Dell Data Guardian

Guida utente di Windows, Mac, Mobile e Web v2.7

Identifier	GUID-5B8DE7B7-879F-45A4-88E0-732155904029
Status	Translated

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.

Identifier	GUID-8935090F-D61D-41F4-ABC8-F4654D88B0FA
Status	Translation Validated

Guida dell'utente di Windows, Mac, Mobile e Web

2019 - 06

Rev. A01

Sommario

Identifier	**GUID-1E29C798-6A65-41FB-8102-6**
Status	**Translation Validated**

Introduzione

La *Guida dell'utente di Dell Data Guardian* fornisce le informazioni necessarie per installare e utilizzare Data Guardian su Windows o Mac, su un dispositivo mobile o in un portale Web.

Identifier	**GUID-6EE59323-7410-43F4-AD47-C5B7B04044E8**
Status	**Translation Validated**

Panoramica

In base ai criteri impostati dall'amministratore, Data Guardian consente di proteggere i dati nei seguenti modi:

- 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, .pdf.
- Protezione di base dei file - Applicazioni e tipi di file aggiuntivi, ad esempio Blocco note.
- 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.

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. L'amministratore indicherà inoltre all'utente le applicazioni e i tipi di file aggiuntivi che è possibile proteggere.

È possibile utilizzare Data Guardian sulle seguenti piattaforme:

- Windows
- iOS
- Android
- Mac
- Portale Web di Data Guardian, se configurato dall'amministratore

N.B.:
Data Guardian per Mac è in grado di aprire i file crittografati da altre piattaforme. Alcuni file potrebbero essere di sola lettura. La maggior parte delle informazioni utente su Data Guardian per Mac è all'interno del software come guida in linea.

Identifier	**GUID-C9552E05-51A1-4C2D-AADE-C078B4639CD4**
Status	**In Translation**

Opzioni di crittografia per Data Guardian

In base al livello di sicurezza stabilito dall'azienda, l'amministratore imposta i criteri per proteggere i dati archiviati e i dati trasmessi in rete. L'amministratore indicherà all'utente quali criteri si applicano alla propria azienda.

Questo elenco fornisce una panoramica di alcune opzioni di crittografia e, per alcune piattaforme, la posizione delle impostazioni dei criteri.

Modalità e documenti Office

È possibile impostare un criterio per proteggere i documenti di Office. Il comportamento della crittografia può variare a seconda della piattaforma e della modalità. Per Mac, vedere la Guida in linea.

Modalità	Documenti Office
Opzioni per **Windows e Mac**: Modalità Consenso esplicito - Sono disponibili alcune opzioni per stabilire quali documenti Office proteggere. • **Windows** e **Mac** - Una cartella **Documenti sicuri** viene aggiunta alla radice della cartella Documenti. Questa offre un altro modo per crittografare un file. Modalità Protezione forzata - L'azienda richiede un livello di sicurezza più alto. Data Guardian esegue una ricerca per crittografare i file. • **Windows** e **Mac** - Un altro criterio può aggiungere una cartella **Documenti non protetti** alla radice della cartella Documenti. Collocare documenti di Office protetti o i tipi Protezione di base dei file in questa cartella per decrittografarli. • **Mac** - Protegge i file in **/Users**. Queste piattaforme non sono basate su modalità: • Mobile • Portale Web	**Documenti di Office utilizzati in Windows, Mac, dispositivi mobili e portale Web** • .docx • .pptx • .xlsx • .docm • .pptm • .xlsm • .pdf - Se il file è protetto da Data Guardian, aprirlo con Adobe Acrobat Reader DC o con Microsoft Word, ma non dalla rete.

Documenti Office - Windows

L'amministratore può impostare criteri aggiuntivi di Data Guardian per controllare o prevenire la perdita di dati tramite queste opzioni. Il comportamento della crittografia può variare a seconda della modalità.

