B., Attenzione e Avvertenza

N.B.: un messaggio N.B. (Nota Bene) indica informazioni importanti che contribuiscono a migliorare l'utilizzo del prodotto.

ATTENZIONE: Un messaggio di ATTENZIONE indica un danno potenziale all'hardware o la perdita di dati, e spiega come evitare il problema.

AVVERTENZA: Un messaggio di AVVERTENZA indica un rischio di danni materiali, lesioni personali o morte.

GUID-559E7DE2-5F31-4AF0-8A01-987470FAB58C

Guida dell'amministratore di Dell Data Guardian per Mac

2017 - 04

Rev. A01

Sommario

1 Introduzione a Dell Data Guardian per Mac....4
Panoramica....4
Contattare Dell ProSupport....4

2 Requisiti di Dell Data Guardian per Mac....6
Server....6
Hardware del client Mac....6
Sistemi operativi....6
Provider di archiviazione cloud....7

3 Attività di installazione di Data Guardian....8
Prerequisiti....8
Criteri....8
Attività di Dell Enterprise Server....8
Configurazione di Security Server per consentire i download dei client cloud....8
Consentire/Negare gli utenti presenti negli elenchi di accesso completo/degli utenti non consentiti....9
Cancellazione remota di un account di un membro del team di Dropbox for Business....11
Attività del client....12
Prerequisiti....12
Procedure consigliate....12
Client di installazione....12

4 Attivazione ed esperienza utente di Data Guardian....15
Attivazione dell'utente finale....15
Interfaccia utente....15
Evitare l'opzione Check out nel sito Web....16
Applicazione Preferenze....16
Sicurezza e altre considerazioni su Data Guardian e sui client di sincronizzazione cloud....18
Google Drive....18
OneDrive for Business....18
Feedback su questo prodotto....18

5 Attività di disinstallazione di Data Guardian....19
Prerequisiti....19
Disinstallazione di Data Guardian....19

6 Glossario....20

Introduzione a Dell Data Guardian per Mac

Questa guida fornisce le informazioni necessarie per amministrare il software del client cloud per Mac.

GUID-DC905DCF-89A3-4894-B120-B1ED63272AA5

Panoramica

Dell Data Guardian per Mac protegge i dati nei sistemi per la condivisione di file basati sul cloud. I computer Mac OS X con Data Guardian possono visualizzare, modificare e crittografare i file sui sistemi per la condivisione di file basati sul cloud per un'archiviazione sicura.

Data Guardian per Mac e Windows è in grado di aprire su un computer Mac i file crittografati con un computer Windows e viceversa.

Data Guardian per Mac è costituito dai seguenti componenti:

- Data Guardian:
  - **Crittografia cloud**: consente di proteggere i dati nei sistemi per la condivisione di file basati sul cloud come i file .xen.
  - **Documenti Office protetti**: consente di proteggere i documenti Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) nel cloud, visualizzando il nome del file originale e l'estensione. Se protetti, i file possono essere aperti solo tramite un client Data Guardian. Se il file viene aperto con un'altra applicazione, viene visualizzata una pagina di copertina indicante che il documento è protetto e in che modo un utente autorizzato può richiedere l'accesso al file crittografato.

    È possibile impostare criteri solo per la crittografia cloud o per entrambi i gruppi di criteri. Per ulteriori informazioni, vedere la *Guida dell'amministratore*.

    Data Guardian per Mac è progettato per la condivisione di file nei provider di crittografia cloud. Tuttavia, se vengono attivati i criteri "Documenti Office protetti" per Mac, si perderanno tutti i dati di controllo e tracciabilità se il file viene salvato dall'utente finale nel computer Mac locale. Se l'organizzazione richiede severi criteri di controllo e tracciabilità, deselezionare il criterio *Consenti attivazione di Data Guardian su Mac* per evitare l'attivazione di Data Guardian sui computer Mac.
- Security Server - Un componente del server Dell che gestisce Data Guardian per Mac. Security Server assicura che i dati siano protetti nel cloud, non importa con chi siano condivisi. Security Server impedisce anche ai dispositivi interni di trasmettere dati sensibili.
- Remote Management Console - Fornisce l'amministrazione centralizzata dei criteri di protezione, integrandosi con le directory aziendali esistenti e creando rapporti.

  Questi componenti Dell devono interagire perfettamente tra loro per fornire un ambiente sicuro senza compromettere l'esperienza dell'utente.

