Dell Data Guardian

Manuale per l'utente v1.2

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.

Manuale per l'utente di Dell Data Guardian

2017 - 04

Rev. A01

Sommario

Introduzione a Dell Data Guardian

Il *Manuale per l'utente di Dell Data Guardian* fornisce le informazioni necessarie per installare e utilizzare Dell Data Guardian.

Panoramica

Dell Data Guardian protegge i dati in base ai criteri impostati da un amministratore, ad esempio:

- Sistemi di condivisione file basati su cloud - I computer Windows o i dispositivi mobili acquisiscono dati destinati all'archiviazione cloud, crittografano tali dati e quindi caricano i dati crittografati nel cloud.
- Documenti d'ufficio archiviati localmente, condivisi con altri utenti in vari modi o archiviati su supporti rimovibili. Questi documenti Office possono essere protetti: .docx, .pptx, .xlsx .docm, .pptm, .xlsm.

> **N.B.:**
> L'amministratore informerà l'utente se l'azienda utilizza Data Guardian solo con l'archiviazione cloud, solo con i documenti Office o con entrambi.

È possibile utilizzare Data Guardian sulle seguenti piattaforme:

- Windows
- iOS
- Android
- Questo prodotto è in grado di aprire i file crittografati da Data Guardian per Mac, e viceversa.
  - Questo documento descrive solo Dell Data Guardian per Windows.
  - Per informazioni su Dell Data Guardian per Mac, consultare la guida in linea all'interno del software.

Ulteriore assistenza

Per ottenere ulteriore assistenza dopo la lettura del presente documento, contattare l'amministratore.

2

Requisiti di Dell Data Guardian

In questo capitolo sono specificati i requisiti hardware e software client.

N.B.:
IPv6 non è supportato.

Server

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

Client di crittografia

- Durante la distribuzione è opportuno seguire le procedure consigliate. In queste procedure sono compresi, a titolo esemplificativo, ambienti di testing controllati per i test iniziali e distribuzioni scaglionate agli utenti.
- L'account utente che esegue l'installazione/l'aggiornamento/la disinstallazione deve essere un utente amministratore del dominio o locale, che può essere assegnato temporaneamente tramite uno strumento di distribuzione, ad esempio Microsoft SMS o Dell KACE. Non sono supportati gli utenti non amministratori con privilegi elevati.
- Prima di iniziare l'installazione/la disinstallazione, eseguire il backup di tutti i dati importanti.
- Durante l'installazione non apportare modifiche al computer, quali l'inserimento o la rimozione di unità esterne (USB).
- Pur non essendo necessario, qualsiasi client di crittografia utilizzato con Data Guardian deve essere della versione v8.12 o successiva.
- Data Guardian non è supportato da Microsoft Office 365.
- Per la crittografia cloud, il computer deve disporre di un'unità disco assegnabile (valore letterale).
- Verificare che i dispositivi di destinazione siano in grado di connettersi a https://yoursecurityservername.domain.com:8443/cloudweb/register e https://yoursecurityservername.domain.com:8443/cloudweb.
- Prima di distribuire Data Guardian, è consigliabile non configurare account di archiviazione cloud nei dispositivi di destinazione.

  Se gli utenti finali decidono di mantenere gli account esistenti, devono assicurarsi che i file che devono rimanere *decrittati* vengano rimossi dal client di sincronizzazione prima dell'installazione di Data Guardian.
- Gli utenti dovranno riavviare il computer al termine dell'installazione del client.
- Data Guardian non interferisce con il comportamento dei client di sincronizzazione. Prima di distribuire Data Guardian, gli amministratori e gli utenti finali dovranno pertanto familiarizzare con le modalità di funzionamento di queste applicazioni. Per maggiori informazioni, consultare il supporto di Box all'indirizzo https://support.box.com/home, il supporto di Dropbox all'indirizzo https://www.dropbox.com/help o il supporto di OneDrive all'indirizzo http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Se si utilizza Office 2010: se sono stati configurati criteri per proteggere i documenti Office e i documenti con attivazione macro, gli utenti devono disporre di Office 2010 Service Pack 1 o versioni successive (v14.0.6029 o versioni successive). Vedere https://support.microsoft.com/en-us/kb/2121559 per determinare se è stato applicato un Service Pack alla suite Microsoft Office 2010. Senza questo aggiornamento, i documenti protetti non sono accessibili. I nuovi documenti Office non sono protetti, a prescindere dal criterio attivo, a meno che non sia abilitata la funzionalità di scansione. La scansione successiva converte i documenti Office in file protetti, ma gli utenti non potranno accedervi senza una versione supportata di Office.
- Data Guardian non supporta lo strumento di ripristino del sistema di Windows.
- Visitare periodicamente www.dell.com/support per la documentazione più recente e i suggerimenti tecnici.

Prerequisiti del client

Se non è già stato installato, il programma di installazione installa Microsoft Visual C++ 2015 Redistributable Package (x86 e x64).

N.B.:
Per Windows 7 e Windows 8.1, i computer devono essere aggiornati con Windows Updates. Per ulteriori informazioni, vedere https://support.microsoft.com/en-us/help/2919355 e https://support.microsoft.com/en-us/help/2999226.

Microsoft .Net 4.5.2 (o versioni successive) è necessario per Data Guardian. Tutti i computer spediti dalla fabbrica Dell sono dotati di .Net 4.5.2 preinstallato. Tuttavia, se non si installa Data Guardian sull'hardware Dell oppure se lo si aggiorna su un hardware Dell precedente, è necessario verificare quale versione di .Net è installata e aggiornarla, se necessario, prima di installare Dell Data Guardian per evitare errori di installazione o di aggiornamento. Per verificare la versione di Microsoft .Net installata, seguire queste istruzioni nel computer destinato all'installazione: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Per installare Microsoft .Net Framework 4.5.2 , accedere a https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Hardware del client Windows

I requisiti hardware minimi devono soddisfare le specifiche minime del sistema operativo. La tabella seguente descrive in dettaglio l'hardware supportato per il client Windows.

Hardware per Windows

- 200 MB di spazio libero su disco, a seconda del sistema operativo
- Scheda di interfaccia di rete 10/100/1000 o Wi-Fi
- TCP/IP installato e attivato

Se la vostra azienda crittografa i dati per l'archiviazione in ambienti cloud, il computer deve avere una lettera dell'alfabeto disponibile da assegnare a un'unità disco.

Sistemi operativi

La tabella seguente descrive in dettaglio i sistemi operativi supportati.

Sistemi operativi Windows (a 32 e 64 bit)

- Windows 7 SP0-SP1
- Windows 8.1
- Windows 10

N.B.:
Windows 7 non è supportato con il criterio di georilevazione per gli eventi di controllo di Data Guardian.

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

Client di sincronizzazione del cloud

La tabella seguente descrive in dettaglio i client di sincronizzazione del cloud che funzionano con Data Guardian. Gli aggiornamenti del client di sincronizzazione vengono rilasciati spesso pertanto, Dell consiglia di eseguire un test sulle nuove versioni del client di sincronizzazione con Data Guardian prima di introdurle nell'ambiente di produzione.

Client di sincronizzazione del cloud

- Dropbox
- Dropbox for Business (solo Windows)

  N.B.:
  A seconda della versione del server Dell usato dall'azienda, tutti i file e le cartelle presenti negli account Dropbox personali che sono collegati agli account aziendali potrebbero essere crittografati.

- Box

  N.B.:
  Box Tools e Box Edit non sono supportati con Data Guardian. L'uso di Box Tools può far apparire una schermata blu.

- Google Drive
- OneDrive
- OneDrive for Business
- Unified OneDrive

  N.B.:
  Unified OneDrive è un client di sincronizzazione unificato per OneDrive e OneDrive for Business.

Browser Web

È possibile utilizzare Data Guardian > Crittografia cloud con Internet Explorer, Mozilla Firefox e Google Chrome.

N.B.:
Data Guardian > Crittografia cloud non supporta il browser Microsoft Edge.

Attività utente - Crittografia cloud e documenti Office protetti

L'amministratore ha già configurato i criteri per Data Guardian e informerà l'utente se l'azienda utilizza Data Guardian:

- Per gestire il client di sincronizzazione cloud
- Per gestire il client di sincronizzazione cloud e offrire una protezione aggiuntiva per i documenti Office; se l'azienda protegge i documenti Office ma non gestisce un client di sincronizzazione cloud, seguire la procedura illustrata in Attività utente - Documenti Office protetti senza crittografia cloud.

Se l'azienda utilizza Data Guardian con l'archiviazione cloud:

- Prima di distribuire Data Guardian, consultare la guida in linea del provider di archiviazione cloud/client di sincronizzazione cloud per comprendere il funzionamento dell'applicazione di archiviazione cloud in uso. Il presente documento spiega principalmente come utilizzare Data Guardian.
- Generalmente è consigliato installare e lavorare con un solo client di sincronizzazione cloud. L'azienda potrebbe avere un client di sincronizzazione cloud preferito e impostare un criterio che permetta all'utente di usare soltanto quello.

Panoramica delle attività

Questa panoramica riepiloga la sequenza per l'installazione e l'utilizzo di Data Guardian.

Installare Data Guardian e un client di sincronizzazione cloud

Attività	Descrizione	Per maggiori informazioni
Se un client di sincronizzazione cloud è stato installato prima di Data Guardian	File e cartelle preesistenti che vengono sincronizzati con il cloud non sono crittografati. **N.B.:** File e cartelle preesistenti che vengono sincronizzati dal cloud sono crittografati.	Vedere Cartelle preesistenti con file non crittografati.
Installare Data Guardian	Determinare quanto segue: L'utente deve installare Data Guardian L'amministratore ha già installato Data Guardian - Continuare con il passaggio successivo.	L'utente effettua l'installazione: vedere Installare Data Guardian su Windows. Riavviare e continuare con il passaggio successivo.
Confermare lo stato di attivazione	Verificare nell'area di notifica che l'icona di Data Guardian abbia un segno di spunta verde  .	Se l'icona è accompagnata da un punto esclamativo arancione, vedere Possibili problemi con l'attivazione - Cloud e documenti Office protetti.
Se i criteri proteggono i	Client di sincronizzazione aziendale Oppure	Account dei client di sincronizzazione cloud aziendali Oppure

Attività	Descrizione	Per maggiori informazioni
documenti nel cloud, installare un client di sincronizzazione cloud	Client sincronizzazione di base	Account dei client di sincronizzazione cloud di base

N.B.:

Se si apre un documento Office e viene visualizzata una pagina di copertina contenente informazioni sull'installazione o sull'attivazione, è possibile che l'amministratore abbia impostato criteri per proteggere i documenti Office. Confermare che Data Guardian sia installato e attivato. Vedere Possibili problemi con l'attivazione - Cloud e documenti Office protetti.

Utilizzare Data Guardian

Attività	Descrizione	Per maggiori informazioni
Visualizzare il client di sincronizzazione cloud in Esplora file	Dopo l'installazione di Data Guardian e di un client di sincronizzazione cloud, in Esplora file viene visualizzata un'Disco virtuale DDG VDisk.	Gestire cartelle e file Accedere a cartelle e file del client di sincronizzazione sul computer locale
Utilizzare il client di sincronizzazione cloud sull'Disco virtuale DDG VDisk	Sull'Disco virtuale DDG VDisk è possibile aggiungere sottocartelle al client di sincronizzazione cloud e trascinare file o creare file in queste sottocartelle. Dopo la sincronizzazione, i file vengono protetti nel cloud: i file di Office possono essere aperti, ma viene visualizzata solo una pagina di copertina; gli altri file vengono crittografati come file .xen. Tuttavia, nell'unità virtuale locale tali file vengono decrittografati e visualizzati come testo non crittografato. Per maggiori informazioni, fare clic sul link appropriato per il proprio client di sincronizzazione cloud.	**Account aziendale:** Dropbox for Business OneDrive for Business/Unified OneDrive **Account di base:** Dropbox Box Google Drive OneDrive
Visualizzare il menu area di notifica	Fornisce informazioni utili riguardo file, cartelle e risoluzione dei problemi.	Acquisire familiarità con le voci di menu dell'area di notifica di Data Guardian
Proteggere i documenti Office, con attivazione macro e .pdf, se è attivo un criterio	Proteggere un documento Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) al momento della creazione. Sarà protetto durante la condivisione con altri o l'archiviazione su un supporto rimovibile.	Utilizzare i documenti Office con la modalità protetta di Data Guardian • Osservare le opzioni del menu File per determinare il livello di sicurezza per i documenti Office • Utilizzare le opzioni del menu File
Condividere una cartella nel cloud con altri utenti per lavorare sugli stessi file	Condividere una cartella con: Utente interno (ha un indirizzo e-mail di dominio) Utente esterno (ha un indirizzo e-mail non di dominio) - Collaborare con l'amministratore.	Utente interno - Consultare la guida online per il provider di archiviazione cloud. Utente esterno - Vedere Utilizzo di Data Guardian come utente esterno.

Installare Data Guardian con Cloud e documenti Office protetti

Cartelle preesistenti con file non crittografati

Prima di distribuire Dell Data Protection | Data Guardian (DDG VDisk), è consigliabile non configurare account dei provider di archiviazione cloud sui dispositivi di destinazione.

Se si dispone già dell'account di un provider di archiviazione cloud con cartelle sincronizzate sul computer locale e, successivamente, si installa Data Guardian:

- File e cartelle preesistenti che vengono sincronizzati con il cloud rimangono in chiaro
- I file aggiunti a quelle cartelle preesistenti rimangono in chiaro
- Il file sincronizzati dal cloud sono crittografati

  Se si desidera che i file preesistenti vengano crittografati, passare all'Disco virtuale DDG VDisk, creare una nuova sottocartella all'interno del client di sincronizzazione cloud e spostare i file preesistenti nella cartella.

  Oppure

  Per contenuti di grandi dimensioni, un manager o l'amministratore può richiedere temporaneamente il menu Gestione cartelle.

Installare Data Guardian su Windows

Per installare Data Guardian è necessario accedere come amministratore locale del computer.

Il computer deve avere una lettera dell'alfabeto disponibile da assegnare a un'unità disco.

Il computer dovrà essere riavviato dopo l'installazione di Data Guardian.

1. Per scaricare il programma di installazione di Data Guardian, accedere alla posizione specificata dall'amministratore.
2. In base al sistema operativo in uso, selezionare il programma di installazione a 32 bit o a 64 bit, in genere **setup32.exe** o **setup64.exe**, e copiarlo sul computer locale.
3. Fare doppio clic sul file per avviare il programma di installazione.
4. Se viene visualizzato un avviso di protezione, fare clic su **Esegui**.
5. Selezionare una lingua e fare clic su **OK**.
6. Se viene richiesto di installare Microsoft Visual C++ 2010 Redistributable Package o Microsoft .NET Framework 4.0 Client Profile, fare clic su **OK**.
7. Nella schermata iniziale, fare clic su **Avanti**.
8. Leggere il contratto di licenza, accettare i termini, e fare clic su **Avanti**.
9. Nella schermata Cartella di destinazione, fare clic su **Avanti** per eseguire l'installazione nel percorso predefinito: C:\Program Files\Dell \Dell Data Protection\Dell Data Guardian\.

   In C:\, non installare Data Guardian nelle cartelle Users o Windows o nella radice di qualsiasi unità. Verrà visualizzato un messaggio di errore.
10. Nel campo *Nome server:*, immettere il nome del server con cui comunicherà questo computer, ad esempio server.domain.com. Non è necessario includere www o http(s). Queste informazioni sono fornite dall'amministratore.

    Non deselezionare la casella di controllo *Abilita verifica trust SSL*, a meno che l'amministratore non lo richieda.
11. Fare clic su **Avanti**.
12. Nella schermata Informazioni di Conferma server di attivazione, confermare che l'indirizzo URL del server è corretto. Il programma di installazione aggiunge www o http(s), e la porta. Fare clic su **Avanti**.

13 Nella finestra Tipo di gestione, selezionare questa opzione:
   - Utente interno - Un utente con un indirizzo e-mail nel dominio dell'azienda.

14 Fare clic su **Installa** per avviare l'installazione.
   Viene visualizzata una finestra di stato che mostra l'avanzamento dell'installazione.

15 Fare clic su **Fine** quando viene visualizzata la schermata Installazione completata.

16 Fare clic su **Sì** per riavviare il sistema.
   L'installazione di Data Guardian è completata.

17 Dopo il riavvio, verificare nell'area di notifica che l'icona di Data Guardian abbia un segno di spunta verde  .

Data Guardian e crittografia cloud

Se l'azienda ha definito criteri per proteggere i dati nel cloud, l'installazione è stata completata ed è stato effettuato l'accesso a un client di sincronizzazione, in Esplora risorse viene visualizzata l'Disco virtuale DDG VDisk.