Opzioni per i documenti di Office protetti in Windows	Descrizione
• Salva - Se un documento Office è protetto, è possibile salvare nuovi contenuti (l'opzione **Salva con nome** non è disponibile per la selezione). • Salva con nome protetto • Se un documento Office è già protetto, l'opzione **Salva con nome** non è disponibile per la selezione.	Altre informazioni relative a Windows: • Documento Office **non protetto** - È possibile selezionare **Salva**, **Salva con nome** o **Salva con nome protetto**. • Viene visualizzato un bordo rosso sui documenti Office protetti e i messaggi e-mail protetti.
Copia/Incolla e Appunti	È possibile copiare e incollare contenuti da un documento di Office protetto a un documento di Office protetto. Non è possibile incollare contenuti da un documento protetto a un documento non protetto.

Opzioni per i documenti di Office protetti in Windows	Descrizione
Stampa	In base al criterio applicato, la stampa di un documento di Office protetto può essere consentita, avere una filigrana o essere disabilitata.
Esporta (Windows e Office 2013 e versioni successive, Mobile)	In base al criterio applicato, l'esportazione può essere consentita, avere una filigrana o essere disabilitata. **N.B.:** Se è stata impostata una filigrana, i documenti Office possono essere esportati. I PDF non possono essere esportati.
Stampa schermo	In base al criterio applicato, la stampa dello schermo può essere consentita o bloccata.
Processi bloccati Esempio: strumento di cattura	In base al criterio impostato dall'azienda, alcuni processi vengono bloccati quando si apre un documento di Office protetto.
Filigrana su schermo	Quando si apre un documento Office protetto, sulla schermata viene visualizza una filigrana con il nome del computer e il nome dell'utente.
Classificazione TITUS (Windows con modalità Consenso esplicito)	Se è attivato un criterio, è possibile fare clic con il pulsante destro del mouse su un documento Office e selezionare una classificazione TITUS. Questa operazione rappresenta un altro modo per consentire agli utenti di proteggere un documento Office.
Classificazione dei dati (Windows con modalità Consenso esplicito)	Se un criterio è attivato e configurato per proteggere le informazioni sensibili, quali ad esempio numeri di previdenza sociale o numeri di carte di credito, i documenti di Office con tali dati vengono crittografati.

Documenti Office - Mac, dispositivi mobili e portale Web

Il comportamento della crittografia può variare a seconda della piattaforma e della modalità. L'amministratore indicherà all'utente quale è applicabile alla propria azienda.

Opzione di crittografia	Descrizione
Mac - Interfaccia Dell Data Guardian	**Mac** - Caricare un documento protetto da crittografare. Scaricare un documento protetto da decrittografare. Dopo aver modificato un documento protetto, le modifiche saranno salvate nel file originale, nel cloud o in locale.
Mobile - All'interno dell'app Data Guardian • Stampa • Filigrana su schermo • Filigrana nascosta • Esporta	**Mobile** - In base al criterio: • I documenti Office all'interno dell'app Data Guardian sono protetti. • La stampa di un documento Office protetto può essere consentita, avere una filigrana o essere disabilitata. • Quando si apre un documento Office protetto, sulla schermata viene visualizza una filigrana con il nome del computer e il nome dell'utente.

Opzione di crittografia	Descrizione
Portale Web • Filigrana su schermo	**Portale Web** - È possibile caricare documenti protetti o non protetti, ma qualsiasi file caricato diventa protetto quando si fa clic su Download. Quando si apre un documento di Office protetto, sulla schermata viene visualizza una filigrana con il nome del computer e il nome dell'utente.

Opzioni aggiuntive

Il comportamento della crittografia può variare a seconda della piattaforma e della modalità. L'amministratore indicherà all'utente quale è applicabile alla propria azienda.