GUID-B47CD81A-486F-43A5-816B-86A247C276EA

Contattare Dell ProSupport

Per assistenza telefonica sui prodotti Dell Data Protection, chiamare il numero +1-877-459-7304, interno 4310039, 24h su 24, 7 giorni su 7.

Inoltre, il supporto online per i prodotti Dell Data Protection è disponibile all'indirizzo dell.com/support. L'assistenza online comprende driver, manuali, consulenze tecniche, FAQ e problemi emergenti.

Per i numeri di telefono esterni agli Stati Uniti, controllare Numeri di telefono internazionali di Dell ProSupport.

Requisiti di Dell Data Guardian per Mac

In questo capitolo sono specificati i requisiti hardware e software client. Prima di continuare con le attività di distribuzione, accertarsi che gli ambienti di distribuzione soddisfino i requisiti.

N.B.:
IPv6 non è supportato.

GUID-213663B0-B65F-4945-B2F1-5BEF78085BDF

Server

Data Guardian per Mac richiede che il client sia collegato a un Dell Enterprise Server o Dell Enterprise Server - VE v9.6 o versione successiva.

GUID-371FFDE5-7A34-4288-AA88-617E73C0F9A4

Hardware del client Mac

Nella tabella seguente, è elencato l'hardware supportato per il client Mac.

Hardware Mac

- Processore Intel Core 2 Duo, Core i3, Core i5, Core i7 o Xeon
- 2 GB RAM
- 10 GB di spazio libero su disco

GUID-3F5F6005-9FEE-46AE-8400-336215F15DB2

Sistemi operativi

Nella tabella seguente, sono elencati i sistemi operativi supportati.

Sistemi operativi Mac

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.3 e 10.12.4

Sistemi operativi Android

- 4.4-4.4.4 KitKat
- 5.0-5.1.1 Lollipop
- 6.0 - 6.0.1 Marshmallow
- 7.0 Nougat

Sistemi operativi iOS

- iOS 8.x
- iOS 9.x
- iOS 10.x - 10.3

GUID-C4B25B4F-15E5-42AF-9493-D09F2473A534

Provider di archiviazione cloud

In base alle impostazioni dei criteri, è possibile che nell'interfaccia di Dell Data Guardian vengano visualizzati i seguenti provider. Non è necessario che l'utente scarichi o installi il client di sincronizzazione cloud.

Provider di archiviazione cloud

- Dropbox
- Box
- Google Drive
- OneDrive
- OneDrive for Business

Attività di installazione di Data Guardian

GUID-168A1BC7-0DED-43F2-9A99-08FC43099963

Prerequisiti

Prima di eseguire queste attività, confermare quanto segue:

- Installare il server Dell e i suoi componenti. Consultare una delle sezioni seguenti:
  - *Guida alla migrazione e all'installazione di Enterprise Server*
  - *Guida introduttiva e all'installazione di Virtual Edition*
- Nella Remote Management Console, assegnare un appropriato ruolo di amministratore Dell.

GUID-D9C4A912-436F-415D-9499-BAE4F1B53233

Criteri

Per impostazione predefinita, Data Guardian crittografa i file degli utenti e invia gli eventi di controllo al DDP EE Server/VE Server. Ai fini del presente documento, entrambi i server sono indicati come "server Dell", a meno che non sia necessario indicare una versione specifica (ad esempio, se una procedura è diversa quando si utilizza Dell Enterprise Server - VE).

Se si desidera che gli eventi di controllo includano i dati di georilevazione, è necessario abilitare il Wi-Fi. Per ulteriori informazioni sulla georilevazione e sugli eventi di controllo, consultare la *Guida dell'amministratore*.

Per modificare il comportamento predefinito per ciascun provider di archiviazione cloud supportato, impostare il criterio *Provider di protezione di archiviazione cloud*. Se l'azienda preferisce un provider di archiviazione cloud specifico, impostare questo criterio su **Blocca** per altri provider. Per informazioni sui criteri, consultare la *Guida dell'amministratore*, disponibile nella Remote Management Console del server Dell.

N.B.:
L'opzione Ignora di questo criterio è per Windows. Se viene selezionato Ignora per Mac, viene visualizzato come Consenti all'utente finale.