N.B.:
Data Guardian non supporta lo smontaggio dell'unità virtuale.

Se è necessario installare e accedere a un client di sincronizzazione, vedere Installare un client di sincronizzazione cloud.

Installare un client di sincronizzazione cloud

Scaricare e installare

Generalmente, un'azienda consiglia a tutti gli utenti di installare lo stesso client di sincronizzazione cloud. Se applicabile, utilizzare il client di sincronizzazione cloud preferito dall'azienda.

N.B.:
Il computer deve avere una lettera dell'alfabeto disponibile da assegnare a un'unità disco.

N.B.:
Attualmente, Data Guardian non supporta un client di sincronizzazione installato in un punto di montaggio.

1 Installare un client di sincronizzazione cloud di base o aziendale:
   - **Account dei client di sincronizzazione cloud aziendali**
     Nel caso in cui l'azienda offra l'opzione per un account aziendale, l'amministratore fornirà il collegamento per scaricarlo e installarlo. Le opzioni sono:
     - **Dropbox for Business** - Se si installa Dropbox for Business è necessario anche Autenticare Dropbox for Business.
     - **OneDrive for Business/Unified OneDrive** - Per le istruzioni dettagliate vedere https://support.microsoft.com/en-us/kb/2903984.
   - **Account dei client di sincronizzazione cloud di base**
     - **Dropbox** - Vedere https://www.dropbox.com/install
     - **Box Sync** - Vedere https://www.box.com/box-for-devices
     - **Google Drive** - Vedere https://www.google.com/drive/download/
     - **OneDrive/Unified OneDrive (Windows 7 e 8)** - Vedere https://onedrive.live.com/about/en-us/download/
       In Windows 8.1 e versioni successive, OneDrive è preinstallato. Se Windows Update è abilitato, Unified OneDrive sostituisce OneDrive.

2 Dopo l'installazione e l'accesso viene visualizzato quanto segue:
   - In Esplora file viene aggiunta un'Disco virtuale DDG VDisk. La cartella del client di sincronizzazione cloud viene aggiunta all'unità virtuale.
     Se si installa più di un client di sincronizzazione cloud, per ciascuno di essi viene visualizzata una cartella nell'unità.

N.B.:
Data Guardian non supporta lo smontaggio dell'unità virtuale.

- In Esplora file > Preferiti, viene aggiunta una cartella per il client di sincronizzazione cloud.
- Nell'area di notifica viene visualizzata l'icona del client di sincronizzazione.
- A seconda del provider di archiviazione cloud, può essere aggiunto automaticamente al desktop un collegamento al client di sincronizzazione.
- Solo nella modalità Consenso esplicito, ma non nella modalità Protezione forzata - Nella radice della cartella Documenti viene aggiunta una cartella Documenti sicuri. Vedere Documenti > cartella Documenti sicuri.

Modificare la lettera dell'unità virtuale o creare una scelta rapida

Dopo l'installazione di Data Guardian e di un client di sincronizzazione cloud, in Esplora file viene visualizzata l'icona dell'Disco virtuale DDG VDisk. La lettera dell'unità viene assegnata usando la prima lettera dell'alfabeto disponibile partendo dal fondo.

Per cambiare la lettera dell'unità:

1 Nell'area di notifica, fare clic sull'icona Data Guardian e selezionare **Configura unità**.

2 Selezionare una lettera disponibile dall'elenco *Correnti*.

3 Fare clic su **Applica** oppure **OK**.
Per aggiungere l'icona dell'Disco virtuale DDG VDisk al desktop, fare clic con il pulsante destro del mouse sull'unità e selezionare **Crea collegamento**.

Autenticare Dropbox for Business

Se si installa Dropbox for Business, Data Guardian chiede di effettuare l'autenticazione.

Per autenticare:

1 Al termine dell'installazione di Data Guardian potrebbe aprirsi la finestra Autenticazione; in alternativa, fare clic sull'icona di Data Guardian e selezionare **Dropbox > Connetti**.
La finestra Autenticazione segnala che Data Guardian deve poter accedere all'account Dropbox dell'utente e può fornire istruzioni sugli account aziendali e personali.

Questo fornisce all'utente le opzioni del menu di scelta rapida ed è essenziale per l'azienda e l'amministratore, in quanto fornisce ulteriori misure di protezione.

2 Nella finestra Autenticazione, fare clic su **Avanti**.

3 Se si apre una finestra Protezione dalle minacce di rete, fare clic su **Sì**.

4 Nella finestra Autenticazione, immettere l'indirizzo di posta elettronica di dominio e la password di Dropbox.

5 Fare clic su **Accedi**.

6 Se gli account Dropbox aziendale e personale sono collegati, verrà richiesto di selezionarne uno. Occorre selezionare l'account aziendale.

7 Fare clic su **Fine** o attendere la chiusura della finestra.

Gestire cartelle e file

Data Guardian funziona in maniera trasparente con il client di sincronizzazione cloud. Quando l'amministratore imposta un criterio per attivare Data Guardian, i file vengono crittografati e protetti nel cloud quando sono sincronizzati dal computer locale.

Seguire le istruzioni nella guida del provider di archiviazione cloud per eseguire le azioni seguenti:

- Creare cartelle
- Caricare/scaricare cartelle e file

N.B.:
Per caricare i file, copiare o trascinare i file nelle cartelle sull'Disco virtuale DDG VDisk. Data Guardian non supporta il trascinamento di file dal computer locale al Web o la creazione di file direttamente nel sito Web del provider di archiviazione cloud.

- Usare la sincronizzazione selettiva delle cartelle
- Condividere cartelle o file con utenti interni che dispongono di Data Guardian. Vedere Condivisione di una cartella con un utente interno.
- Condividere le cartelle o i file con utenti esterni. Vedere Utilizzo di Data Guardian come utente esterno.
- Annullare la condivisione delle cartelle

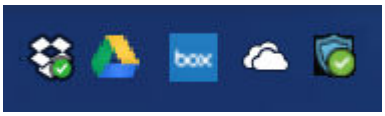
Visualizzare le cartelle e i file nel computer locale e nel cloud

Accedere a cartelle e file del client di sincronizzazione sul computer locale

Per accedere a cartelle e file sincronizzati, fare clic sull'**Disco virtuale DDG VDisk** in Esplora file. Viene visualizzato il client di sincronizzazione cloud.

Di seguito sono elencati altri modi per accedere al client di sincronizzazione cloud.

- Nell'area di notifica, selezionare l'icona del client di sincronizzazione e aprire la cartella del client di sincronizzazione. Per maggiori informazioni, consultare la Guida del provider di archiviazione cloud.

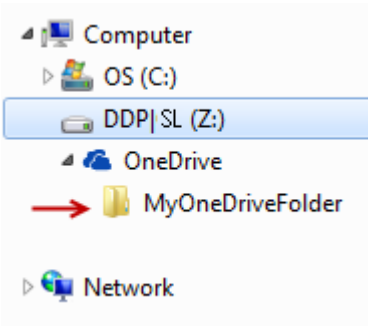


- In Preferiti, fare clic sull'icona del client di sincronizzazione.
  Quando si fa clic sull'icona del client di sincronizzazione nell'area di notifica o in Preferiti, è possibile notare che l'Disco virtuale DDG VDisk è evidenziata. Data Guardian reindirizza l'utente a questa unità virtuale, che consente di visualizzare le cartelle e i file decrittati in locale nel formato di testo in chiaro.

È inoltre possibile accedere all'Disco virtuale DDG VDisk attraverso una scelta rapida sul desktop. Vedere Modificare la lettera dell'unità virtuale o creare una scelta rapida.

Aggiungere cartelle

Con Data Guardian, è necessario aggiungere sottocartelle alla cartella di sincronizzazione cloud. Non aggiungere file nella radice dell'Disco virtuale DDG VDisk.



Aggiungere file

Quando si aggiunge un file a una cartella, Data Guardian aggiunge automaticamente un file alla cartella sul Web. Data Guardian usa il file Come accedere ai file sicuri.html quando si condivide una cartella con utenti esterni. Non è necessario aprire o scaricare questo file. Vedere Utilizzo di Data Guardian come utente esterno.

Visualizzare cartelle e file del client di sincronizzazione nel cloud

Data Guardian crittografa i dati nel cloud; i nomi dei file hanno l'estensione .xen. L'icona del file può variare per ogni provider di archiviazione cloud, ma non viene visualizzato alcun contenuto. Non è possibile aprire file nel cloud. Pertanto, se qualcuno riuscisse ad accedere a un account di archiviazione cloud privato, questi non potrebbe aprire o visualizzare i file che contiene. Questo aumenta la sicurezza nel cloud. È possibile visualizzare i file con testo in chiaro solo sull'Disco virtuale DDG VDisk.

Occasionalmente, quando si scarica un file .xen sul desktop e lo si decritta, rimane una copia del file con l'estensione .xen. È possibile eliminare la copia scaricata del file .xen.

Se l'azienda richiede un'ulteriore protezione per le cartelle e i file nel cloud, l'amministratore può impostare un criterio per offuscare i nomi dei file sia nel cloud sia una volta scaricati. Se qualcuno riuscisse ad accedere a un account di archiviazione cloud privato, questi non potrebbe né aprire i file, né leggerne i nomi.

Visualizzare cartelle e file del client di sincronizzazione su un computer locale con Data Guardian e un'unità virtuale installati

Per facilitare l'uso di Data Guardian sul computer locale, quando si apre una cartella sull'Disco virtuale DDG VDisk, i file provenienti dal cloud vengono automaticamente decrittati e visualizzati in chiaro anche se sono protetti come file crittografati nel cloud.

Proteggere cartelle e file su dispositivi che non dispongono di Data Guardian

Se una persona non autorizzata scarica un file protetto dal cloud a un dispositivo su cui **non** è installato Data Guardian, la persona non è in grado di accedere ai dati. In base ai criteri impostati dall'amministratore:

- Documenti Office - Il documento si apre, ma viene visualizzata solo una pagina di copertina con un messaggio specifico dell'azienda.
- Documenti non di Office - Il file viene scaricato come file .xen. La persona non è in grado di aprire il file.

> **N.B.:**
> Per gli utenti interni, se si scarica un file da un computer su cui è installato Data Guardian a un dispositivo che non dispone dell'applicazione, non è possibile visualizzare il file finché non si installa Data Guardian come utente esterno.

Occasionalmente, è possibile che venga visualizzato un file .xen su un computer su cui è installato Data Guardian. Per esempio, se la connessione Internet si è interrotta prima del completamento del download, la chiave per aprire il file potrebbe non essere disponibile. Una finestra di dialogo indica che il file non può essere decrittografato.

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'Disco virtuale DDG VDisk.

Cercare nomi di file e contenuti sull'Disco virtuale DDG VDisk

Se si desidera cercare nomi di file o contenuti sull'Disco virtuale DDG VDisk, è necessario abilitare l'indicizzazione della ricerca di Windows per tale unità.

> **N.B.:**
> L'Indicizzazione di ricerca di Windows è abilitata solo per le cartelle utenti.

Per abilitare l'indicizzazione della ricerca di Windows per l'Disco virtuale DDG VDisk:

1. Nel Pannello di controllo, immettere **Indicizzazione ricerca** nel campo di ricerca.
2. Selezionare **Opzioni di indicizzazione**.
3. In *Cambia percorsi selezionati*, selezionare la casella di controllo per l'Disco virtuale DDG VDisk.

N.B.:
La procedura da eseguire successivamente può variare in base al sistema operativo.

4 Fare clic su **OK**.

5 In Opzioni di indicizzazione, fare clic su **Chiudi**.

Ora è possibile eseguire una ricerca sull'Disco virtuale DDG VDisk.

Condivisione di una cartella con un utente interno

Un utente interno dispone di un indirizzo e-mail nel dominio dell'azienda.

Per condividere una cartella con un utente interno, è necessario accedere al sito Web del provider di archiviazione cloud e selezionare **Condividi**. Consultare la guida online relativa al provider di archiviazione cloud.

Condivisione di una cartella con Data Guardian e Box

Nel sito Web Box, selezionare una delle seguenti opzioni.

Opzione del sito Web Box	Opzioni	Descrizione
Condividi	Disponibile per cartelle e file Accesso in visualizzazione	Quando viene visualizzata la finestra Condividi, assicurarsi che Consenti download sia impostato su **Sì**. Dopo aver scaricato le cartelle o i file, le persone che effettuano la condivisione devono estrarre la cartella compressa e quindi spostare la cartella e file nell'Disco virtuale DDG VDisk.
Invita collaboratori	Disponibile per le cartelle Accesso in visualizzazione o modifica	Quando viene visualizzata la finestra di dialogo Invita è possibile selezionare **Modifica** o **Visualizzazione**. Le persone che effettuano la condivisione possono sincronizzare la cartella sul loro computer; la sincronizzazione avviene nell'Disco virtuale DDG VDisk.

Utilizzare i documenti Office con la modalità protetta di Data Guardian

Per migliorare la sicurezza aziendale, l'amministratore può abilitare un criterio per proteggere i file di queste applicazioni Office:

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm

Se una persona non autorizzata accede a un file protetto, il file rimane crittografato, ad esempio quando:

- Il file viene allegato a un messaggio e-mail
- Il file viene spostato in un browser - In alcuni client di sincronizzazione cloud, è possibile fare clic con il pulsante destro del mouse su un nome di file e selezionare **Sposta**.
- Il file viene condiviso sulla rete
- Il file viene caricato in un provider di archiviazione cloud
- Il file viene salvato su un supporto rimovibile

Per i documenti Office, potrebbe essere visualizzata una pagina di copertina con le istruzioni per l'installazione o l'attivazione di Data Guardian, ad esempio:

- È necessario installare Data Guardian.
- È necessario attivare Data Guardian.
- È stato aperto un documento Office protetto nel cloud.
- Un file di Office è stato scaricato da un computer dotato di Data Guardian a un dispositivo personale privo della medesima applicazione.
- Un utente non autorizzato accede a uno dei file Office - Viene visualizzata una pagina di copertina con un messaggio specifico dell'azienda, ma l'utente non può visualizzare il contenuto del file.

Se l'azienda utilizza la modalità protetta di Data Guardian, vedere:

- Osservare le opzioni del menu File per determinare il livello di sicurezza per i documenti Office
- Utilizzare le opzioni del menu File
- Stabilire con quale modalità di consenso esplicito sono protetti i documenti
- Opzioni di menu aggiuntive per i documenti Office protetti
- Utenti esterni e documenti Office protetti

Osservare le opzioni del menu File per determinare il livello di sicurezza per i documenti Office

Per determinare se l'amministratore ha abilitato i criteri di Data Guardian, aprire un documento Office e selezionare **File**. Se nel riquadro sinistro viene visualizzato *Salva come protetto*, è disponibile una protezione supplementare sui documenti Office.

Per stabilire il livello di sicurezza, osservare le opzioni abilitate o disabilitate:

- **Modalità Consenso esplicito** - Sono disponibili alcune opzioni per stabilire quali documenti Office proteggere.
  - *Salva con nome* e *Salva come protetto* sono abilitati - Se si decide di proteggere un documento Office, selezionare **Salva come protetto**.
  - *Stampa* ed *Esporta* possono essere abilitati o disabilitati in base ai criteri.
  - *Condividi* (*Salva e invia* per Office 2010) è abilitato.
  - Cartella **Documenti > Documenti sicuri** - Nella modalità Consenso esplicito, ma non nella modalità Protezione forzata, nella radice della cartella Documenti viene aggiunta una cartella Documenti sicuri. I documenti Office in questa cartella sono crittografati. Se si rimuove un documento Office protetto da questa cartella, il file rimane crittografato. Se si rinomina la cartella, i contenuti della cartella rinominata sono crittografati. Se si elimina la cartella, la stessa viene ricreata.
- **Modalità Protezione forzata** - L'azienda richiede un livello di sicurezza più alto.
  - *Salva con nome* è disabilitato e *Salva come protetto* è abilitato - È necessario salvare tutti i documenti Office nella modalità protetta.
  - *Stampa* ed *Esporta* possono essere abilitati o disabilitati in base ai criteri.
  - *Condividi* (*Salva e invia* per Office 2010) è disabilitato.

    N.B.:
    Con la modalità Force-Protected, i criteri impostati consentono anche di utilizzare determinati intervalli di tempo per effettuare ricerche nel computer e individuare eventuali file Office non protetti e modificarli attivando la modalità protetta. È necessario avere effettuato l'accesso ed essere connessi alla rete perché Data Guardian cerchi eventuali file Office non protetti.

- Se si seleziona **Salva come protetto**, l'unica opzione nel campo *Salva come* è *Documento Office protetto*.