Opzione	Descrizione (modalità Consenso esplicito e Protezione forzata)
Protezione di base dei file - Consente di proteggere applicazioni e tipi di file aggiuntivi (Windows, Mac, dispositivi mobili e portale Web). • Esempi: .txt o .png **N.B.:** Attualmente, per questi tipi di file non viene visualizzato un bordo rosso, anche quando sono protetti.	L'amministratore configurerà una policy per specificare le applicazioni e i tipi di file da crittografare. **Windows, Mac e Mobile** - Questi file vengono ricercati e crittografati. • **Mac** - per estensioni di file impostate dall'amministratore, crittografa questi tipi di file nella cartella */Users*. **Portale Web** - Sempre in base alla policy, questi file possono essere di sola lettura o modificabili dall'utente.
Condividere i documenti di Office protetti con **utenti esterni**. (Windows, Mac, dispositivi mobili e portale Web). Una pagina di copertina include link per la registrazione e informazioni per l'installazione di Data Guardian.	• Utenti esterni e **Windows** - È possibile anche aggiungere una **restrizione di data (embargo)** sui documenti di Office protetti e i PDF. • **Portale Web** - È possibile caricare file condivisi sul portale Web. Non è possibile condividere un file dall'interno del portale Web se non dopo averlo scaricato.
Pagina di copertina o file manomesso (Windows, Mac, dispositivi mobili e portale Web)	Per i file Office, Data Guardian è in grado di analizzare i documenti protetti per rilevare alcune forme di manomissione.
Gruppi di accesso (on-premises) (Windows, Mac, dispositivi mobili e portale Web).	Se sono stati abilitati dall'amministratore, solo le persone nel proprio gruppo di accesso possono visualizzare i file crittografati. È possibile concedere l'accesso agli utenti interni ed esterni per singoli file e tali utenti possono richiedere l'accesso. In base a un criterio aggiuntivo, è possibile fare clic con il pulsante destro del mouse su un messaggio e-mail di Outlook contrassegnato come [PROTETTO] e rimuoverne l'accesso a singoli utenti.
Geofencing (dispositivi mobili)	Solo gli utenti in un'area specifica possono accedere ai file dai propri telefoni cellulari.
Crittografia Email in Outlook (Windows)	In base al criterio applicato, il pulsante *Proteggi* consente di crittografare il contenuto di un messaggio di posta elettronica e dei relativi allegati. Se inviata agli utenti esterni, una pagina di copertina include link per la registrazione e informazioni per l'installazione di Data Guardian.

Hosted o on-premises

Se si deve installare Data Guardian autonomamente, l'amministratore indicherà quali sono le opzioni da utilizzare per la propria azienda.

N.B.:
Per le applicazioni mobili, se è installato Workspace ONE, è possibile eseguire l'autenticazione in Data Guardian con single sign-on.

Dell Security Center Hosted	Dell Management Server On-premises
Una soluzione SaaS (Software-as-a-Service) hosted per la gestione del software Dell Data Security. Se l'azienda è multi-tenant, l'amministratore fornirà un ID di installazione. Quando viene visualizzata una pagina di copertina per un utente che non può ancora accedere a un documento protetto, le informazioni sull'ID di installazione sono incluse nella pagina di copertina. Tutte le piattaforme - se un tenant non riesce a pagare per un periodo di tempo specificato, può essere sospeso.	Un server on-premises che si trova all'interno della rete aziendale per la gestione del software Dell Data Security. L'amministratore indicherà il nome dell'URL del Dell Server.

Crittografia cloud

Il comportamento della crittografia può variare a seconda della piattaforma e della modalità. L'amministratore indicherà all'utente quale è applicabile alla propria azienda.

Piattaforme	Descrizione
Mobile	Vedere Utilizzare Protezione cloud con i dispositivi mobili.
Mac	Consultare la Guida in linea.
Portale Web	Consultare la Guida in linea.
Windows	Attualmente, la protezione della crittografia cloud di Data Guardian è stata disabilitata su Windows per evitare problemi di compatibilità con le funzioni più recenti dei fornitori di servizi cloud. Per visualizzare i file .xen già protetti con Crittografia cloud, utilizzare l'app mobile di Data Guardian, il portale Web o Data Guardian con Mac.

Impostazioni dei criteri

Alcune piattaforme includono un elenco parziale di impostazioni dei criteri per il dispositivo in uso.

Piattaforma	Posizione delle impostazioni dei criteri
Mac	Riquadro *Preferenze*
Mobile	Icona **Impostazioni** > **Informazioni su**
Portale Web	Icona **Impostazioni** > **Informazioni su**

Identifier	**GUID-DEFFD392-F513-445E-A87C-2CE7250245A2**
Status	**Translation Validated**

Ulteriore assistenza

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

Identifier	**GUID-1DE0401E-4073-46BA-95E3-**
Status	**Translation Validated**

Requisiti

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

Identifier	**GUID-7C606C28-5532-4F36-AFA3-03126F14A6EF**
Status	**Translation Validated**

Dell Server

Data Guardian per Windows, Mac e dispositivi mobili richiede Security Management Server o Security Management Server Virtual v9.6 o successiva. Il client Web Data Guardian richiede Security Management Server o Security Management Server Virtual v9.8 o successiva. Ai fini del presente documento, entrambi i server sono indicati come Dell Server, a meno che non sia necessario indicare una versione specifica (ad esempio, se una procedura è diversa quando si utilizza Security Management Server Virtual).