GUID-EE401419-8E85-45A9-9775-2C16EEE3FDB0

Attività di Dell Enterprise Server

GUID-0E37A5B7-8FF3-4F1E-9A8E-AB49D649C05B

Configurazione di Security Server per consentire i download dei client cloud

DDP Enterprise Server

1 Nel DDP Enterprise Server, accedere a <directory di installazione di Security Server>\webapps\cloudweb\brand\dell\resources\
2 Aprire il file **messages.properties** con un editor di testo.
3 Verificare che le voci siano impostate come segue.
Per l'installazione **locale**:

download.deviceWin.mode=local

download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg

Per l'installazione **remota**:

```
download.deviceWin.mode=remote
```

```
download.deviceMac.remote.link=https://[NomeMacchina:IndirizzoIP]:[porta]/percorso/
nomefile.dmg
```

4 Salvare e chiudere i file.
5 Accedere alla <directory di installazione di Security Server> e creare una cartella di nome Download (Security Server\Download).
6 All'interno della cartella Download, creare una cartella CloudWeb (Security Server\Download\CloudWeb).
7 Aggiungere i programmi di installazione di Dell Data Guardian a questa cartella.

Virtual Edition: installazione manuale di una versione differente del client cloud

Non è necessaria alcuna azione per consentire agli utenti di scaricare il programma di installazione più recente di Dell Data Guardian. Il programma di installazione più recente è preinstallato nel VE Security Server.

Per installare manualmente una versione differente del programma di installazione di Data Guardian su VE Security Server, aggiornare il file message.properties.

1 Andare a:
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 Aprire il file **messages.properties** con un editor di testo.
Per l'installazione **locale**:

```
download.deviceWin.mode=local
```

```
download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg
```

Per l'installazione **remota**:

download.deviceWin.mode=remote

```
download.deviceMac.remote.link=https://[NomeMacchina:IndirizzoIP]:[porta]/percorso/
nomefile.dmg
```

3 Salvare e chiudere i file.
4 Copiare i file in /opt/dell/server/security-server/download/cloudweb.
5 Aggiungere i programmi di installazione di Data Guardian a questa cartella.

GUID-40291F18-814A-40EC-9D60-A185154BA6FC

Consentire/Negare gli utenti presenti negli elenchi di accesso completo/degli utenti non consentiti

Le voci degli elenchi di accesso completo e degli utenti non consentiti stabiliscono quali utenti sono autorizzati a registrarsi nel server Dell per l'utilizzo di Data Guardian.

Elenco accesso completo

L'elenco di accesso completo permette a utenti o gruppi di utenti specifici di registrarsi nel server Dell e utilizzare Data Guardian.

Gli utenti esterni devono essere inseriti nell'elenco di accesso completo per poter effettuare la registrazione. Seguono alcuni esempi per consentire agli utenti di registrarsi:

Tipo di utente	Immettere
Tutti gli indirizzi di posta elettronica del dominio organizzazione.com	`organization.com`
Un utente specifico	`jdoe@organization.com`
Tutti gli utenti Gmail	`gmail.com`

Elenco degli utenti non consentiti

L'elenco degli utenti non consentiti impedisce a utenti o gruppi di utenti specifici di eseguire la registrazione nel server Dell e di usare Data Guardian. Gli utenti corrispondenti agli indirizzi e-mail inclusi nell'elenco degli utenti non consentiti ricevono un messaggio in cui vengono informati che non possono registrarsi a Data Guardian.

N.B.:
Se un utente è già registrato, questo elenco **non** gli impedisce di usare Data Guardian.

È possibile usare l'elenco degli utenti non consentiti per escludere determinati utenti che appartengono ai gruppi approvati nell'elenco di accesso completo. Inoltre, è possibile includere interi domini nell'elenco degli utenti non consentiti per impedire la registrazione a chiunque utilizzi un indirizzo e-mail appartenente a tale dominio. Seguono alcuni esempi per impedire a un utente o a un gruppo di utenti di registrarsi nel server Dell:

Tipo di utente	Immettere
Tutti gli indirizzi di posta elettronica del dominio organizzazione.com	`organization.com`
Un utente specifico e quell'indirizzo di posta elettronica	`jdoe@organization.com`
Tutti gli utenti Gmail	`gmail.com`

Per modificare gli elenchi di accesso completo/degli utenti non consentiti, attenersi a queste istruzioni:

1. Nel riquadro sinistro della Remote Management Console, fare clic su **Gestione > Gestione utenti esterni**.
2. Fare clic su **Aggiungi**.
3. Selezionare Tipo di accesso per la registrazione:

   Lista nera: blocca la registrazione per un utente o un dominio. L'utente non è in grado di aprire un documento Office protetto o un file .xen.