- **File > Informazioni** è diverso, ad esempio:
  - Per entrambe le modalità Consenso esplicito e Protezione forzata: viene visualizzato *Aggiungi restrizione data* se l'amministratore ha abilitato tale criterio. Vedere Migliorare la sicurezza aggiungendo restrizioni alla data.
  - Per entrambe le modalità Consenso esplicito e Protezione forzata: le informazioni sulle proprietà di questo documento di Office, come autore e data, vengono nascoste per maggiore sicurezza.
  - Stato di sola lettura: vedere di seguito per ulteriori informazioni.

N.B.:
L'opzione *Proteggi documento* in File > Informazioni è legata a Microsoft Office e non alla modalità protetta di Data Guardian.

Se si apre un documento Office e l'applicazione segnala che è attiva la modalità di sola lettura, controllare quanto segue:

- Se nel riquadro sinistro non viene visualizzato *Salva come protetto*, la modalità di sola lettura non è stabilita dai criteri di Data Guardian.
- Se l'amministratore ha impostato criteri per la modalità Protezione forzata, con un livello di sicurezza maggiore, i documenti Office non protetti vengono aperti nella modalità di sola lettura.

N.B.:
Per OneDrive, se si apre un documento Office protetto tramite **File > Apri > OneDrive** e il documento è di sola lettura, verificare di aver installato e configurato il client di sincronizzazione OneDrive.

Utilizzare le opzioni del menu File

Questa tabella elenca le opzioni del menu File per i documenti Office. A seconda del livello di sicurezza, alcune opzioni sono visualizzate in grigio.

N.B.:
Attualmente, i documenti Office incorporati non sono supportati nella modalità protetta di Office.

Menu File	Modalità di consenso esplicito e documenti Office protetti	Modalità di protezione forzata per documenti protetti e non protetti
Aprire	**I file vengono aperti come di consueto**	**I documenti non protetti vengono aperti in modalità di sola lettura.**
Salva	• Opzioni: Documento già protetto - Viene salvato come protetto. Documento non protetto - Viene salvato come non protetto. Per proteggerlo, fare clic su **Salva come protetto**. • Documento di sola lettura - Una finestra di dialogo informa che non è possibile salvare un documento non protetto. Viene visualizzata una finestra Salva con nome, nella quale occorre salvare il file con un nome diverso. • File .xen - È possibile aprire e salvare il file .xen nella modalità protetta, ma il file viene rimosso dal cloud. Il documento Office ha la sua normale estensione, ma è protetto. **N.B.:** **Nell'unità virtuale, se l'utente fa clic con il pulsante destro del mouse per creare un nuovo documento Office, il documento viene salvato come file .xen. È necessario salvarlo manualmente come documento protetto.**	• Il documento è protetto. • Documento di sola lettura - È possibile modificarlo, ma non salvare l'originale. Quando si fa clic su Salva viene visualizzata la finestra Salva come protetto ed è necessario salvare il documento nella modalità protetta con un nuovo nome. • Documenti remoti - Se si apre un documento non protetto in una posizione remota, è necessario salvarlo sull'unità locale per modificarlo e salvarlo. Non è possibile salvarlo nella posizione remota. **N.B.:** **Facendo clic su Salva viene aperta la finestra Salva con nome e l'unica opzione nel campo Salva come è Documento Office protetto (Documento, Presentazione o Cartella di lavoro).** • File .xen - È possibile aprire e salvare il file .xen nella modalità protetta, ma il file viene rimosso dal cloud. Il documento Office ha la sua normale estensione, ma è protetto.
Salva con nome	**Presenta le opzioni standard (ma non la modalità protetta)**	**Disabilitato**
Salva con nome protetto	**L'unica opzione nel campo Salva come è Documento Office protetto**	**L'unica opzione nel campo Salva come è Documento Office protetto**
Stampa	**Può essere attivato o disattivato in base ai criteri impostati dall'amministratore. Se l'opzione di menu è abilitata, un criterio potrebbe applicare una filigrana, contenente il nome utente, il nome di dominio e l'ID del computer, su ogni pagina stampata.**	**A seconda del criterio, questa opzione può essere abilitata o disabilitata. Se l'opzione di menu è abilitata, un criterio potrebbe applicare una filigrana, contenente il nome utente, il nome di dominio e l'ID del computer, su ogni pagina stampata.**
Condividi	**Abilitata**	**Disabilitato**
Salva e invia (Office 2010)	**Abilitata**	**Disabilitato Se Stampa è abilitato, è possibile selezionare Stampa per stampare il documento in formato PDF.**
Esporta (Office 2013 e versioni successive)	**Può essere attivato o disattivato in base ai criteri impostati dall'amministratore.**	**Può essere attivato o disattivato in base ai criteri impostati dall'amministratore.**
Esporta protetto (Office 2013 e versioni successive)	Se l'opzione di menu Esporta è disattivata ed Esportazione protetta è abilitata, il documento viene esportato con una filigrana, contenente il nome utente, il nome di dominio e l'ID computer, su ogni pagina. **N.B.:** Se si esporta un documento nella modalità protetta per un utente esterno, egli potrà aprire e visualizzare il file, ma non esportarlo o stamparlo.	Se l'opzione di menu Esporta è disattivata ed Esportazione protetta è abilitata, il documento viene esportato con una filigrana, contenente il nome utente, il nome di dominio e l'ID computer, su ogni pagina. **N.B.:** Se si esporta un documento nella modalità protetta per un utente esterno, egli potrà aprire e visualizzare il file, ma non esportarlo o stamparlo.

Lavorare online con i documenti Office protetti

Durante la creazione di documenti Office protetti, la procedura migliore prevede di lavorare online in modo da generare le chiavi per tali documenti. Se il computer deve essere riformattato e sono stati creati documenti Office protetti offline, è necessario informare l'amministratore.

Lavorare online con i documenti con attivazione macro protetti

Nel caso di un documento con attivazione macro protetto, la macro esiste ma è bloccata. Al momento Data Guardian è in grado di controllare un documento con attivazione macro solo dopo aver chiuso e riaperto il nuovo documento protetto (.docm, .pptm, .xlsm). Inoltre, se si salva un documento con attivazione macro protetto come documento non protetto, è necessario chiudere e riaprire il documento per eseguire le macro.

Allegare un documento Office protetto a un messaggio e-mail di Outlook

Per allegare un documento Office protetto a un messaggio e-mail di Outlook, selezionare **Inserisci** anziché *Inserisci come testo*. Il comando *Inserisci come testo* incolla il contenuto del documento direttamente nel corpo del messaggio e-mail, pertanto il contenuto non è più protetto.

Risoluzione dei problemi per la modalità di consenso esplicito

In File > Informazioni, se il comando Stampa è disattivato, significa che un criterio di Data Guardian ha disabilitato la stampa per i documenti Office protetti. Al momento, quando si fa clic con il pulsante destro del mouse su un file Office protetto in Esplora risorse, l'opzione Stampa non è disattivata. Tuttavia, se si seleziona Stampa, si verifica quanto segue:

- Word - Una finestra di dialogo indica che Word ha smesso di funzionare.
- Excel - Una finestra di dialogo indica che il comando Stampa è disattivato da un criterio.
- PowerPoint - Una finestra di dialogo indica che il comando Stampa è disattivato da un criterio. Se si fa clic su OK, viene stampata una pagina di copertina che comunica che il documento è protetto.

Stabilire con quale modalità di consenso esplicito sono protetti i documenti

Se si utilizza la modalità di protezione forzata, tutti i documenti Office vengono protetti. Se si utilizza la modalità di consenso esplicito e si desidera confermare se un documento è protetto o meno, aprire il documento e verificare che sulla barra del titolo sia indicato che il documento è protetto.

Opzioni di menu aggiuntive per i documenti Office protetti

Il tipo di documento Office, protetto o non protetto, può influenzare le operazioni riportate di seguito.

Clic con il pulsante destro del mouse > Proteggi

È possibile fare clic con il pulsante destro del mouse su un documento Office e selezionare **Proteggi**. È necessario aggiungere contenuti perché l'opzione di menu sia visualizzata. Non è possibile proteggere un documento vuoto.

Proprietà file > scheda Dell Data Guardian

Per i documenti Office protetti, è possibile fare clic con il pulsante destro del mouse e selezionare **Proprietà**: viene visualizzata una scheda **Dell Data Guardian** contenente informazioni quali l'ID chiave del file e i dati di accesso ed embargo.

Incolla

Se l'amministratore imposta un criterio per proteggere i documenti Office:

- È possibile copiare e incollare i dati nel documento protetto originale.
- Non è possibile copiare o incollare da un documento protetto a un documento non protetto. Negli Appunti non viene visualizzato nulla e un messaggio di testo specifico per l'azienda comunica che non è possibile incollare nel documento non protetto o non gestito.

N.B.:
Se si taglia testo da un documento protetto e si riceve il messaggio in un documento non protetto, fare clic su **Annulla** nel documento protetto per recuperare il testo.

Trascinamento nella modalità protetta

È possibile trascinare e rilasciare contenuti in un documento Word protetto. Attualmente, il trascinamento è disabilitato per i file Excel e PowerPoint protetti.

Stampa per buste ed etichette

Se l'amministratore ha impostato un criterio per aggiungere una filigrana durante la stampa di un documento Office protetto, seguire questi passaggi per stampare buste o etichette:

1 In un documento Word, selezionare la scheda **Lettere**.
2 Selezionare l'opzione **Buste** o **Etichette**.
3 Dopo aver immesso l'indirizzo o l'indirizzo di risposta, fare clic su **Stampa**.

N.B.: Se si utilizza un'altra opzione per la stampa e l'amministratore ha impostato un criterio per aggiungere una filigrana ai documenti Office stampati, sulla busta o sull'etichetta sarà visualizzata una filigrana.

Manomissione e documenti Office protetti

Data Guardian è in grado di analizzare i documenti Office protetti per rilevare alcune forme di manomissione.

Se un utente interno manomette un documento Office protetto:

- Data Guardian può riparare o ripristinare alcune manomissioni.
- Per eventuali manomissioni che non possono essere riparate, potrebbe essere visualizzata una finestra di dialogo che segnala che il file è stato manomesso e occorre contattare l'amministratore.

Se un utente non autorizzato apre un documento Office protetto, viene visualizzata solo la pagina di copertina. Se l'utente non autorizzato modifica la pagina di copertina, Data Guardian ripristinerà la pagina di copertina quando un utente autorizzato salverà nuovamente il file protetto.

Utenti esterni e documenti Office protetti

Migliorare la sicurezza aggiungendo restrizioni alla data

Con Data Guardian, un documento Office protetto viene caricato nel cloud e condiviso:

- Tutti gli utenti interni di Data Guardian possono visualizzarlo.
- Gli utenti esterni possono visualizzarlo in base ai criteri impostati.

Per una maggiore sicurezza con gli utenti esterni, è possibile aggiungere una restrizione di data per limitare il tempo per cui un utente esterno può visualizzare un documento Office protetto.

1 Selezionare **File > Informazioni > Restrizione data**.
2 Dal menu a discesa, selezionare la data e l'ora di inizio e di fine entro le quali un utente esterno può visualizzare il documento.

N.B.:
La data e l'ora di inizio possono essere nel futuro, se si desidera inviare il documento ma impedire all'utente esterno di visualizzarlo fino alla data e all'ora previste.

3 Fare clic su **OK**.

Il documento viene salvato, protetto, chiuso e riaperto.

N.B.:
Se si modificano le date per un documento Office non protetto e si fa clic su Annulla, Data Guardian continua a proteggere il file.

N.B.:
Attualmente, se si aggiungono restrizioni di data a un documento Office protetto e si prevede di salvarlo in un'unità di rete, è necessario salvare il file in locale e poi copiarlo in rete.

Se un utente esterno apre un file dopo l'intervallo di date e orari, una finestra di dialogo indica che il file presenta restrizioni di accesso e che l'utente esterno può contattare l'autore del file. La finestra di dialogo non mostra le date all'utente esterno.

Se si imposta il campo Data di inizio su una data o un orario futuri e l'utente esterno apre il file prima di tale periodo, viene visualizzata una finestra di dialogo che comunica che il file non può essere aperto fino alla data e all'ora indicate a causa di restrizioni di accesso.

Lavorare in mancanza di una connessione Internet

Senza una connessione Internet, è comunque possibile visualizzare i file di sincronizzazione cloud sull'unità locale utilizzando Esplora file. Tuttavia, l'Disco virtuale DDG VDisk non viene visualizzata. Inoltre, le modifiche non saranno sincronizzate nel cloud finché non verrà stabilita una connessione Internet.

Limite di caratteri per i nomi di percorso delle cartelle

I nomi di percorso in Windows hanno un limite di 248 caratteri.

Nel cloud tale limite non è previsto. Pertanto, è possibile creare cartelle e sottocartelle con un nome di percorso superiore al limite. Tuttavia, localmente, in Windows, nel caso in cui i nomi di percorso superino tale limite, le cartelle non vengono create. Pertanto, accertarsi di limitare i nomi di percorso di cartelle e sottocartelle a 248 caratteri.

Dropbox for Business

Dropbox for Business ha requisiti specifici. Vedere Installare un client di sincronizzazione cloud.

Guida del provider di archiviazione cloud

Prima di utilizzare Data Guardian, accertarsi di conoscere le informazioni sul provider di archiviazione cloud. L'assistenza per Dropbox for Business è disponibile all'indirizzo:

https://www.dropbox.com/help.

Anche se è possibile caricare i file nel sito Web del provider di archiviazione cloud, è consigliabile lavorare con le cartelle e i file nell'Disco virtuale DDG VDisk.

Connettere Data Guardian e Dropbox for Business

Se l'azienda utilizza Dropbox for Business, è necessario consentire a Data Guardian di rimanere connesso.

Per connettersi:

1 Nell'area di notifica, fare clic sull'icona Data Guardian, quindi selezionare **Dropbox > Connetti**.
2 Nella finestra di autenticazione di Dropbox, leggere le informazioni e fare clic su **Avanti**.
3 Se gli account Dropbox aziendale e personale sono collegati, verrà richiesto di selezionarne uno. Occorre selezionare l'account aziendale.
4 Quando viene richiesto di consentire a Data Guardian di accedere a file e cartelle di Dropbox, fare clic su **Consenti**.
5 Fare clic su **Fine**.

Impostare la sincronizzazione selettiva per le cartelle

Per effettuare la sincronizzazione selettiva delle cartelle:

1 Nell'area di notifica, fare clic sull'icona **Dropbox for Business**.
2 Fare clic sull'icona **Impostazioni** e selezionare **Preferenze**.
3 Fare clic sulla scheda **Account**, quindi fare clic su **Sincronizzazione selettiva**.
4 Selezionare solo le cartelle o sottocartelle da sincronizzare dal computer.
5 Fare clic su **Aggiorna**.
6 Nella finestra di dialogo di conferma dell'aggiornamento, fare clic su **OK**.
7 Nella finestra delle preferenze di Dropbox, fare clic su **OK**.
Nell'area di notifica viene visualizzato un pop-up che indica che è in corso la sincronizzazione delle cartelle.

Sarà l'azienda a determinare se l'utente può disporre di un account aziendale o se può usare entrambe le cartelle, aziendale e personale. Se vi sono cartelle preesistenti, contenenti dati o file personali, che non devono essere crittografate, deselezionare tali cartelle prima di installare Data Guardian. Altrimenti, potrebbero essere crittografati anche i dati personali.

Usare l'icona di Dropbox for Business nell'area di notifica

Nell'area di notifica, fare clic sull'icona di Dropbox.

- Per accedere al sito Web - Selezionare l'icona a forma di globo.

  N.B.:
  Se si usa Chrome oppure Firefox per aprire Dropbox.com, accertarsi di chiudere il browser al termine delle operazioni con file e cartelle. Anche se si apre un'altra scheda nel browser, il contenuto è sempre crittografato che si tratti di posta elettronica, allegati o upload effettuati tramite browser.

- Per la cartella - Selezionare l'icona della cartella di Dropbox per essere reindirizzati all'Disco virtuale DDG VDisk.

Usare il menu di scelta rapida di Dropbox for Business

In Esplora risorse, quando è installato Data Guardian, Dropbox for Business dispone di un menu di scelta rapida.

N.B.:
È necessario connettere Data Guardian a Dropbox.

Per accedere al menu di scelta rapida, in Esplora risorse aprire una cartella di Dropbox e fare clic con il pulsante destro del mouse su un file. L'icona del cloud ha queste opzioni:

- Collegamento alla condivisione protetta Dropbox
- Visualizza in Dropbox.com

- Visualizza versioni precedenti

Usare gli account Dropbox aziendale e personale

Se l'azienda dispone di Dropbox for Business e consente anche di collegare un account Dropbox personale all'account aziendale, informarsi sui criteri impostati dall'amministratore per tali account. Per esempio, un'azienda potrebbe impostare i seguenti criteri:

- I file aziendali e personali sono crittografati.
  Oppure
- Solo file e cartelle aziendali sono crittografati. I file personali rimangono non crittografati.
  Per sicurezza, l'organizzazione potrebbe avere un criterio di controllo. I nomi dei file nella cartella personale vengono registrati e inviati al Dell Data Protection Server.