   Elenco accesso completo: consente la registrazione e l'accesso ai file per un utente o un dominio. Se l'utente o il dominio è presente anche nella lista nera, l'accesso non viene autorizzato.
4. Nel campo Immetti dominio/indirizzo e-mail, immettere il dominio dell'utente per impostare l'accesso per l'intero dominio o l'indirizzo e-mail per impostare l'accesso solo per tale utente.
5. Fare clic su **Aggiungi**.

Per ulteriori informazioni sull'uso dell'elenco di accesso completo/lista nera, consultare la *Guida dell'amministratore*, accessibile dalla Remote Management Console del server Dell.

Un utente esterno può richiedere l'accesso da parte di un utente interno per la chiave di un file protetto. Se l'utente interno non è disponibile, è possibile utilizzare la Remote Management Console per approvare o negare l'accesso.

1 Selezionare **Gestione > Gestione richieste chiavi**.
2 Per ulteriori informazioni, selezionare **?** (Guida).

GUID-038F598E-1FF3-4FC8-A419-2F628C92F934

Cancellazione remota di un account di un membro del team di Dropbox for Business

Se l'azienda dispone di Dropbox for Business, è possibile rimuovere in remoto un membro del team dall'account aziendale di Dropbox for Business se, ad esempio, un utente lascia l'azienda. File e cartelle associati all'account di tale membro del team verranno rimossi da tutti i dispositivi utilizzati dall'account. Questa azione revoca l'accesso dell'utente a tali file.

Prerequisiti

N.B.:
Prima di eseguire questa operazione, è necessario effettuare il backup di qualsiasi file o cartella presente nell'account del membro del team, di cui l'azienda o altri membri del team Dropbox for Business potrebbero avere bisogno.

Solamente un amministratore Dropbox for Business può cancellare da remoto un account Dropbox for Business.

L'utente finale deve aver attivato Dell Data Guardian e averlo collegato a Dropbox for Business.

Registrarsi alla Remote Management Console

È necessaria la registrazione di un solo amministratore Dropbox for Business.

1 Nel riquadro sinistro della Remote Management Console, selezionare **Gestione** > **Gestione Dropbox**.
2 Nella pagina Dropbox for Business, fare clic su **Registra**.
Il browser apre il sito Dropbox for Business.
3 Se richiesto, accedere a Dropbox con il proprio account amministratore di Dropbox for Business.
4 Per consentire l'accesso a Dell Data Guardian, fare clic su **Consenti**.
Viene visualizzata una pagina di conferma che indica che l'autorizzazione di Dropbox è stata concessa a DDP Enterprise Server - VE.
5 Nella Remote Management Console, tornare a **Gestione** > **Gestione Dropbox** e fare clic su **Aggiorna**.
Viene visualizzato il nome dell'amministratore.

N.B.:
In genere la procedura consigliata è quella di non annullare la propria registrazione. Tuttavia, per revocare i privilegi dell'amministratore di Dropbox for Business per la rimozione dei membri dal team Dropbox for Business, fare clic su **Annulla registrazione**.

Cancellazione remota di un account di un membro del team

N.B.:
L'opzione Cancellazione remota è disponibile solamente per gli account dei membri del team Dropbox for Business registrati. Se un account utente non visualizza l'opzione Cancellazione remota, l'utente non è registrato a un account Dropbox for Business.

1 Nella Remote Management Console, scegliere **Popolamenti** > **Utenti** nel riquadro a sinistra.
2 Cercare l'utente specificato.

3 Accedere alla pagina **Dettagli utente**.

4 Nella colonna Comando, fare clic su **Cancellazione remota**.

Viene eseguita la cancellazione remota.

> **N.B.:**
> Prima di selezionare Cancellazione remota, è necessario effettuare il backup di qualsiasi file o cartella presente nell'account del membro del team, di cui l'azienda o altri membri del team Dropbox for Business potrebbero avere bisogno.

5 Alla richiesta di conferma di Cancellazione remota, fare clic su **Sì**.

La pagina Dettagli utente elenca la data in cui ha avuto luogo la cancellazione remota.

6 Nella pagina personale Membri console di amministrazione di Dropbox for Business, aggiornare l'elenco dei Membri del team.

L'utente viene rimosso dall'elenco. È possibile selezionare la scheda **Membri rimossi** per visualizzare gli utenti rimossi.

GUID-B495F3E1-6516-4DFC-9107-4AA52FE296AB

Attività del client

GUID-88098FA1-F419-45AD-A4BA-F5C30D04DDE3

Prerequisiti

- Verificare che i dispositivi di destinazione siano in grado di connettersi a:
  - https://nomesecurityserver.dominio.com:8443/cloudweb/register
  - https://nomesecurityserver.dominio.com:8443/cloudweb
- Verificare che l'utente che esegue l'installazione abbia un account amministratore locale per installare.
- Se si installa usando la riga di comando, verificare di essere in possesso del nome di dominio completo del Dell Security Server con cui gli utenti eseguiranno l'attivazione.