Se si usano account Dropbox aziendali e personali, non archiviare file aziendali nella cartella Dropbox personale.

Decrittare le cartelle in un account personale

Se una cartella personale viene accidentalmente crittografata, l'amministratore può concedere l'accesso temporaneo all'utente per gestire la crittografia delle sue cartelle. Deselezionare le cartelle che non devono essere crittografate. È inoltre possibile rimuovere la sincronizzazione delle cartelle scollegando l'account oppure annullare la sincronizzazione delle cartelle personali che non devono essere crittografate.

OneDrive for Business/Unified OneDrive

N.B.:
Data Guardian non è supportato da Microsoft Office 365.

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

Guida del provider di archiviazione cloud

Prima di utilizzare Data Guardian, accertarsi di conoscere le informazioni sul provider di archiviazione cloud. L'assistenza per OneDrive for Business è disponibile all'indirizzo:

http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

Anche se è possibile caricare i file nel sito Web del provider di archiviazione cloud, è consigliabile lavorare con le cartelle e i file nell'Disco virtuale DDG VDisk.

Impostare la sincronizzazione selettiva per le cartelle

Per effettuare la sincronizzazione selettiva delle cartelle:

1. Nell'area di notifica, fare clic con il pulsante destro del mouse sull'icona **OneDrive for Business/Unified OneDrive**, quindi fare clic su **Sincronizza una nuova libreria**.
2. Immettere l'URL della libreria.
3. Selezionare **Sincronizza ora**.
4. Selezionare **Mostra file personali**.

Usare l'icona di OneDrive for Business nell'area di notifica

Nell'area di notifica:

- Per il sito Web - Fare clic con il pulsante destro del mouse e selezionare **Vai a OneDrive.com**.
- Per la cartella - Fare clic con il pulsante sinistro o destro del mouse e selezionare **Apri la cartella OneDrive for Business personale**. L'utente viene reindirizzato all'Disco virtuale DDG VDisk.

Considerazioni sulla sicurezza - Data Guardian e OneDrive o OneDrive for Business

Dell Data Guardian crittografa le cartelle e i file per proteggere i dati. Data Guardian collabora con i client di sincronizzazione, pertanto è bene essere consapevoli di questi aspetti.

- Durante il download, non selezionare Annulla. in quanto determina un errore. Se si desidera cancellare un file, attendere che il download sia completo.
- Per Windows 8.1, Microsoft OneDrive crea dei file segnaposto che compaiono nel client di sincronizzazione ma non vengono effettivamente scaricati. Pertanto, Dell Data Guardian non è in grado di crittografarli. Se si apre un file segnaposto, Data Guardian visualizza una finestra di dialogo che segnala che il file non sarà protetto. È possibile fare clic con il pulsante destro del mouse e selezionare **Scarica**; **Data Guardian** lo converte in un file .xen.

Dropbox

Guida del provider di archiviazione cloud

Prima di utilizzare Data Guardian, accertarsi di conoscere le informazioni sul provider di archiviazione cloud. Il supporto per Dropbox è disponibile all'indirizzo https://www.dropbox.com/help.

Anche se è possibile creare i file nel cloud o caricare i file nel sito Web del provider di archiviazione cloud, è consigliabile lavorare con le cartelle e i file nell'Disco virtuale DDG VDisk.

N.B.:
Per Dropbox e Data Guardian, se si crea un file Office nel cloud e si esegue la sincronizzazione, il file viene crittografato nel formato .xen. Pertanto, sull'unità virtuale, il file si apre nella modalità di sola lettura. Non è possibile modificarlo.

Se si eliminano tutte le cartelle sull'unità virtuale, i file vengono eliminati ma le cartelle potrebbero rimanere. In tal caso, eliminare le cartelle nel cloud.

Impostare la sincronizzazione selettiva per le cartelle

Per effettuare la sincronizzazione selettiva delle cartelle:

1. Nell'area di notifica, fare clic sull'icona di **Dropbox**.
2. Fare clic sull'icona **Impostazioni** e selezionare **Preferenze**.
3. Fare clic sulla scheda **Account**, quindi fare clic su **Sincronizzazione selettiva**.
4. Selezionare solo le cartelle o sottocartelle da sincronizzare dal computer.
5. Fare clic su **Aggiorna**.
6. Nella finestra di dialogo di conferma dell'aggiornamento, fare clic su **OK**.
7. Nella finestra delle preferenze di Dropbox, fare clic su **OK**.

Nell'area di notifica viene visualizzato un pop-up che indica che è in corso la sincronizzazione delle cartelle.

Usare l'icona di Dropbox nell'area di notifica

Nell'area di notifica, fare clic sull'icona di Dropbox.

- Per accedere al sito Web - Selezionare l'icona a forma di globo.

  N.B.:
  Se si usa Chrome oppure Firefox per aprire Dropbox.com, accertarsi di chiudere il browser al termine delle operazioni con file e cartelle. Anche se si apre un'altra scheda nel browser, il contenuto è sempre crittografato che si tratti di posta elettronica, allegati o upload effettuati tramite browser.

- Per la cartella - Selezionare l'icona della cartella di Dropbox per essere reindirizzati all'Disco virtuale DDG VDisk.

Considerazioni sulla sicurezza - Data Guardian e Dropbox

Se è in esecuzione in una macchina virtuale, non trascinare un file dal desktop del server al browser, in quanto tale file non sarà protetto. Eseguire una delle seguenti operazioni: nel browser, utilizzare l'opzione Carica; sul desktop, trascinare il file nell'Disco virtuale DDG VDisk.

FAQ su Dropbox

Domanda

Il mio account Dropbox contiene molti file in conflitto. Se li elimino dal cloud, vengono comunque ricreati.

Risposta

A volte, quando una cartella è già stata condivisa e vengono attivati più account Data Guardian contemporaneamente, questi file vengono considerati come creati nello stesso momento. Nel tentativo di conservare i file originali, Dropbox crea più file con lo stesso nome e dello stesso tipo e li posiziona nel cloud. Pertanto, Data Guardian consente di creare tutti i file senza interferenze.

Soluzione

1 Tutti coloro che condividono quel file devono deselezionare la cartella per la sincronizzazione dall'applicazione Dropbox. Vedere Dropbox for Business.
2 Una volta rimossi tutti i file e la cartella da ogni computer locale, un solo utente deve accedere al cloud ed eliminare i file duplicati.

A questo punto, tutti gli utenti possono utilizzare la sincronizzazione selettiva per aggiungere nuovamente la cartella da sincronizzare.

Box

Guida del provider di archiviazione cloud

Prima di utilizzare Data Guardian, accertarsi di conoscere le informazioni sul provider di archiviazione cloud. Il supporto per Box è disponibile all'indirizzo https://support.box.com/home.

Anche se è possibile caricare i file nel sito Web del provider di archiviazione cloud, è consigliabile lavorare con le cartelle e i file nell'Disco virtuale DDG VDisk.

N.B.:

Se si utilizza Internet Explorer per caricare i file nel provider di archiviazione cloud Box o per aprire un file, è possibile che si verifichi un ritardo nella finestra Esplora file.

N.B.:

Data Guardian non supporta gli strumenti di Box e la funzione di modifica di Box. L'uso degli strumenti di Box può causare la comparsa di una schermata blu.

Impostare la sincronizzazione selettiva per le cartelle

Per effettuare la sincronizzazione selettiva delle cartelle:

1 Nell'area di notifica, fare clic con il pulsante destro del mouse sull'icona Box e selezionare **Apri sito Web Box**.

2 Nel sito Web del client di sincronizzazione con il cloud, fare clic con il pulsante destro del mouse su una cartella e selezionare **Sincronizza cartella con computer**.

3 Nella finestra Sincronizza cartella, fare clic su **Sincronizza cartella**.

L'icona nell'area di notifica indica che è in corso l'applicazione delle impostazioni. L'operazione potrebbe richiedere alcuni minuti.

4 Al termine, accedere a **Esplora risorse** > **Sincronizzazione Box**. Le cartelle sincronizzate vengono visualizzate con un segno di spunta.

Usare l'icona di Box nell'area di notifica

Nell'area di notifica, fare clic con il pulsante destro del mouse sull'icona di Box.

- Per il sito Web - Selezionare **Apri sito Web Box**.
- Per la cartella - Selezionare **Apri cartella sincronizzazione Box**. L'utente viene reindirizzato all'Disco virtuale DDG VDisk.

FAQ sul client di sincronizzazione Box

Domanda

Sto usando il client di sincronizzazione Box. Ho creato una nuova cartella in locale a cui ho aggiunto alcuni file. Il client di sincronizzazione sembra funzionare, ma non è stato creato nulla nel cloud.

Risposta

Il client di sincronizzazione Box può richiedere tempo per raccogliere le informazioni sulle nuove cartelle e i nuovi file. Il processo può richiedere diversi minuti rispetto ad altri client di sincronizzazione. Attendere alcuni minuti per consentire il completamento dell'operazione da parte del client di sincronizzazione prima di creare nuove cartelle e nuovi file.

Domanda

Sto usando il client di sincronizzazione Box. Ho finito lo spazio libero sulla partizione principale, pertanto l'ho spostato in un'altra unità. Ora, nella cartella File Box personali sono state create una o più cartelle denominate **Nuova cartella**.

Risposta

Al momento, quando i file vengono sincronizzati tra due computer con la stessa condivisione di file, se questa cartella viene spostata in un'altra posizione, per qualsiasi cartella creata dagli altri utenti in tale condivisione di file verrà creata una cartella vuota denominata **Nuova cartella**.

Soluzione

Eliminare la nuova cartella direttamente dal cloud. Questa cartella verrà rimossa da tutti i sistemi che condividono tale cartella.

Considerazioni sulla sicurezza - Data Guardian e Box

Tutti i file creati nel sito Web del cloud Box saranno sincronizzati. Tuttavia, questi file verranno scaricati come file crittografati.

Internet Explorer potrebbe causare un ritardo durante il caricamento o l'apertura su Box.

Google Drive

Guida del provider di archiviazione cloud

Prima di utilizzare Data Guardian, accertarsi di conoscere le informazioni sul provider di archiviazione cloud. Il supporto per Google Drive è disponibile all'indirizzo https://support.google.com/drive/?hl=en#topic=14940.

Anche se è possibile caricare i file nel sito Web del provider di archiviazione cloud, è consigliabile lavorare con le cartelle e i file nell'Disco virtuale DDG VDisk.

Impostare la sincronizzazione selettiva per le cartelle

Per effettuare la sincronizzazione selettiva delle cartelle:

1 Nell'area di notifica, fare clic sull'icona di **Google Drive**.
2 Selezionare l'icona Impostazioni.
3 Selezionare **Preferenze**.
4 Per eseguire una sincronizzazione selettiva, fare clic su **Solo queste cartelle**.
5 Deselezionare la casella di controllo per le cartelle che non è necessario proteggere nel cloud.
6 Fare clic su **Applica**.
7 Per confermare, fare clic su **Continua**.

Usare l'icona di Google Drive nell'area di notifica

Nell'area di notifica, fare clic sull'icona di Google Drive.

- Per il sito Web - Selezionare **Visita Google Drive sul Web**.
- Per la cartella - Selezionare la cartella **Apri Google Drive**. L'utente viene reindirizzato all'Disco virtuale DDG VDisk

Considerazioni sulla sicurezza - Data Guardian e Google Drive

Data Guardian crittografa le cartelle e i file per proteggere i dati. Data Guardian collabora con i client di sincronizzazione, pertanto è bene essere consapevoli di questi aspetti.

- Il criterio di protezione aziendale proibisce l'uso di Documenti Google con Data Guardian. Quando si installa Data Guardian, una finestra di dialogo informa l'utente di questo criterio. Per ulteriori 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. Per Windows e Data Guardian, qualsiasi documento Documenti Google creato viene visualizzato nelle cartelle del client di sincronizzazione Documenti Google.

Tuttavia, se si apre la cartella, una finestra di dialogo avvisa che Data Guardian non può crittografare tale documento. Inoltre, per assicurare la protezione dei dati, l'amministratore può eseguire rapporti per identificare i documenti Google in fase di sincronizzazione, al fine di fornire ulteriore protezione.

- Le opzioni di Google Drive comprendono **Rimuovi** (spostamento nel cestino) ed **Elimina**. Google Drive con Data Guardian dispone solo di Elimina, per la coerenza con altre funzionalità di Data Guardian.

  N.B.:
  Se si eliminano più file dall'unità virtuale Data Guardian, ma alcuni di essi sono ancora visualizzati nel browser o nella riga di comando, eliminarli nel browser o dalla riga di comando.

- Con Google Drive, è possibile che sia mostrata un'avvertenza secondo la quale le proprietà vengono rimosse quando si copiano i file nell'Disco virtuale DDG VDisk. Questi attributi servono per la sicurezza.

OneDrive

N.B.:
Data Guardian non è supportato da Microsoft Office 365.

Guida del provider di archiviazione cloud

Prima di utilizzare Data Guardian, accertarsi di conoscere le informazioni sul provider di archiviazione cloud. Il supporto per OneDrive è disponibile all'indirizzo http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

Anche se è possibile caricare i file nel sito Web del provider di archiviazione cloud, è consigliabile lavorare con le cartelle e i file nell'Disco virtuale DDG VDisk.

Impostare la sincronizzazione selettiva per le cartelle

Per effettuare la sincronizzazione selettiva delle cartelle:

1. Nell'area di notifica, fare clic con il pulsante destro del mouse sull'icona **OneDrive** e selezionare **Impostazioni**.
2. Selezionare la scheda **Scegli cartelle** e fare clic su **Scegli cartelle**.
3. Selezionare **Scegli cartelle da sincronizzare**.
4. Viene visualizzato un elenco di cartelle. Selezionare o deselezionare le caselle di controllo per sincronizzare tali cartelle. Fare clic su **OK**.
5. Fare clic su **OK**.
6. L'icona nell'area di notifica indica che è in corso l'applicazione delle impostazioni. L'operazione potrebbe richiedere alcuni minuti.
7. Al termine, accedere a **Esplora risorse** > **OneDrive**. Le cartelle sincronizzate vengono visualizzate con un segno di spunta.

Usare l'icona di OneDrive nell'area di notifica

Nell'area di notifica:

- Per il sito Web - Fare clic con il pulsante destro del mouse e selezionare **Vai a OneDrive.com**.
- Per la cartella - Fare clic con il pulsante sinistro o destro del mouse e selezionare **Apri la cartella OneDrive personale**. L'utente viene reindirizzato all'Disco virtuale DDG VDisk.

Considerazioni sulla sicurezza - Data Guardian e OneDrive o OneDrive for Business

Vedere Considerazioni sulla sicurezza - Data Guardian e client di sincronizzazione.

Acquisire familiarità con le voci di menu dell'area di notifica di Data Guardian

Schermata Dettagli

La schermata Dettagli di Data Guardian fornisce informazioni utili, ad esempio:

- Per il supporto tecnico, è possibile fornire le informazioni sullo stato o sulla versione.
- Per visualizzare il nome di file non offuscato associato a un file .xen, selezionare **File** > **Stato file**.
- Per eseguire la ricerca di un nome file, selezionare Copia in basso a destra e incollare i contenuti in un file di testo.
- Per vedere chi è il proprietario di una cartella, selezionare Cartelle e scorrere fino alla colonna PROPRIETÀ CARTELLA.

Per accedere alla schermata Dettagli:

Fare clic sull'icona **Data Guardian** nell'area di notifica, quindi fare clic su **Dettagli...**.

Nell'angolo superiore sinistro della schermata Dettagli sono visualizzate le seguenti informazioni:

Stato servizio: stato del servizio Windows Data Guardian. I valori disponibili sono: Arrestato, Avvio in corso, Arresto in corso, In esecuzione, Ripresa in corso, Sospensione in corso, In pausa

Stato esecuzione: lo stato di attivazione del dispositivo. I valori sono: Attivo, Riattivazione in corso, Sospeso, Sospensione in corso

Modalità utente: Utente interno - Un utente con indirizzo all'interno di questo dominio

Utente esterno - Un utente con indirizzo all'esterno di questo dominio

E-mail registrazione: per gli utenti interni è l'indirizzo e-mail di dominio. Per gli utenti esterni, questo è l'indirizzo e-mail con cui hanno effettuato la registrazione.

URL server: DDP EE Server/VE Server che comunica con questo client.

Ultima modifica criterio: data e ora dell'ultima volta in cui il criterio è stato modificato e utilizzato dal client.

Versione criterio: versione del criterio generata da DDP EE Server/VE Server.

L'area **File** della schermata Dettagli mostra le seguenti informazioni:

Nome: nome del file

Cloud: mostra il nome del file offuscato o indica se il file è *Non protetto*.

Stato file: questo valore indica il proprietario della cartella. ed è determinato dall'ID della chiave.

Stato elaborazione: indica se il file necessita di una chiave o se è *Completo*.

Azienda: indica il server predefinito. Se in questa colonna è visualizzato il messaggio *Errore: chiave non proveniente dal server*, la chiave non appartiene al server dell'azienda. La chiave di un file crittografato deve appartenere al server aziendale.

Chiave: ID della chiave assegnata alla cartella (i nuovi file utilizzano tale chiave per la crittografia).

Cartella: il nome di percorso completo della cartella.

Ultima modifica: la data di ultima modifica del file.

Stato persistenza: indica se il file è su disco.

Lettura file XEN: *Vero* o *Falso*.

Creato da browser: *Vero* o *Falso*.

Per visualizzare i file di registro, nell'angolo inferiore sinistro della schermata Dettagli, fare clic su **Visualizza registro**.

N.B.:
I file di registro sono disponibili anche nel percorso **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian**.

L'area **Cartelle** della schermata Dettagli mostra le seguenti informazioni:

Nome: nome della cartella

Chiave: ID della chiave assegnata alla cartella (i nuovi file utilizzano tale chiave per la crittografia).

Client di sincronizzazione: l'ultimo client di sincronizzazione che ha sincronizzato la cartella (vedere Client di sincronizzazione cloud)

Proprietà cartella: questo valore indica il proprietario della cartella. ed è determinato dall'ID della chiave.

Ignora: le opzioni sono *Nessuno* e *Preesistenti*. I file preesistenti non sono protetti. Inoltre, se l'utente ha accesso a Gestione cartelle e ha tolto la protezione ad alcuni file, questa colonna indica che tali file non sono protetti.

Tipo di offuscamento: se l'azienda gestisce l'archiviazione cloud, questo criterio viene impostato su ogni cartella per indicare quale tipo di file .xen saranno creati nel cloud. Questo è un criterio impostato dall'amministratore. Se l'amministratore seleziona *Solo estensione*, sarà visualizzato il nome file effettivo con l'estensione ".xen". Se l'amministratore seleziona *Guid*, sarà visualizzato un nome file criptato con l'estensione ".xen". Questa è un'impostazione del criterio che ha effetto solo sulle nuove cartelle. L'impostazione predefinita è *Solo estensione*.

Menu Gestione cartelle

Alcuni manager o amministratori potrebbero dover eseguire una risoluzione temporanea dei problemi delle cartelle condivise da più utenti. È possibile richiedere all'amministratore l'autorizzazione per l'opzione Gestione cartelle. In genere, si tratta di un'opzione temporanea.

Verificare la disponibilità di aggiornamenti ai criteri

Se l'amministratore modifica un criterio e invia una notifica di aggiornamento dei criteri, accedere all'area di notifica di Windows, fare clic sull'icona **Dell Data Protection | Data Guardian** e selezionare **Verifica la disponibilità di aggiornamenti ai criteri**.

Se l'amministratore modifica un criterio per proteggere i file creati in Microsoft Word, è necessario chiudere Word per applicare tale aggiornamento.

Individuare File di registro

Per la risoluzione dei problemi, l'amministratore può richiedere i file di registro.

Per individuare i file di registro:

1 Passare a
2 Selezionare **Xendow.Service.log**.

> **N.B.:**
> Quando Xendow.Service.log raggiunge 3 MB, viene salvato come Xendow.Service1.log, quindi Xendow.Service2.log.

Aggiornare Data Guardian

La procedura consigliata è quella di disinstallare la versione precedente e di installare la versione corrente. Vedere Disinstallare Data Guardian.

Fornire un feedback a Dell

Se l'amministratore ha abilitato un criterio di feedback, l'utente può inviare feedback a Dell su questo prodotto. Il breve modulo per il feedback comprende due domande sul livello di soddisfazione, con scale di valutazione (in cui 10 indica il massimo livello di soddisfazione) e un campo per i commenti.

Per accedere al modulo, fare clic sull'icona Data Guardian nell'area di notifica e selezionare **Invia feedback**.

Se questa funzionalità non è abilitata dal criterio, l'opzione non viene visualizzata.

Possibili problemi con l'attivazione - Cloud e documenti Office protetti

Se Data Guardian è installato, ma l'icona Data Guardian nell'area di notifica non è accompagnata da un segno di spunta verde  , occorre tenere presente quanto riportato di seguito, valutando se si utilizzano la crittografia cloud, i documenti Office protetti o entrambi:

- L'accesso ai siti Web di sincronizzazione cloud è bloccato
- È impossibile connettere le applicazioni di sincronizzazione cloud ai relativi servizi Web
- Le cartelle locali sincronizzate non vengono aggiornate in questo lasso di tempo
- Data Guardian può convertire i documenti Office esistenti nella modalità protetta prima dell'attivazione. In tal caso, quando si apre un documento Office, viene visualizzata una pagina di copertina con le informazioni su come eseguire l'attivazione.

Eseguire una delle azioni seguenti:

- Riavviare ed eseguire nuovamente l'accesso con un suffisso UPN, ad esempio user_name@domain.com.
- Verificare con l'amministratore se è necessario selezionare la casella di controllo **Abilita verifica trust SSL** durante l'installazione di Data Guardian.
- Contattare l'amministratore di sistema per informazioni sulla configurazione del computer per l'attivazione manuale. Vedere Attivare Data Guardian.

Attivare Data Guardian

In genere, Data Guardian si attiva automaticamente dopo l'installazione e il riavvio del sistema. Se l'amministratore comunica che è necessario effettuare manualmente l'attivazione, seguire la procedura riportata di seguito:

1 Accedere a Windows.

Nell'area di notifica, viene visualizzata un'icona a forma di scudo con un punto esclamativo arancione.

2 Fare clic sull'icona **Data Guardian** nell'area di notifica e selezionare **Attivazione utente**.

3 Immettere l'indirizzo e-mail di dominio e la password di dominio, quindi fare clic su **Attiva**.

In caso di utente interno (con un indirizzo e-mail di dominio), ignorare il pulsante Registra. È richiesta la registrazione solo agli utenti esterni.

Quando l'attivazione è stata completata, sull'icona Data Guardian nell'area di sistema viene visualizzato un segno di spunta verde  .

4 Confermare lo stato della modalità utente. Fare clic sulla scheda nell'area di sistema e selezionare **Dettagli**.

5 Nella parte superiore, confermare la Modalità utente:

Interno: un utente con un indirizzo e-mail nel dominio dell'azienda.

Esterno: un utente con un indirizzo e-mail non di dominio. Per ulteriori informazioni, vedere Utilizzo di Data Guardian come utente esterno.

Attività utente - Documenti Office protetti senza crittografia cloud

L'amministratore ha già configurato i criteri per Data Guardian per proteggere i documenti Office.

N.B.:
Se l'azienda gestisce anche un client di sincronizzazione cloud, vedere Attività utente - Crittografia cloud e documenti Office protetti.

Panoramica delle attività

Questa panoramica riepiloga la sequenza per l'installazione e l'utilizzo di Data Guardian.

Installare Data Guardian

Attività	Descrizione	Per maggiori informazioni
Installare Data Guardian	Determinare quanto segue: L'utente deve installare Data Guardian L'amministratore ha già installato Data Guardian - Continuare con il passaggio successivo.	L'utente effettua l'installazione: vedere Installare Data Guardian su Windows. Riavviare e continuare con il passaggio successivo.
Confermare lo stato di attivazione	Verificare nell'area di notifica che l'icona di Data Guardian abbia un segno di spunta verde  .	Se l'icona è accompagnata da un punto esclamativo arancione, vedere Possibili problemi con l'attivazione - Documenti Office protetti.

Utilizzare Data Guardian

Attività	Descrizione	Per maggiori informazioni
Visualizzare il menu area di notifica	Fornisce informazioni utili riguardo file, cartelle e risoluzione dei problemi.	Acquisire familiarità con le voci di menu dell'area di notifica di Data Guardian
Proteggere i documenti Office e con attivazione macro, se è attivato un criterio	Proteggere un documento Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) al momento della creazione. Sarà protetto durante la condivisione con altri o l'archiviazione su un supporto rimovibile.	Utilizzare i documenti Office con la modalità protetta di Data Guardian • Osservare le opzioni del menu File per determinare il livello di sicurezza per i documenti Office • Utilizzare le opzioni del menu File
Condividere una cartella con altri utenti per lavorare sugli stessi file	Condividere una cartella con: Utente interno (ha un indirizzo e-mail di dominio)	Utente interno - Consultare la guida online per il provider di archiviazione cloud. Utente esterno - Vedere Utilizzo di Data Guardian come utente esterno.

Attività	Descrizione	Per maggiori informazioni
	Utente esterno (ha un indirizzo e-mail non di dominio) - Collaborare con l'amministratore.	

N.B.:

Se si apre un documento Office e viene visualizzata una pagina di copertina contenente informazioni sull'installazione o sull'attivazione, è possibile che l'amministratore abbia impostato criteri per proteggere i documenti Office. Confermare che Data Guardian sia installato e attivato. Vedere Possibili problemi con l'attivazione - Documenti Office protetti.

Installare Data Guardian per documenti Office protetti

Installare Data Guardian su Windows

Per installare Data Guardian è necessario accedere come amministratore locale del computer.

Il computer deve avere una lettera dell'alfabeto disponibile da assegnare a un'unità disco.

Il computer dovrà essere riavviato dopo l'installazione di Data Guardian.

1. Per scaricare il programma di installazione di Data Guardian, accedere alla posizione specificata dall'amministratore.
2. In base al sistema operativo in uso, selezionare il programma di installazione a 32 bit o a 64 bit, in genere **setup32.exe** o **setup64.exe**, e copiarlo sul computer locale.
3. Fare doppio clic sul file per avviare il programma di installazione.
4. Se viene visualizzato un avviso di protezione, fare clic su **Esegui**.
5. Selezionare una lingua e fare clic su **OK**.
6. Se viene richiesto di installare Microsoft Visual C++ 2010 Redistributable Package o Microsoft .NET Framework 4.0 Client Profile, fare clic su **OK**.
7. Nella schermata iniziale, fare clic su **Avanti**.
8. Leggere il contratto di licenza, accettare i termini, e fare clic su **Avanti**.
9. Nella schermata Cartella di destinazione, fare clic su **Avanti** per eseguire l'installazione nel percorso predefinito: C:\Program Files\Dell \Dell Data Protection\Dell Data Guardian\.

   In C:\, non installare Data Guardian nelle cartelle Users o Windows o nella radice di qualsiasi unità. Verrà visualizzato un messaggio di errore.
10. Nel campo `Nome server:`, immettere il nome del server con cui comunicherà questo computer, ad esempio server.domain.com. Non è necessario includere www o http(s). Queste informazioni sono fornite dall'amministratore.

    Non deselezionare la casella di controllo *Abilita verifica trust SSL*, a meno che l'amministratore non lo richieda.
11. Fare clic su **Avanti**.
12. Nella schermata Informazioni di Conferma server di attivazione, confermare che l'indirizzo URL del server è corretto. Il programma di installazione aggiunge www o http(s), e la porta. Fare clic su **Avanti**.
13. Nella finestra Tipo di gestione, selezionare questa opzione:
    - Utente interno - Un utente con un indirizzo e-mail nel dominio dell'azienda.
14. Fare clic su **Installa** per avviare l'installazione.

    Viene visualizzata una finestra di stato che mostra l'avanzamento dell'installazione.
15. Fare clic su **Fine** quando viene visualizzata la schermata Installazione completata.
16. Fare clic su **Sì** per riavviare il sistema.

    L'installazione di Data Guardian è completata.
17. Dopo il riavvio, verificare nell'area di notifica che l'icona di Data Guardian abbia un segno di spunta verde  .

Utilizzare i documenti Office con la modalità protetta di Data Guardian

Per migliorare la sicurezza aziendale, l'amministratore può abilitare un criterio per proteggere i file di queste applicazioni Office:

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm

Se una persona non autorizzata accede a un file protetto, il file rimane crittografato, ad esempio quando:

- Il file viene allegato a un messaggio e-mail
- Il file viene spostato in un browser - In alcuni client di sincronizzazione cloud, è possibile fare clic con il pulsante destro del mouse su un nome di file e selezionare **Sposta**.
- Il file viene condiviso sulla rete
- Il file viene caricato in un provider di archiviazione cloud
- Il file viene salvato su un supporto rimovibile

Per i documenti Office, potrebbe essere visualizzata una pagina di copertina con le istruzioni per l'installazione o l'attivazione di Data Guardian, ad esempio:

- È necessario installare Data Guardian.
- È necessario attivare Data Guardian.
- È stato aperto un documento Office protetto nel cloud.
- Un file di Office è stato scaricato da un computer dotato di Data Guardian a un dispositivo personale privo della medesima applicazione.
- Un utente non autorizzato accede a uno dei file Office - Viene visualizzata una pagina di copertina con un messaggio specifico dell'azienda, ma l'utente non può visualizzare il contenuto del file.

Se l'azienda utilizza la modalità protetta di Data Guardian, vedere:

- Osservare le opzioni del menu File per determinare il livello di sicurezza per i documenti Office
- Utilizzare le opzioni del menu File
- Stabilire con quale modalità di consenso esplicito sono protetti i documenti
- Opzioni di menu aggiuntive per i documenti Office protetti
- Utenti esterni e documenti Office protetti

Osservare le opzioni del menu File per determinare il livello di sicurezza per i documenti Office

Per determinare se l'amministratore ha abilitato i criteri di Data Guardian, aprire un documento Office e selezionare **File**. Se nel riquadro sinistro viene visualizzato *Salva come protetto*, è disponibile una protezione supplementare sui documenti Office.

Per stabilire il livello di sicurezza, osservare le opzioni abilitate o disabilitate:

- **Modalità Consenso esplicito** - Sono disponibili alcune opzioni per stabilire quali documenti Office proteggere.
  - *Salva con nome* e *Salva come protetto* sono abilitati - Se si decide di proteggere un documento Office, selezionare **Salva come protetto**.
  - *Stampa* ed *Esporta* possono essere abilitati o disabilitati in base ai criteri.
  - *Condividi* (*Salva e invia* per Office 2010) è abilitato.
  - Cartella **Documenti > Documenti sicuri** - Nella modalità Consenso esplicito, ma non nella modalità Protezione forzata, nella radice della cartella Documenti viene aggiunta una cartella Documenti sicuri. I documenti Office in questa cartella sono crittografati. Se si

rimuove un documento Office protetto da questa cartella, il file rimane crittografato. Se si rinomina la cartella, i contenuti della cartella rinominata sono crittografati. Se si elimina la cartella, la stessa viene ricreata.

- **Modalità Protezione forzata** - L'azienda richiede un livello di sicurezza più alto.
  - *Salva con nome* è disabilitato e *Salva come protetto* è abilitato - È necessario salvare tutti i documenti Office nella modalità protetta.
  - *Stampa* ed *Esporta* possono essere abilitati o disabilitati in base ai criteri.
  - *Condividi* (*Salva e invia* per Office 2010) è disabilitato.

    N.B.:
    Con la modalità Force-Protected, i criteri impostati consentono anche di utilizzare determinati intervalli di tempo per effettuare ricerche nel computer e individuare eventuali file Office non protetti e modificarli attivando la modalità protetta. È necessario avere effettuato l'accesso ed essere connessi alla rete perché Data Guardian cerchi eventuali file Office non protetti.

- Se si seleziona **Salva come protetto**, l'unica opzione nel campo *Salva come* è *Documento Office protetto*.

- **File > Informazioni** è diverso, ad esempio:
  - Per entrambe le modalità Consenso esplicito e Protezione forzata: viene visualizzato *Aggiungi restrizione data* se l'amministratore ha abilitato tale criterio. Vedere Migliorare la sicurezza aggiungendo restrizioni alla data.
  - Per entrambe le modalità Consenso esplicito e Protezione forzata: le informazioni sulle proprietà di questo documento di Office, come autore e data, vengono nascoste per maggiore sicurezza.
  - Stato di sola lettura: vedere di seguito per ulteriori informazioni.

    N.B.:
    L'opzione *Proteggi documento* in File > Informazioni è legata a Microsoft Office e non alla modalità protetta di Data Guardian.