GUID-5A15F45E-2F97-4EB4-90CD-66CD73275BAB

Procedure consigliate

Durante la distribuzione, assicurarsi di seguire le procedure consigliate. Questo include, ma non è limitato a:

- Ambienti di testing controllati per i test iniziali
- Distribuzioni scaglionate agli utenti

GUID-CF4B86F3-DBAF-4834-B15B-8913EEA7289D

Client di installazione

Ora, gli utenti che erano stati aggiunti all'elenco degli utenti consentiti possono effettuare la registrazione alla pagina: https://nomesecurityserver.dominio.com:8443/cloudweb/register.

Dopo essersi registrato, l'utente riceve un'e-mail che lo indirizza alla pagina https://nomesecurityserver.dominio.com:8443/cloudweb per effettuare l'accesso e scaricare il client appropriato.

L'installazione del client Mac è opzionale per gli amministratori, poiché gli utenti finali in genere installano il client Mac autonomamente (dopo la registrazione) dalla pagina https://yoursecurityservername.domain.com:8443/cloudweb.

Tuttavia, è possibile installare il client Mac se l'organizzazione lo richiede. Installare il client di Data Guardian tramite l'interfaccia utente o la riga di comando, utilizzando qualsiasi tecnologia push a disposizione della propria organizzazione. Sono ancora richieste la registrazione e l'attivazione da parte dell'utente finale.

Aggiornamento da versioni precedenti di Cloud Edition

Se un'azienda dispone di una versione precedente di Cloud Edition ed effettua l'aggiornamento a Data Guardian, la versione precedente di Cloud Edition viene rimossa.

N.B.:
Se l'azienda effettua l'aggiornamento da Cloud Edition per Data Guardian, gli utenti devono autenticare e ricollegare Data Guardian con il proprio provider di archiviazione cloud. Per maggiori informazioni sull'autenticazione, consultare la Guida di Dell Data Guardian online.

Opzioni di installazione

Per installare/aggiornare il client, selezionare uno dei metodi seguenti:

- Installazione interattiva - Questo è il metodo più semplice per installare Data Guardian per Mac. Tuttavia, utilizzare questo metodo solo se si intende installare il client in un computer alla volta.

  Oppure

- Installazione dalla riga di comando - Per questo metodo di installazione avanzato, gli amministratori devono aver esperienza con la sintassi della riga di comando. Questo metodo può essere utilizzato per un'installazione tramite script, utilizzando file batch o qualsiasi altra tecnologia push a disposizione della propria organizzazione.

Installazione interattiva

1 Per il client di Data Guardian, individuare il programma di installazione in **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2 Utilizzare il file **.pkg** in DDPSL-Explorer-0.x.x.xxxx.dmg per l'installazione o l'aggiornamento. È possibile utilizzare un'installazione tramite script, file batch o qualsiasi altra tecnologia push a disposizione della propria organizzazione.
3 Fare doppio clic sul pacchetto **Dell-Data-Guardian-x.x.x**.
4 Fare clic su **Continua**.
5 Nella finestra Introduzione, fare clic su **Continua**.
6 Nella finestra Contratto di licenza software, fare clic su **Continua**.
7 Fare clic su **Accetto**per continuare.
8 Nella finestra Tipo di installazione, effettuare una delle seguenti operazioni:
   - Fare clic su **Installa**, quindi andare al passaggio 9.
   - Nella finestra di selezione della destinazione, selezionare un'opzione di seguito, fare clic su **Continua l'installazione**, quindi andare al passaggio 9.
     - Installa per tutti gli utenti di questo computer
     - Installa solo per me
9 Nella finestra di dialogo, immettere nome e password e fare clic su **Installa software**.
10 Nella finestra Riepilogo, fare clic su **Chiudi**.
11 Vedere Attivazione dell'utente finale.

N.B.:
Se l'azienda effettua l'aggiornamento da Cloud Edition per Data Guardian, gli utenti devono autenticare e ricollegare Data Guardian con il proprio provider di archiviazione cloud. Per maggiori informazioni sull'autenticazione, consultare la Guida di Dell Data Guardian online.