Se si apre un documento Office e l'applicazione segnala che è attiva la modalità di sola lettura, controllare quanto segue:

- Se nel riquadro sinistro non viene visualizzato *Salva come protetto*, la modalità di sola lettura non è stabilita dai criteri di Data Guardian.
- Se l'amministratore ha impostato criteri per la modalità Protezione forzata, con un livello di sicurezza maggiore, i documenti Office non protetti vengono aperti nella modalità di sola lettura.

  N.B.:
  Per OneDrive, se si apre un documento Office protetto tramite **File > Apri > OneDrive** e il documento è di sola lettura, verificare di aver installato e configurato il client di sincronizzazione OneDrive.

Utilizzare le opzioni del menu File

Questa tabella elenca le opzioni del menu File per i documenti Office. A seconda del livello di sicurezza, alcune opzioni sono visualizzate in grigio.

N.B.:
Attualmente, i documenti Office incorporati non sono supportati nella modalità protetta di Office.

Menu File	Modalità di consenso esplicito e documenti Office protetti	Modalità di protezione forzata per documenti protetti e non protetti
Aprire	**I file vengono aperti come di consueto**	**I documenti non protetti vengono aperti in modalità di sola lettura.**
Salva	• Opzioni: Documento già protetto - Viene salvato come protetto. Documento non protetto - Viene salvato come non protetto. Per proteggerlo, fare clic su **Salva come protetto**. • Documento di sola lettura - Una finestra di dialogo informa che non è possibile salvare un documento non protetto. Viene visualizzata una finestra Salva con nome, nella quale occorre salvare il file con un nome diverso. • File .xen - È possibile aprire e salvare il file .xen nella modalità protetta, ma il file viene rimosso dal cloud. Il documento Office ha la sua normale estensione, ma è protetto. **N.B.:** **Nell'unità virtuale, se l'utente fa clic con il pulsante destro del mouse per creare un nuovo documento Office, il documento viene salvato come file .xen. È necessario salvarlo manualmente come documento protetto.**	• Il documento è protetto. • Documento di sola lettura - È possibile modificarlo, ma non salvare l'originale. Quando si fa clic su Salva viene visualizzata la finestra Salva come protetto ed è necessario salvare il documento nella modalità protetta con un nuovo nome. • Documenti remoti - Se si apre un documento non protetto in una posizione remota, è necessario salvarlo sull'unità locale per modificarlo e salvarlo. Non è possibile salvarlo nella posizione remota. **N.B.:** **Facendo clic su Salva viene aperta la finestra Salva con nome e l'unica opzione nel campo Salva come è Documento Office protetto (Documento, Presentazione o Cartella di lavoro).** • File .xen - È possibile aprire e salvare il file .xen nella modalità protetta, ma il file viene rimosso dal cloud. Il documento Office ha la sua normale estensione, ma è protetto.
Salva con nome	**Presenta le opzioni standard (ma non la modalità protetta)**	**Disabilitato**
Salva con nome protetto	**L'unica opzione nel campo Salva come è Documento Office protetto**	**L'unica opzione nel campo Salva come è Documento Office protetto**
Stampa	**Può essere attivato o disattivato in base ai criteri impostati dall'amministratore. Se l'opzione di menu è abilitata, un criterio potrebbe applicare una filigrana, contenente il nome utente, il nome di dominio e l'ID del computer, su ogni pagina stampata.**	**A seconda del criterio, questa opzione può essere abilitata o disabilitata. Se l'opzione di menu è abilitata, un criterio potrebbe applicare una filigrana, contenente il nome utente, il nome di dominio e l'ID del computer, su ogni pagina stampata.**
Condividi	**Abilitata**	**Disabilitato**
Salva e invia (Office 2010)	**Abilitata**	**Disabilitato Se Stampa è abilitato, è possibile selezionare Stampa per stampare il documento in formato PDF.**
Esporta (Office 2013 e versioni successive)	**Può essere attivato o disattivato in base ai criteri impostati dall'amministratore.**	**Può essere attivato o disattivato in base ai criteri impostati dall'amministratore.**
Esporta protetto (Office 2013 e versioni successive)	Se l'opzione di menu Esporta è disattivata ed Esportazione protetta è abilitata, il documento viene esportato con una filigrana, contenente il nome utente, il nome di dominio e l'ID computer, su ogni pagina. **N.B.:** Se si esporta un documento nella modalità protetta per un utente esterno, egli potrà aprire e visualizzare il file, ma non esportarlo o stamparlo.	Se l'opzione di menu Esporta è disattivata ed Esportazione protetta è abilitata, il documento viene esportato con una filigrana, contenente il nome utente, il nome di dominio e l'ID computer, su ogni pagina. **N.B.:** Se si esporta un documento nella modalità protetta per un utente esterno, egli potrà aprire e visualizzare il file, ma non esportarlo o stamparlo.

Lavorare online con i documenti Office protetti

Durante la creazione di documenti Office protetti, la procedura migliore prevede di lavorare online in modo da generare le chiavi per tali documenti. Se il computer deve essere riformattato e sono stati creati documenti Office protetti offline, è necessario informare l'amministratore.

Lavorare online con i documenti con attivazione macro protetti

Nel caso di un documento con attivazione macro protetto, la macro esiste ma è bloccata. Al momento Data Guardian è in grado di controllare un documento con attivazione macro solo dopo aver chiuso e riaperto il nuovo documento protetto (.docm, .pptm, .xlsm). Inoltre, se si salva un documento con attivazione macro protetto come documento non protetto, è necessario chiudere e riaprire il documento per eseguire le macro.

Allegare un documento Office protetto a un messaggio e-mail di Outlook

Per allegare un documento Office protetto a un messaggio e-mail di Outlook, selezionare **Inserisci** anziché *Inserisci come testo*. Il comando *Inserisci come testo* incolla il contenuto del documento direttamente nel corpo del messaggio e-mail, pertanto il contenuto non è più protetto.

Risoluzione dei problemi per la modalità di consenso esplicito

In File > Informazioni, se il comando Stampa è disattivato, significa che un criterio di Data Guardian ha disabilitato la stampa per i documenti Office protetti. Al momento, quando si fa clic con il pulsante destro del mouse su un file Office protetto in Esplora risorse, l'opzione Stampa non è disattivata. Tuttavia, se si seleziona Stampa, si verifica quanto segue:

- Word - Una finestra di dialogo indica che Word ha smesso di funzionare.
- Excel - Una finestra di dialogo indica che il comando Stampa è disattivato da un criterio.
- PowerPoint - Una finestra di dialogo indica che il comando Stampa è disattivato da un criterio. Se si fa clic su OK, viene stampata una pagina di copertina che comunica che il documento è protetto.

Stabilire con quale modalità di consenso esplicito sono protetti i documenti

Se si utilizza la modalità di protezione forzata, tutti i documenti Office vengono protetti. Se si utilizza la modalità di consenso esplicito e si desidera confermare se un documento è protetto o meno, aprire il documento e verificare che sulla barra del titolo sia indicato che il documento è protetto.

Opzioni di menu aggiuntive per i documenti Office protetti

Il tipo di documento Office, protetto o non protetto, può influenzare le operazioni riportate di seguito.

Clic con il pulsante destro del mouse > Proteggi

È possibile fare clic con il pulsante destro del mouse su un documento Office e selezionare **Proteggi**. È necessario aggiungere contenuti perché l'opzione di menu sia visualizzata. Non è possibile proteggere un documento vuoto.

Proprietà file > scheda Dell Data Guardian

Per i documenti Office protetti, è possibile fare clic con il pulsante destro del mouse e selezionare **Proprietà**: viene visualizzata una scheda **Dell Data Guardian** contenente informazioni quali l'ID chiave del file e i dati di accesso ed embargo.

Incolla

Se l'amministratore imposta un criterio per proteggere i documenti Office:

- È possibile copiare e incollare i dati nel documento protetto originale.

- Non è possibile copiare o incollare da un documento protetto a un documento non protetto. Negli Appunti non viene visualizzato nulla e un messaggio di testo specifico per l'azienda comunica che non è possibile incollare nel documento non protetto o non gestito.

  N.B.:
  Se si taglia testo da un documento protetto e si riceve il messaggio in un documento non protetto, fare clic su **Annulla** nel documento protetto per recuperare il testo.

Trascinamento nella modalità protetta

È possibile trascinare e rilasciare contenuti in un documento Word protetto. Attualmente, il trascinamento è disabilitato per i file Excel e PowerPoint protetti.

Stampa per buste ed etichette

Se l'amministratore ha impostato un criterio per aggiungere una filigrana durante la stampa di un documento Office protetto, seguire questi passaggi per stampare buste o etichette:

1 In un documento Word, selezionare la scheda **Lettere**.
2 Selezionare l'opzione **Buste** o **Etichette**.
3 Dopo aver immesso l'indirizzo o l'indirizzo di risposta, fare clic su **Stampa**.

N.B.: Se si utilizza un'altra opzione per la stampa e l'amministratore ha impostato un criterio per aggiungere una filigrana ai documenti Office stampati, sulla busta o sull'etichetta sarà visualizzata una filigrana.

Manomissione e documenti Office protetti

Data Guardian è in grado di analizzare i documenti Office protetti per rilevare alcune forme di manomissione.

Se un utente interno manomette un documento Office protetto:

- Data Guardian può riparare o ripristinare alcune manomissioni.
- Per eventuali manomissioni che non possono essere riparate, potrebbe essere visualizzata una finestra di dialogo che segnala che il file è stato manomesso e occorre contattare l'amministratore.

Se un utente non autorizzato apre un documento Office protetto, viene visualizzata solo la pagina di copertina. Se l'utente non autorizzato modifica la pagina di copertina, Data Guardian ripristinerà la pagina di copertina quando un utente autorizzato salverà nuovamente il file protetto.

Utenti esterni e documenti Office protetti

Migliorare la sicurezza aggiungendo restrizioni alla data

Con Data Guardian, un documento Office protetto viene caricato nel cloud e condiviso:

- Tutti gli utenti interni di Data Guardian possono visualizzarlo.
- Gli utenti esterni possono visualizzarlo in base ai criteri impostati.

Per una maggiore sicurezza con gli utenti esterni, è possibile aggiungere una restrizione di data per limitare il tempo per cui un utente esterno può visualizzare un documento Office protetto.

1 Selezionare **File > Informazioni > Restrizione data**.
2 Dal menu a discesa, selezionare la data e l'ora di inizio e di fine entro le quali un utente esterno può visualizzare il documento.

N.B.:
La data e l'ora di inizio possono essere nel futuro, se si desidera inviare il documento ma impedire all'utente esterno di visualizzarlo fino alla data e all'ora previste.

3 Fare clic su **OK**.
Il documento viene salvato, protetto, chiuso e riaperto.

N.B.:
Se si modificano le date per un documento Office non protetto e si fa clic su Annulla, Data Guardian continua a proteggere il file.

N.B.:
Attualmente, se si aggiungono restrizioni di data a un documento Office protetto e si prevede di salvarlo in un'unità di rete, è necessario salvare il file in locale e poi copiarlo in rete.

Se un utente esterno apre un file dopo l'intervallo di date e orari, una finestra di dialogo indica che il file presenta restrizioni di accesso e che l'utente esterno può contattare l'autore del file. La finestra di dialogo non mostra le date all'utente esterno.

Se si imposta il campo Data di inizio su una data o un orario futuri e l'utente esterno apre il file prima di tale periodo, viene visualizzata una finestra di dialogo che comunica che il file non può essere aperto fino alla data e all'ora indicate a causa di restrizioni di accesso.

Acquisire familiarità con le voci di menu dell'area di notifica di Data Guardian

Schermata Dettagli

La schermata Dettagli di Data Guardian fornisce informazioni utili, ad esempio:

- Per il supporto tecnico, è possibile fornire le informazioni sullo stato o sulla versione.
- Per visualizzare il nome di file non offuscato associato a un file .xen, selezionare **File** > **Stato file**.
- Per eseguire la ricerca di un nome file, selezionare Copia in basso a destra e incollare i contenuti in un file di testo.
- Per vedere chi è il proprietario di una cartella, selezionare Cartelle e scorrere fino alla colonna PROPRIETÀ CARTELLA.

Per accedere alla schermata Dettagli:

Fare clic sull'icona **Data Guardian** nell'area di notifica, quindi fare clic su **Dettagli...**.

Nell'angolo superiore sinistro della schermata Dettagli sono visualizzate le seguenti informazioni:

Stato servizio: stato del servizio Windows Data Guardian. I valori disponibili sono: Arrestato, Avvio in corso, Arresto in corso, In esecuzione, Ripresa in corso, Sospensione in corso, In pausa

Stato esecuzione: lo stato di attivazione del dispositivo. I valori sono: Attivo, Riattivazione in corso, Sospeso, Sospensione in corso

Modalità utente: Utente interno - Un utente con indirizzo all'interno di questo dominio

Utente esterno - Un utente con indirizzo all'esterno di questo dominio

E-mail registrazione: per gli utenti interni è l'indirizzo e-mail di dominio. Per gli utenti esterni, questo è l'indirizzo e-mail con cui hanno effettuato la registrazione.

URL server: DDP EE Server/VE Server che comunica con questo client.

Ultima modifica criterio: data e ora dell'ultima volta in cui il criterio è stato modificato e utilizzato dal client.

Versione criterio: versione del criterio generata da DDP EE Server/VE Server.

L'area **File** della schermata Dettagli mostra le seguenti informazioni:

Nome: nome del file

Cloud: mostra il nome del file offuscato o indica se il file è *Non protetto*.

Stato file: questo valore indica il proprietario della cartella. ed è determinato dall'ID della chiave.

Stato elaborazione: indica se il file necessita di una chiave o se è *Completo*.

Azienda: indica il server predefinito. Se in questa colonna è visualizzato il messaggio *Errore: chiave non proveniente dal server*, la chiave non appartiene al server dell'azienda. La chiave di un file crittografato deve appartenere al server aziendale.

Chiave: ID della chiave assegnata alla cartella (i nuovi file utilizzano tale chiave per la crittografia).

Cartella: il nome di percorso completo della cartella.

Ultima modifica: la data di ultima modifica del file.

Stato persistenza: indica se il file è su disco.

Lettura file XEN: *Vero* o *Falso*.

Creato da browser: *Vero* o *Falso*.

Per visualizzare i file di registro, nell'angolo inferiore sinistro della schermata Dettagli, fare clic su **Visualizza registro**.

N.B.:
I file di registro sono disponibili anche nel percorso **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian**.

L'area **Cartelle** della schermata Dettagli mostra le seguenti informazioni:

Nome: nome della cartella

Chiave: ID della chiave assegnata alla cartella (i nuovi file utilizzano tale chiave per la crittografia).

Client di sincronizzazione: l'ultimo client di sincronizzazione che ha sincronizzato la cartella (vedere Client di sincronizzazione cloud)

Proprietà cartella: questo valore indica il proprietario della cartella. ed è determinato dall'ID della chiave.

Ignora: le opzioni sono *Nessuno* e *Preesistenti*. I file preesistenti non sono protetti. Inoltre, se l'utente ha accesso a Gestione cartelle e ha tolto la protezione ad alcuni file, questa colonna indica che tali file non sono protetti.

Tipo di offuscamento: se l'azienda gestisce l'archiviazione cloud, questo criterio viene impostato su ogni cartella per indicare quale tipo di file .xen saranno creati nel cloud. Questo è un criterio impostato dall'amministratore. Se l'amministratore seleziona *Solo estensione*, sarà visualizzato il nome file effettivo con l'estensione ".xen". Se l'amministratore seleziona *Guid*, sarà visualizzato un nome file criptato con l'estensione ".xen". Questa è un'impostazione del criterio che ha effetto solo sulle nuove cartelle. L'impostazione predefinita è *Solo estensione*.

Menu Gestione cartelle

Alcuni manager o amministratori potrebbero dover eseguire una risoluzione temporanea dei problemi delle cartelle condivise da più utenti. È possibile richiedere all'amministratore l'autorizzazione per l'opzione Gestione cartelle. In genere, si tratta di un'opzione temporanea.

Individuare File di registro

Per la risoluzione dei problemi, l'amministratore può richiedere i file di registro.

Per individuare i file di registro:

1 Passare a
2 Selezionare **Xendow.Service.log**.

> **N.B.:**
> Quando Xendow.Service.log raggiunge 3 MB, viene salvato come Xendow.Service1.log, quindi Xendow.Service2.log.

Verificare la disponibilità di aggiornamenti ai criteri

Se l'amministratore modifica un criterio e invia una notifica di aggiornamento dei criteri, accedere all'area di notifica di Windows, fare clic sull'icona **Dell Data Protection | Data Guardian** e selezionare **Verifica la disponibilità di aggiornamenti ai criteri**.

Se l'amministratore modifica un criterio per proteggere i file creati in Microsoft Word, è necessario chiudere Word per applicare tale aggiornamento.

Aggiornare Data Guardian

La procedura consigliata è quella di disinstallare la versione precedente e di installare la versione corrente. Vedere Disinstallare Data Guardian.