Installazione dalla riga di comando

1 Montare il file .dmg.
2 Eseguire un'installazione del pacchetto dalla riga di comando utilizzando il comando del programma di installazione:

```
sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -
target /
```

3 Indicare agli utenti finali di attivare Data Guardian. Vedere Attivazione dell'utente finale.

Attivazione ed esperienza utente di Data Guardian

GUID-FCD7AF63-06D4-4D0C-8FA3-369265AB00E2

Attivazione dell'utente finale

Dopo aver aperto Dell Data Guardian sul computer Mac per la prima volta, seguire questi passaggi:

1 Nel Finder, selezionare **Applicazioni**, e fare doppio clic su **Dell Data Guardian**.
2 Quando viene visualizzata la finestra del server Dell, immettere l'indirizzo del server DDP e fare clic su **Salva**.

   Si apre la finestra Credenziali.

3 Immettere l'indirizzo e-mail di dominio e la password di dominio.
4 Fare clic su **Accesso** per attivare Dell Data Guardian.

   Una volta aperta l'applicazione Dell Data Guardian e completata l'attivazione, il nome del provider di archiviazione cloud viene attivato nel riquadro sinistro.

   Se un'azienda desidera che tutti gli utenti collaborino utilizzando lo stesso provider di servizi cloud, l'amministratore può impostare un criterio per abilitare solo quel provider e bloccare la visualizzazione degli altri.

   Se l'attivazione non è stata completata o se l'autenticazione dell'applicazione Dell Data Guardian è stata revocata o è scaduta, il nome del provider di archiviazione cloud è disattivato.

5 Nel riquadro sinistro, selezionare il provider di archiviazione cloud.

   Si apre una finestra che richiede le credenziali dell'utente.
6 Per maggiori informazioni sull'autenticazione, consultare la Guida di Dell Data Guardian online.

GUID-9917238E-00E5-4F56-909D-C76F09426D53

Interfaccia utente

L'interfaccia di Dell Data Guardian è simile alla modalità di *visualizzazione in colonne* dell'applicazione Finder di OS X. Ogni colonna rappresenta una cartella nel provider di archiviazione cloud selezionato.

N.B.:
la barra del titolo può variare in base al sistema operativo.

Per crittografare e decrittografare i file è necessario utilizzare l'interfaccia di Dell Data Guardian, non il sito Web del provider di archiviazione cloud.

È possibile eseguire queste attività direttamente nella finestra di Dell Data Guardian:

- **File** > **Nuova cartella** - Per creare nuove cartelle.

N.B.:
Google Drive e OneDrive aggiungono automaticamente una cartella condivisa. Tuttavia, in OneDrive for Business la condivisione dei dati non è supportata.

- Menu di scelta rapida - Selezionare una o più cartelle o file nella finestra principale. Quindi, premere Control-clic (o fare clic con il pulsante destro del mouse) e selezionare un'opzione di menu:
  - **Scarica**
  - **Rinomina** - Quando si rinomina un file nell'interfaccia di Dell Data Guardian, Dell Data Guardian sincronizza la modifica sul sito Web del provider di archiviazione cloud. Non rinominare un file .xen nel sito Web del provider di archiviazione cloud. Non verrebbe sincronizzato.
  - **Elimina**

    N.B.:
    Google Drive con Data Guardian non dispone di un'opzione Rimuovi (Sposta nel cestino). Dispone solo dell'opzione Elimina, per coerenza con le altre funzionalità di Data Guardian.
- **Scollega** - Per scollegare Dell Data Guardian da un provider di archiviazione su cloud, selezionare il provider nel riquadro sinistro, premere il tasto Control e fare clic con il mouse (o fare clic con il pulsante destro del mouse), quindi selezionare Scollega dal menu.

Informazioni aggiuntive su file e cartelle:

- Per aggiungere file e cartelle alle cartelle mostrate nell'interfaccia utente di Dell Data Guardian, trascinarli da Finder di OS X o da altre applicazioni che supportano il trascinamento. I file verranno crittografati in base al criterio corrente.
- Per decrittografare e aprire i file nelle applicazioni, fare doppio clic sul file nella finestra di Dell Data Guardian. Se il file viene modificato in un'applicazione esterna, il file modificato verrà quindi crittografato e caricato come una nuova revisione nel provider di archiviazione cloud.
- Per creare una copia locale non crittografata, trascinare un file o una cartella dalla finestra di Dell Data Guardian in Finder.
- Data Guardian di *Data Guardian* non consente modifiche ai file senza estensione. Tali file vengono trattati come file di sola lettura. Per modificare un file senza estensione, scaricarlo dal sito Web del provider di archiviazione cloud, modificarlo, quindi caricarlo tramite l'interfaccia di Dell Data Guardian.
- Gli attributi estesi non vengono copiati nel cloud.

GUID-12385ECF-2D63-4BD1-8719-260F247D161E

Evitare l'opzione Check out nel sito Web

Data Guardian non protegge o crittografa i file utilizzati con l'opzione *Apri e check out* sul sito Web di OneDrive for Business o di qualsiasi provider di archiviazione cloud. Se un file viene aperto e ne viene effettuato il check out, non usare il comando Apri nell'interfaccia di Dell Data Guardian poiché il caricamento automatico verrà bloccato.

Quando si proteggono i file con Data Guardian, utilizzare Dell Data Guardian per lavorare con i file.

Se si desidera lavorare con un file che ha proprietà speciali dal sito Web di un provider di archiviazione cloud:

1 Nell'interfaccia di Dell Data Guardian, premere Ctrl+clic (o fare clic con il pulsante destro del mouse) su un file e selezionare **Download**.
2 Selezionare e modificare il file.
3 Tramite l'interfaccia di Dell Data Guardian, caricare il file.

GUID-B1BB3439-4C04-4F3A-AADA-DD5552F902D6

Applicazione Preferenze

Per avviare Preferenze:

1 Avviare Dell Data Guardian.
2 Dalla barra dei menu di Dell Data Guardian, selezionare **Preferenze**.

N.B.:
Queste informazioni sono disponibili anche dall'icona Guida.

È possibile modificare queste impostazioni:

- Nascondi i file che iniziano con " .": per impostazione predefinita, questa casella è selezionata, pertanto i file sono nascosti. Per visualizzare i file nascosti, deselezionare la casella di controllo.

  N.B.:
  Generalmente, i file preceduti da un separatore punto sono nascosti in OS X Finder.

- **Scollega il provider di archiviazione su cloud** - Qui sono indicati i provider di archiviazione cloud autenticati da Data Guardian. Per rimuovere un provider di archiviazione cloud da Data Guardian, selezionare il nome del provider e fare clic sul pulsante meno (-) in basso a sinistra della finestra Preferenze.

Criteri del server - L'amministratore del server DDP imposta i seguenti criteri che controllano il modo in cui Data Guardian gestisce file e cartelle:

- **Server DDP** - Qui è indicato l'URL del server.
- **Intervallo di polling** - Indica l'intervallo in minuti in cui il software client esegue il polling degli aggiornamenti dei criteri.
- **Crittografa** - Criterio di crittografia principale che consente la crittografia di file e cartelle sul sito Web di archiviazione su cloud.
- **Solo estensione** o **Offusca**

  Solo estensione (impostazione predefinita di criterio) visualizza il nome del file nel sito Web.

  Se un'azienda necessita di una protezione aggiuntiva per i file, impostare questo criterio su **Offusca** per nascondere i nomi dei file nel sito Web del cloud come nomi GUID.

  N.B.:
  Se il criterio viene inizialmente impostato su Solo estensione e gli utenti hanno dei file nel sito Web del cloud e successivamente il criterio viene modificato in Offuscamento, i nomi dei file preesistenti nel sito Web non verranno offuscati. Per offuscare i nomi dei file preesistenti, l'utente deve scaricare e poi ricaricare i file tramite l'interfaccia di Data Guardian. Oppure, se l'utente modifica un file, verrà ricaricato con un nome di file offuscato.

- **Documenti Office protetti**: consente di proteggere i documenti Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) nel cloud, visualizzando l'estensione del file, non un'estensione .xen.

  Se questo criterio è abilitato, i documenti Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) nel cloud visualizzano l'estensione del file, non un'estensione .xen. Tuttavia, il file non può essere aperto nel cloud o scaricato. Se viene aperto, viene visualizzata solo una pagina di copertina, che indica che il documento è protetto. Se è stato installato Data Guardian ma non è stata eseguita l'autenticazione, la pagina di copertina riporta questa informazione.
- **Eventi di controllo** - Se questa opzione è attivata, consente di inviare eventi di controllo al server Dell.
- **Posizione geografica** - Se questa opzione è attivata, gli eventi di controllo inviati al server Dell includono i dati sulla posizione geografica (latitudine e longitudine).
- **Beacon richiamata** - Se questa opzione è attivata, consente di inviare un beacon richiamata in ogni file Office protetto.
- **URL beacon richiamata** - Se questa opzione è attivata, specifica l'URL da utilizzare quando il beacon richiamata viene inserito in file protetti da Office.
- **Provider di protezione di archiviazione cloud** - Il nome del provider viene visualizzato in base alle impostazioni del criterio. Le opzioni sono **Box**/**Dropbox**/**Google Drive**/**OneDrive**/**OneDrive for Business**.