Fornire un feedback a Dell

Se l'amministratore ha abilitato un criterio di feedback, l'utente può inviare feedback a Dell su questo prodotto. Il breve modulo per il feedback comprende due domande sul livello di soddisfazione, con scale di valutazione (in cui 10 indica il massimo livello di soddisfazione) e un campo per i commenti.

Per accedere al modulo, fare clic sull'icona Data Guardian nell'area di notifica e selezionare **Invia feedback**.

Se questa funzionalità non è abilitata dal criterio, l'opzione non viene visualizzata.

Possibili problemi con l'attivazione - Documenti Office protetti

Se Data Guardian è installato, ma l'icona Data Guardian nell'area di notifica non è accompagnata da un segno di spunta verde  , occorre tenere presente quanto riportato di seguito:

- Data Guardian può convertire i documenti Office esistenti nella modalità protetta prima dell'attivazione. In tal caso, quando si apre un documento Office, viene visualizzata una pagina di copertina con le informazioni su come eseguire l'attivazione.

Eseguire una delle azioni seguenti:

- Riavviare ed eseguire nuovamente l'accesso con un suffisso UPN, ad esempio user_name@domain.com.
- Verificare con l'amministratore se è necessario selezionare la casella di controllo **Abilita verifica trust SSL** durante l'installazione di Data Guardian.

- Contattare l'amministratore di sistema per informazioni sulla configurazione del computer per l'attivazione manuale. Vedere Attivare Data Guardian.

Attivare Data Guardian

In genere, Data Guardian si attiva automaticamente dopo l'installazione e il riavvio del sistema. Se l'amministratore comunica che è necessario effettuare manualmente l'attivazione, seguire la procedura riportata di seguito:

1 Accedere a Windows.
Nell'area di notifica, viene visualizzata un'icona a forma di scudo con un punto esclamativo arancione.
2 Fare clic sull'icona **Data Guardian** nell'area di notifica e selezionare **Attivazione utente**.
3 Immettere l'indirizzo e-mail di dominio e la password di dominio, quindi fare clic su **Attiva**.
In caso di utente interno (con un indirizzo e-mail di dominio), ignorare il pulsante Registra. È richiesta la registrazione solo agli utenti esterni.

Quando l'attivazione è stata completata, sull'icona Data Guardian nell'area di sistema viene visualizzato un segno di spunta verde  .
4 Confermare lo stato della modalità utente. Fare clic sulla scheda nell'area di sistema e selezionare **Dettagli**.
5 Nella parte superiore, confermare la Modalità utente:
Interno: un utente con un indirizzo e-mail nel dominio dell'azienda.

Esterno: un utente con un indirizzo e-mail non di dominio. Per ulteriori informazioni, vedere Utilizzo di Data Guardian come utente esterno.

Uso di Data Guardian Mobile con iOS o Android

La presente sezione descrive le informazioni di base sull'utilizzo di Data Guardian Mobile con dispositivi iOS o Android. Quando l'amministratore imposta un criterio per abilitare Data Guardian, i file vengono crittografati e protetti nel cloud. Tuttavia, è possibile utilizzare l'app Data Guardian Mobile per visualizzarli sul proprio dispositivo mobile.

Prerequisito

Prima di utilizzare l'app Data Guardian è necessario conoscere il nome del Dell Data Protection Server aziendale, ad esempio server.domain.com. Queste informazioni sono fornite dall'amministratore.

Guida introduttiva a Data Guardian Mobile

Seguire questa procedura per utilizzare Data Guardian Mobile.

Attività	Descrizione	Consultare questa sezione
Installare Data Guardian	Determinare quanto segue: L'amministratore ha già installato L'utente deve installare	L'amministratore effettua l'installazione: toccare l'app Data Guardian e accedere. L'utente effettua l'installazione: vedere uno di questi argomenti: Installazione su un dispositivo iOS Installazione su un dispositivo Android
Accedere all'account del provider di archiviazione cloud	Sul dispositivo, passare alla pagina iniziale dell'app Data Guardian e toccare il provider di archiviazione cloud.	Consultare una delle sezioni seguenti: Accedere al proprio account del provider di archiviazione cloud da iOS Accedere al proprio account del provider di archiviazione cloud per Android

L'app Data Guardian Mobile indica il client di sincronizzazione cloud utilizzato dall'azienda e consente di scaricarlo.

N.B.:
Se sul dispositivo è stata scaricata l'app del client di sincronizzazione cloud, Data Guardian non crittografa le cartelle o i file caricati direttamente dall'app. Per crittografare e proteggere i file è necessario utilizzare l'app Data Guardian per caricarli.

Per proteggere i dati nel cloud Data Guardian li crittografa. Pertanto, l'app Data Guardian deve essere installata sul dispositivo mobile per visualizzare i file crittografati.

- I file Office protetti (.docx, .pptx, .potx, .xlsx) mantengono le loro estensioni di file.
- I file non di Office nel cloud hanno un'estensione .xen.

Se una persona non autorizzata accede all'account di archiviazione cloud e scarica un file su un dispositivo mobile su cui **non** è installato Data Guardian, la persona non è in grado di aprire o visualizzare i file. Se tale persona apre un file Office protetto, viene visualizzata solo una pagina di copertina che indica che la persona non può visualizzare il documento senza Data Guardian. In questo modo i dati sono più sicuri.

Nei dispositivi mobili è possibile:

- Creare cartelle
- Caricare e scaricare file

  N.B.:
  Con Data Guardian è necessario avviare il caricamento e lo scaricamento dal dispositivo. Per i file che devono essere crittografati durante il caricamento nel cloud, è necessario caricarli dalla schermata iniziale di Data Guardian, non dall'app del client di sincronizzazione cloud. Quando si tocca un file, Data Guardian lo decritta automaticamente e lo visualizza in chiaro all'interno dell'app. Tuttavia, nel cloud, il file rimane protetto in quanto file con estensione .xen.

- Aggiungere un file ai Preferiti
  - Per iOS, consultare il drawer di navigazione. Per Android, tenere premuto il nome del file.
- Eliminare cartelle e file
- Accettare una cartella condivisa da un utente interno

  N.B.:
  Se un utente interno condivide una cartella mediante Data Guardian, è necessario accedere al sito Web di archiviazione cloud e spostarla nella cartella radice, oppure scaricare la cartella condivisa, per visualizzarla sul dispositivo.

- Condividere un documento con un utente esterno (se è abilitato il criterio per gli utenti esterni) - Per iOS, vedere Visualizzazione dei criteri di archiviazione cloud di Data Guardian per il dispositivo iOS.
- Modificare i file Office .docx e .ppt.

  N.B.:
  Attualmente, i file .csv e .csv.xen non possono essere modificati su dispositivi mobili.

Documenti Office protetti nella modalità offline

Quando si crea un documento Office protetto o un documento con attivazione macro protetto e si è offline, viene creata una chiave per il documento. Quando il dispositivo torna online, le chiavi vengono caricate nel Dell Server. Se il dispositivo rimane offline per tre giorni, una notifica segnala che Data Guardian non è stato in grado di contattare Dell Server. La notifica viene visualizzare tutti i giorni fino a quando non ci si connette alla rete. Per visualizzare i file crittografati, il dispositivo mobile deve essere online.

Protezione aggiuntiva tramite geofencing

In base ai criteri impostati dall'amministratore, i dispositivi mobili possono disporre di una protezione aggiuntiva, per la quale i documenti Office protetti e i file .xen non possono essere aperti al di fuori di una specifica regione. È necessario trovarsi in una regione approvata per aprire i file protetti. Attualmente, le regioni sono gli Stati Uniti e il Canada. È necessario abilitare i servizi di localizzazione sul dispositivo per utilizzare il geofencing. Se la funzione di geofencing viene abilitata dall'amministratore e i servizi di localizzazione sono disattivati, l'accesso ai file viene negato.

Utilizzare un PIN

L'amministratore può impostare un criterio per richiedere un PIN.

Data Guardian su un dispositivo iOS

Installazione su un dispositivo iOS

1. Sul dispositivo, toccare **App Store** e cercare **Data Guardian Mobile**.
2. Selezionare e installare l'app **Data Guardian**.
3. Nel campo Server della schermata di accesso, immettere il nome host del Dell Data Protection Server aziendale, ad esempio server.domain.com.
4. Immettere nome utente e password.
5. Toccare **Accedi**.

Accedere al proprio account del provider di archiviazione cloud da iOS

Dopo aver effettuato l'accesso a Data Guardian, un criterio Data Guardian determina quali provider di archiviazione cloud vengono visualizzati nella schermata iniziale. L'amministratore può designare un provider di archiviazione cloud specifico da usare all'interno dell'azienda.

Il drawer di navigazione dispone di opzioni aggiuntive.

Per accedere a un account:

1 Nella pagina iniziale di Data Guardian, toccare il provider di archiviazione cloud.
2 Eseguire una delle azioni seguenti, consultando le istruzioni online:
   - Creare un account con il provider di archiviazione cloud.
   - Accedere a un account esistente del provider di archiviazione cloud.

> **N.B.:**
> Per maggiori informazioni, consultare la guida del provider di archiviazione cloud.

Scollegare un provider di archiviazione cloud

Se l'utente ha più di un account con lo stesso provider di archiviazione cloud, non è possibile essere connessi a entrambi contemporaneamente. L'utente deve deselezionare la casella di controllo per scollegarsi e disconnettersi dall'account attuale, quindi effettuare l'accesso con le credenziali dell'altro account.

1 Aprire il drawer di navigazione di Data Guardian e toccare **Impostazioni**.
2 Toccare **Scollega**.

Visualizzare i criteri di archiviazione cloud di Data Guardian per il dispositivo iOS

1 Nel drawer di navigazione di Data Guardian, toccare **Impostazioni**.
2 Toccare **Criteri**.
   L'elenco può comprendere:
   - Revisione - Numero di criteri rivisti
   - Offusca nomi file - L'impostazione predefinita è **No**
   - Client di sincronizzazione cloud - Il criterio dovrebbe essere impostato su **Crittografa**
   - Visualizzatori esterni - Se è impostato su **Sì**, il criterio di condivisione è abilitato. Quando si apre un documento nell'app, un'opzione del menu permette di condividere i file.

Disinstallare l'app Data Guardian

1 Nel drawer delle app di iOS, toccare e tenere premuto sull'icona **Data Guardian**.
2 Toccare **x**.
3 Toccare **Elimina**.

Risoluzione dei problemi di iOS e Data Guardian

Su un dispositivo iOS, se si apre un documento Office protetto di dimensioni superiori a 25 MB e viene visualizzata una finestra di dialogo di memoria insufficiente, l'avviso proviene da Polaris Office, non da Data Guardian. Se il dispositivo dispone di memoria sufficiente, chiudere il file e riaprirlo.

Con Dropbox for Business, se si contrassegna un file come disponibile offline e quindi si rinomina il file nel sito Web Dropbox, il file non sarà aperto sul dispositivo iOS con l'app Data Guardian.

Data Guardian su un dispositivo Android

Installazione su un dispositivo Android

1 Sul dispositivo, accedere a **Google Play** e cercare **Data Guardian Mobile**.
2 Selezionare e installare l'app **Data Guardian**.
3 Nel campo Server della schermata di accesso, immettere il nome del Dell Data Protection Server aziendale, ad esempio server.domain.com.
4 Immettere nome utente e password.
5 Toccare **Accedi**.

L'account è stato attivato.

Accedere al proprio account del provider di archiviazione cloud per Android

Dopo aver effettuato l'accesso a Data Guardian, un criterio Data Guardian determina quali provider di archiviazione cloud vengono visualizzati. L'amministratore può designare un provider di archiviazione cloud specifico da usare all'interno dell'azienda e bloccare gli altri.

Per accedere a un account:

1 Nella pagina iniziale di Data Guardian, toccare il provider di archiviazione cloud.
2 Eseguire una delle azioni seguenti, seguendo le schermate online:
   - Creare un account con il provider di archiviazione cloud.
   - Accedere a un account esistente del provider di archiviazione cloud.

> **N.B.:**
> Per maggiori informazioni, consultare la guida del provider di archiviazione cloud.

3 Dopo aver effettuato l'accesso all'account, aprire il drawer di navigazione e toccare **Impostazioni**. Quando si ottiene l'accesso a un provider di archiviazione cloud, un segno di spunta viene visualizzato nella casella di controllo.

> **N.B.:**
> Se l'utente ha più di un account con lo stesso provider di archiviazione cloud, non è possibile essere connessi a entrambi contemporaneamente. L'utente deve deselezionare la casella di controllo per scollegarsi e disconnettersi dall'account attuale, quindi effettuare l'accesso con le credenziali dell'altro account.

> **N.B.:**
> Per OneDrive e Dropbox, se non si è in grado di condividere un file da Applicazioni e il file condivide un collegamento con l'app Data Guardian, condividere il file dall'app Browser file sul dispositivo.

Disinstallare l'app Data Guardian

1 Nel drawer delle app di Android, toccare **Impostazioni**.
2 In **Impostazioni**, toccare **App**.
3 Premere in corrispondenza dell'icona **Data Guardian**.
4 Trascinare l'icona sull'opzione Disinstalla.
5 Fare clic su **OK**.

Considerazioni sulla sicurezza - Data Guardian e client di sincronizzazione

Data Guardian crittografa le cartelle e i file per proteggere i dati. Data Guardian collabora con i client di sincronizzazione, pertanto è bene essere consapevoli di questi aspetti.

Google Drive

Google Drive contiene l'app Documenti Google che permette agli utenti di collaborare sui documenti in tempo reale. Tuttavia, la collaborazione avviene su un server Google, non in Dell Data Protection EE Server/VE Server. Pertanto, i file non sono crittografati. Per i

dispositivi Android e iOS con Data Guardian, l'accesso a questi documenti Google è bloccato. Cambia lievemente a seconda della piattaforma:

- Android
- iOS - viene visualizzato un messaggio.

OneDrive e OneDrive for Business

Con OneDrive for Business, quando l'utente avvia il download di diversi file e poi lo annulla, l'applicazione annullerà il download dei file che non sono ancora stati scaricati ma porterà a termine i download in corso. Questo è un problema di Microsoft. Pertanto, accertarsi che il download dei file sia completo prima di annullarlo.

Registri

Per ragioni di sicurezza, nei dispositivi mobili non sono disponibili file di registro.

Inviare un feedback a Dell

Se l'amministratore ha abilitato un criterio di feedback, l'utente può inviare feedback a Dell su questo prodotto. Se questa funzionalità non è abilitata dal criterio, l'opzione non viene visualizzata.

Per inviare un feedback:

1 Nel drawer di navigazione di Data Guardian, toccare **Feedback**.
2 Rispondendo ad alcune brevi domande l'utente può classificare il proprio livello di soddisfazione (10 indica il livello massimo di soddisfazione) e lasciare un commento.

Utilizzo di Data Guardian come utente esterno

Anche un utente esterno, che dispone di un indirizzo e-mail non di dominio, ha la possibilità di utilizzare Data Guardian. Di seguito sono elencati alcuni esempi.

- L'utente ha installato e attivato Data Guardian essendo parte dell'azienda, ma deve condividere file protetti o collaborare su file protetti con un utente esterno all'azienda.
- L'utente dispone di un indirizzo e-mail aziendale appartenente al dominio dell'azienda, ma desidera installare e attivare Data Guardian anche su un computer o dispositivo mobile con un indirizzo e-mail personale, non di dominio. In questo modo può interagire con i file protetti anche da un indirizzo e-mail non appartenente al dominio aziendale.

Per gli utenti esterni, vedere Requisiti del server. Inoltre, il dominio o l'utente non devono trovarsi nella blacklist dell'azienda.

N.B.:
Se l'azienda effettua l'aggiornamento, sarà eseguita la migrazione degli utenti esterni che sono stati registrati con Secure Lifecycle 1.0 o versioni successive.

Attività dell'utente interno

Per condividere file protetti con un utente esterno, è possibile inviare un documento Office protetto o un file .xen tramite un messaggio e-mail di Outlook. Un prompt di conferma ricorda all'utente che la chiave del file protetto sarà condivisa.

N.B.:
Se un utente esterno invia per e-mail un file protetto, le chiavi non vengono condivise.

È anche possibile utilizzare l'opzione Concedi accesso per condividere i file sicuri con un utente esterno. È necessario:

- Mettere a disposizione dell'utente esterno uno o più file sicuri.
  - Documenti Office protetti - Concedere l'accesso a uno o più file sicuri tramite:
    - Unità di rete o cartella locale
    - E-mail
    - Supporto rimovibile
    - Condivisione di rete
  - File .xen non di Office - Creare una cartella da condividere sul client di sincronizzazione e aggiungere i file.
- Concedere all'utente esterno l'accesso a uno o più file.