  Abilitare o disabilitare la crittografia di file caricati in quel provider di archiviazione cloud. Viene visualizzato uno tra i seguenti:

  - **Crittografa** - I file inviati al cloud sono crittografati.
  - **Consenti** - L'utente può accedere ai file nel cloud, ma i file inviati al sito Web di un provider di archiviazione cloud non sono crittografati.

- **Bloccato** - Il provider di archiviazione cloud non è disponibile e ciò significa che il nome corrispondente non viene visualizzato nella finestra principale.

GUID-74395D32-C5C3-46A5-A090-CE195AD5DCC0

Sicurezza e altre considerazioni su Data Guardian e sui client di sincronizzazione cloud

GUID-ED3DC4CF-B650-4583-83F3-84FE0288BBC3

Google Drive

Data Guardian di *Data Guardian* crittografa le cartelle e i file nel cloud per proteggere i dati. Tenere presenti le seguenti considerazioni.

- Il criterio di protezione aziendale, impostato su Proteggi, proibisce l'uso di documenti Google con Data Guardian. Se i criteri sono impostati su Consenti, è possibile modificarli. Per maggiori informazioni, contattare l'amministratore IT.

  Google Drive contiene l'app Documenti Google che permette agli utenti di collaborare sui documenti in tempo reale. Tuttavia, tale collaborazione avviene in un server Google e i file non sono crittografati. I Documenti Google creati vengono visualizzati nelle cartelle del provider di archiviazione cloud di Documenti Google dell'utente.

  Tuttavia, se si apre la cartella, una finestra di dialogo avvisa che Data Guardian non può crittografare tale documento.

GUID-5454F809-40A1-4609-BED2-7D3D06391FC4

OneDrive for Business

In OneDrive for Business la condivisione dei dati non è supportata.

GUID-A6AA7EB4-E62B-44A2-BAC2-902473A21C42

Feedback su questo prodotto

Se questa funzione è abilitata dal criterio, gli utenti possono fornire un feedback su Dell Data Guardian. Il modulo per commenti e suggerimenti è disponibile nella barra dei menu > **Fornisci un feedback su Dell Data Protection**.

Attività di disinstallazione di Data Guardian

In questa sezione, viene illustrata la procedura amministrativa per la disinstallazione di Data Guardian. Se dispone di un account amministratore locale, l'utente finale può eseguire la disinstallazione di Data Guardian per Mac autonomamente.

GUID-0AEC84CA-AADA-44B7-A403-5D8C97FFAFD5

Prerequisiti

Per eseguire la disinstallazione, è necessario disporre di un account amministratore locale.

GUID-C8A4F2ED-6FE8-4B26-A3FB-60795D070304

Disinstallazione di Data Guardian

Per rimuovere Data Guardian, effettuare una delle operazioni seguenti:

Finder

1 Mentre si preme il tasto <opzione>, selezionare **Vai** dalla barra dei menu.
2 Aprire la cartella **~/Library/Application Support/Dell**.
3 Rimuovere la cartella **DataGuardian**.
4 Selezionare **Vai** nella barra dei menu, aprire la cartella Applicazioni e rimuovere l'applicazione **Data Guardian**.

Terminale

È possibile avere Data Guardian in una o entrambe le posizioni seguenti.

1 Utilizzare uno o entrambi i comandi seguenti:
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Rimuovere la cartella **DataGuardian**.

Glossario

Attivare/Attivato - L'attivazione avviene quando il computer è stato registrato con il server Dell e ha ricevuto almeno un insieme iniziale di criteri.

Server Dell - Il server Dell è costituito da una raccolta di componenti. Quando si fa riferimento al lato server del prodotto nell'insieme, è collettivamente noto come server Dell.

Remote Management Console - La Remote Management Console è la console di amministrazione dell'intera distribuzione aziendale ed è un componente di Dell Enterprise Server.

Security Server - Un componente del server Dell che gestisce Dell Data Guardian. Security Server assicura che i dati siano protetti nel cloud, non importa con chi siano condivisi. Security Server impedisce anche ai dispositivi interni di trasmettere dati sensibili.

Utenti esterni - Utenti esterni all'indirizzo del dominio dell'organizzazione.