Se si prevede di condividere file .xen non di Office, è necessario aggiungerli a una cartella del client di sincronizzazione e quindi concedere l'accesso. Per i file Office protetti, è necessario concedere l'accesso. Le procedure potrebbero variare a seconda del metodo o del client di sincronizzazione utilizzato.

Condividere una cartella sul client di sincronizzazione per condividere file .xen

1 In Windows Explorer, accedere al client di sincronizzazione, creare una cartella e caricare il file da condividere con un utente esterno. Vedere Visualizzare cartelle e file sul computer locale e nel cloud.

I documenti Office protetti possono trovarsi sull'Disco virtuale DDG VDisk, nella cartella Data Guardian o sul desktop.

N.B.:
Con i file Office protetti, non è possibile selezionare una cartella.

Si apre una pagina *Condivisione accesso a documenti protetti* con una colonna che mostra i file selezionati.

2 Nel sito Web del client di sincronizzazione, dare conferma che il file e la cartella sono stati creati e crittografati.
Quando si aggiunge un file .xen a una nuova cartella sull'Disco virtuale DDG VDisk, Data Guardian aggiunge un documento, *Come accedere ai file sicuri.html*, alla cartella sul sito Web. Questo file viene usato solo quando la cartella viene condivisa con un utente esterno.

3 Nel sito Web del client di sincronizzazione, fare clic con il pulsante destro del mouse sulla cartella creata, quindi fare clic su **Condividi**.
Si apre una finestra che permette di immettere l'account di posta elettronica di un utente esterno. La procedura cambia in base al client di sincronizzazione usato. Per i collegamenti alle informazioni relative al client di sincronizzazione, vedere Utilizzare il client di sincronizzazione cloud sull'unità virtuale DDG VDisk.

4 Concedere l'accesso ai singoli file all'interno della cartella che si desidera condividere.

Concedere l'accesso a uno o più file Office protetti

Per tutti i file condivisi con utenti esterni è necessario concedere l'accesso.

1 Fare clic con il pulsante destro del mouse su un file sicuro e selezionare **Concedi accesso a file protetto**. È possibile selezionare uno o più file, fino a 50.
2 Nel campo *Indirizzo e-mail per condivisione*, immettere l'indirizzo e-mail dell'utente non di dominio e fare clic su **Aggiungi**.
3 Ripetere questo passaggio per aggiungere fino a dieci indirizzi e-mail.
4 Fare clic su **OK**.
Una finestra di dialogo segnala che la condivisione è riuscita o che l'indirizzo e-mail non è autorizzato a ricevere file protetti.
5 La procedura ottimale prevede di informare l'utente esterno che riceverà un messaggio e-mail con le istruzioni per registrarsi con un Dell Server, scaricare e attivare Dell Data Protection | Data Guardian e quindi visualizzare i file protetti condivisi.

Approvare o rifiutare l'accesso quando un utente esterno richiede l'accesso

Un utente esterno che ha installato Data Guardian può richiedere l'accesso a un documento protetto, se non ha la chiave per tale documento.

1 Se si riceve un messaggio e-mail da un utente esterno, in cui viene richiesto l'accesso a un documento protetto, è possibile visualizzare il nome dell'utente esterno e il file richiesto.
2 Selezionare **Approva** o **Nega**.
Viene inviato un messaggio e-mail all'utente esterno. In caso di approvazione, viene condivisa la chiave per il documento protetto.

Se l'utente non è disponibile, anche l'amministratore ha la possibilità di approvare o rifiutare l'accesso.

Attività dell'utente esterno

Per aprire e visualizzare un documento di Data Guardian, l'utente esterno deve:

- Registrarsi in Data Guardian
- Installare Data Guardian - L'utente esterno deve disporre dei diritti di amministratore sul suo computer

- Se l'utente interno condivide una cartella mediante un client di sincronizzazione, l'utente esterno deve disporre di un account del client di sincronizzazione. Vedere Installare un client di sincronizzazione cloud e quindi Utilizzare il client di sincronizzazione cloud sull'unità virtuale DDG VDisk.

Registrare Data Guardian

La prima volta che un utente interno condivide un file, l'utente esterno deve effettuare la registrazione.

Per registrare Data Guardian:

1 Nel messaggio e-mail di verifica dell'account inviato da Dell Enterprise Server, fare clic sul collegamento ipertestuale.
2 Passare alla pagina Web.
3 Nella pagina di conferma, fare clic su **Continua per effettuare l'accesso**.
4 Nella pagina di accesso, fare clic su **Password dimenticata**.

> **N.B.:**
> Il server Dell ha assegnato una password casuale, che è necessario reimpostare.

5 Nella pagina di reimpostazione della password, immettere e confermare la password, quindi fare clic su **Registra**.
Viene visualizzata una finestra di dialogo di conferma della registrazione e viene inviato un messaggio e-mail all'indirizzo immesso dall'utente interno.
6 Aprire il messaggio e-mail di attivazione dell'account e fare clic sul collegamento.
Nel messaggio e-mail è indicato anche il nome del server da utilizzare durante l'installazione di Data Guardian.
7 Nella pagina Accedi, immettere l'indirizzo di posta elettronica e la password usati per registrarsi.
8 Fare clic su **Accedi**.
Viene visualizzata una pagina Scarica Data Guardian.
9 Scaricare e installare Data Guardian.
Viene visualizzata una pagina Download con le opzioni per Windows, iOS, Android e Mac OS X. Per un Enterprise Server viene visualizzata la pagina Download. Per un Dell Enterprise Server - VE, facendo clic su Windows l'utente viene reindirizzato al sito dell.com/support.

In questa procedura è descritta l'installazione di Data Guardian su Windows. Vedere anche Attività utente - Documenti Office protetti senza crittografia cloud.

> **N.B.:**
> La pagina di download indica anche il nome del server da usare durante la procedura.

10 In Windows, fare clic su **Scarica (32 bit)** o **Scarica (64-bit)**, a seconda del sistema operativo del computer.
11 Scaricare il file di installazione in una directory del computer.
12 Fare doppio clic sul file di installazione per avviare il programma di installazione.
13 Selezionare una lingua e fare clic su **OK**.
14 Se viene richiesto di installare Microsoft Visual C++ 2010 Redistributable Package, fare clic su **OK**.
15 Nella schermata iniziale, fare clic su **Avanti**.
16 Leggere il contratto di licenza, accettare i termini, e fare clic su **Avanti**.
17 Nella schermata Cartella di destinazione, fare clic su **Avanti** per eseguire l'installazione nel percorso predefinito: **C:\Program Files\Dell \Dell Data Protection\Dell Data Guardian**.
18 Nel campo *Nome server:*, immettere il nome del server con cui comunicherà questo computer. Il nome si trova nel messaggio di attivazione ricevuto nella posta elettronica o in cima alla pagina di download.
19 Fare clic su **Avanti**.
20 Nella schermata Conferma server di attivazione, verificare l'esattezza dell'indirizzo URL del server. Il programma di installazione aggiunge www o http(s), e la porta. Fare clic su **Avanti**.
21 Nella finestra Tipo di gestione, selezionare questa opzione:
   - Utente esterno - Un utente con un indirizzo e-mail non appartenente al dominio aziendale.
22 Fare clic su **Installa** per avviare l'installazione.

Viene visualizzata una finestra di stato che mostra l'avanzamento dell'installazione.

23 Fare clic su **Fine** quando viene visualizzata la schermata Installazione completata.

24 Fare clic su **Sì** per riavviare il sistema.
L'installazione di Data Guardian è completata.

25 Vedere Attivare Data Guardian.

Attivare Data Guardian

Al termine dell'installazione di Data Guardian e in seguito al riavvio del sistema, seguire la procedura riportata di seguito per attivarlo:

1 Accedere a Windows.
Nell'area di notifica, viene visualizzata un'icona a forma di nuvola con un punto esclamativo arancione.

2 Quando viene visualizzata una finestra di dialogo nell'area di notifica, fare clic su **Fare clic qui per attivare**.
Se la finestra di dialogo non viene visualizzata, fare clic sull'icona **Data Guardian** nell'area di notifica e selezionare **Attivazione utente**.

3 Immettere l'indirizzo di posta elettronica e la password usati per registrarsi e fare clic su **Attiva**.

Quando l'attivazione è stata completata, sull'icona Data Guardian nell'area di sistema viene visualizzato un segno di spunta verde  .

4 Confermare lo stato della modalità utente. Fare clic sull'icona nell'area di sistema e selezionare **Dettagli**.
In alto, la Modalità utente è:

Esterno: un utente con un indirizzo e-mail non di dominio.

Se l'installazione è stata completata ed è stato effettuato l'accesso a un client di sincronizzazione, in Esplora risorse viene visualizzata l'Disco virtuale DDG VDisk.

Richiesta di accesso da parte di un utente interno

Con la versione Mobile o Windows, se un utente esterno ha installato e attivato Data Guardian, l'utente può richiedere l'accesso a un file da un utente interno. L'utente esterno deve effettuare una richiesta separata per ciascun file.

1 Se si apre un file Office protetto e il file indica che è necessario richiedere l'accesso, fare clic su **Sì** o **No**.
Una finestra di dialogo indica che la richiesta è stata inviata correttamente. L'utente interno può approvare o rifiutare l'accesso; l'utente esterno riceve un messaggio e-mail con il risultato. Se l'utente esterno apre il file protetto prima che l'utente interno approvi l'accesso, viene visualizzato un messaggio che indica che la richiesta è in sospeso.

2 Dopo 48 ore, l'utente esterno può richiedere nuovamente l'accesso.
Nell'area di notifica, l'utente esterno può fare clic con il pulsante destro del mouse sull'icona Data Guardian e selezionare la pagina **Dettagli**. Fare clic sulla scheda **Sicurezza**. Quando il tempo per una richiesta ritorna a *Nessuno*, l'utente esterno può richiedere nuovamente l'accesso.

Visualizzare un documento Office protetto

Se un'azienda attiva un criterio per proteggere i documenti Office e un utente interno invia un file protetto a un utente esterno, l'utente esterno deve connettersi al Dell Server durante la prima apertura del documento. A seguire, può possono aprire e visualizzare il documento in modalità offline per un periodo di tempo specificato, ad esempio una settimana. L'utente esterno deve quindi connettersi al server e riaprire il documento protetto.

Per motivi di sicurezza, un utente esterno non può effettuare le operazioni riportate di seguito con un documento Office protetto.

- Stampa
- Esporta
- Salva con nome
- Condividi

Disinstallare il client di sincronizzazione o Data Guardian

Se Data Guardian è stato installato dall'amministratore, solo l'amministratore può disinstallare il prodotto. Anche un utente esterno, invitato a condividere una cartella e che dispone dei diritti di amministratore su un computer esterno, può disinstallare Data Guardian dal quel computer esterno.

Disinstallare un client di sincronizzazione cloud

Se si disinstalla il client di sincronizzazione cloud mantenendo Data Guardian installato sul computer, è comunque possibile visualizzare i file come testo in chiaro sull'Disco virtuale DDG VDisk.

Tuttavia, se si reinstalla lo stesso client di sincronizzazione cloud, occorre una nuova chiave per aprirli sull'Disco virtuale DDG VDisk e sarà necessario scaricare i file dal sito Web del client di sincronizzazione.

Disinstallare Data Guardian

Per disinstallare Data Guardian è necessario accedere come amministratore locale del computer.

Copiare i file nell'unità locale

Se si disinstalla Data Guardian dal computer o dal dispositivo, i file sul sito Web del client di sincronizzazione devono comunque essere protetti per rimanere crittografati.

1 Prima della disinstallazione, determinare se è necessario accedere ad alcuni file.
2 Copiare i file dall'Disco virtuale DDG VDisk all'unità locale.

Questi file copiati dall'Disco virtuale DDG VDisk saranno visualizzati in chiaro. Le cartelle e i file nel sito Web del client di sincronizzazione rimarranno crittografati anche una volta scaricati. Per visualizzarli è necessario reinstallare Data Guardian.

Disinstallare Data Guardian

1 Utilizzare il pannello di controllo di Windows per disinstallare il programma.
2 Selezionare Dell Data Protection | Data Guardian e fare clic su **Modifica** nel menu in alto.
3 Fare clic su **Avanti** quando viene visualizzata la schermata di benvenuto.
4 Selezionare **Rimuovi** e fare clic su **Avanti**.
5 Viene visualizzato un avviso in cui si chiede di confermare se si desidera disinstallare Dell Data Protection | Data Guardian. Fare clic su **Avanti**.
6 Nella schermata Rimuovi il programma, fare clic su **Rimuovi**.
Una finestra di stato mostra il progresso.
7 Se viene visualizzata una finestra di dialogo di errore dal client di sincronizzazione, fare clic su **Continua**.
8 Fare clic su **Fine** quando viene visualizzata la schermata Operazione completata.
9 Fare clic su **Sì** per riavviare il sistema.

La disinstallazione di Dell Data Protection | Data Guardian è completata.

8

FAQ - Domande frequenti

FAQ varie

Domanda

Ho spostato la cartella di sincronizzazione del provider del cloud in Programmi e ora non riesco a decrittare i file scaricati nella cartella di sincronizzazione dal cloud.

Risposta

Per impostazione, la cartella Programmi o le cartelle escluse non sono protette in base ai criteri. Data Guardian non decritta i file scaricati in questa cartella o nelle sue sottocartelle.

Soluzione

Scollegare o disinstallare il client di sincronizzazione e spostare nuovamente la cartella di sincronizzazione nella sua posizione predefinita o in un'altra posizione gestita.

N.B.:
Per un elenco delle posizioni gestite e non gestite, contattare l'amministratore.

Domanda

Dopo aver archiviato alcuni file .xen, li avevo copiati sul desktop. Alcuni di essi erano decrittografati, altri non lo erano.

Risposta

Durante una sincronizzazione, Data Guardian è progettato per eseguire la decrittazione direttamente nell'unità virtuale, o per eseguire la decrittazione durante il download tramite un browser Web. Per i file copiati da un altro percorso, usare Esplora risorse e spostare il file .xen nell'unità virtuale da decrittare.

Soluzione

Spostare i file .xen nella cartella dell'unità virtuale per caricarli nel cloud. A questo punto, verranno decrittografati in locale.

Domanda

Ho rinominato il mio computer. Ora non ricevo alcun aggiornamento dei criteri e non riesco ad eseguire la crittografia nel cloud.

Risposta

Attualmente, il server riconosce solo l'endpoint con cui è stata eseguita inizialmente l'attivazione. Se si modifica il nome dell'endpoint, il server non sarà in grado di riconoscere la posizione di invio del criterio e Data Guardian non funzionerà nel modo previsto.

Soluzione

1 Interrompere la sincronizzazione dei file nel computer locale prima della disinstallazione.

N.B.:
In caso contrario, è possibile che alcuni dati importanti siano eliminati o non siano più protetti nel cloud.

2 Disinstallare Data Guardian e reinstallarlo. Per disinstallare è necessario avere diritti di amministratore.

Domanda

Nei dispositivi Windows sospesi, quando tento di caricare i file nel cloud, non succede nulla. Se chiudo le finestre già aperte, viene visualizzato il messaggio di errore Accesso negato.

Risposta

Il messaggio di errore non proviene da Data Guardian. È possibile accedere ai file localmente, ma non saranno disponibili aggiornamenti futuri dei file.

FAQ sui documenti Office e sulla modalità protetta

Domanda

Ho provato ad aprire un documento Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm), ma viene visualizzata una pagina di copertina.

Risposta

Se l'amministratore ha impostato un criterio per proteggere i documenti Office, l'utente o l'amministratore deve installare Data Guardian. Verificare che l'icona Data Guardian nell'area di notifica sia accompagnata da un segno di spunta verde, a indicare che l'applicazione è attiva.

Soluzione

Stabilire se è necessario installare o attivare Data Guardian. Vedere Installare Data Guardian o Possibili problemi con l'attivazione.

Domanda

Non riesco ad aprire un documento Office protetto (Word, PowerPoint o Excel).

Risposta

Controllare quanto segue:

- Impostazioni di blocco dei file - Se l'amministratore ha impostato un criterio per proteggere i documenti Office, non utilizzano questa impostazione in **File > Opzioni**.

Soluzione

Per verificare le impostazioni di blocco dei file:

1 In un documento Office, selezionare **File > Opzioni**.
2 Selezionare **Centro protezione** dall'elenco.
3 Sulla destra, fare clic su **Impostazioni Centro protezione**.
4 Selezionare **Impostazioni di blocco dei file** dall'elenco.
5 Per *Documenti e modelli di Word/Excel/PowerPoint 2007 e versioni successive*, assicurarsi che la casella di controllo *Apri* sia deselezionata.
6 Fare clic su **OK**.