Identifier	**GUID-198D0A89-3C37-4C12-87A4-1F801B60DB21**
Status	**In Translation**

Data Guardian per Windows

- 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).
- Data Guardian è supportato con alcune versioni specifiche di Microsoft Office 2016 e di Microsoft Office 365 Business e Business Premium. Non è supportato nel caso di Office 365 Business Essentials.
- Data Guardian per Windows è compatibile con Workspace ONE. Il programma di installazione di Data Guardian per Workspace UNO e un'installazione MSI ha estensione .msi.
- Data Guardian v2.4 e versioni successive su Windows è supportato in ambienti Air-Gap, ma con alcune limitazioni. Al momento, i dati sulla posizione geografica negli eventi di controllo e nei file di embargo non sono supportati. Il Web beacon richiede una configurazione.
- Verificare che i dispositivi di destinazione siano in grado di connettersi a https://nomesecurityserver.dominio.com:8443/cloudweb/register e https://nomesecurityserver.dominio.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 dovranno pertanto familiarizzare con le modalità di funzionamento di queste applicazioni. Per maggiori informazioni, consultare il supporto Box all'indirizzo https://support.box.com/home, il supporto Dropbox all'indirizzo https://www.dropbox.com/help o il supporto OneDrive all'indirizzo http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- I documenti di Office protetti sono supportati da Mozy, una soluzione complementare di Data Guardian e da altri prodotti di archiviazione NFS, e-mail e cloud.

- Sebbene Dell Encryption non sia necessario, se utilizzato, il client di crittografia deve essere nella versione v8.12 o successiva.
- Data Guardian non supporta lo strumento di ripristino del sistema di Windows, né il programma Windows Insider Preview.
- La funzione Reindirizzamento cartelle di Microsoft non è supportata con Data Guardian.
- Visitare periodicamente dell.com/support per la documentazione più recente e i suggerimenti tecnici.

Prerequisiti

Prerequisiti .exe

Se non è già stato installato, il programma di installazione installa Microsoft Visual C++ 2017 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.

Prerequisiti .msi

È necessario installare Microsoft Visual Studio C++ 2017 Redistributable Package (x86 e x64).

N.B.:
Inoltre, se si esegue MSI, è necessario anche installare Visual Studio 2010 Tools per Office Runtime (x86 e x64).

Prerequisito generale

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 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

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

Sistemi operativi

La tabella seguente descrive in dettaglio i sistemi operativi supportati.

Sistemi operativi Windows (a 32 e 64 bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro dalla versione 1703 (Creators Update/Redstone 2) alla versione 1809 (aggiornamento di ottobre 2018/Redstone 5)

N.B.:
Il client deve trovarsi su uno di questi sistemi operativi altrimenti verrà bloccato. Se necessario, un'impostazione in una chiave di registro consente all'amministratore di ignorare il blocco.

Per il supporto Redstone 4, è necessario aggiornare l'agente prima del sistema operativo. Vedere https://www.dell.com/support/article/us/en/04/sln307922.

N.B.:
Data Guardian non è compatibile con Windows Defender Exploit Guard (WDEG) di Microsoft in Redstone 3 e versioni successive o con Enhanced Mitigation Experience Toolkit (EMET) di Microsoft in Redstone 2 e versioni precedenti.

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

Data Guardian non supporta più versioni di Office su un unico computer.

Microsoft Office

Data Guardian supporta le seguenti versioni di Office. È necessario, tuttavia, installare solo una versione di Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019
- Office 365 ProPlus: versioni 1705, 1708 e 1803 (canale semestrale)

Identifier	**GUID-371FFDE5-7A34-4288-AA88-617E73C0F9A4**
Status	**In Translation**

Data Guardian per Mac

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

Hardware Mac

- Processore Intel Core 2 Duo, Core i3, Core i5, Core i7 o Xeon
- 2 GB RAM

Hardware Mac

- 10 GB di spazio libero su disco

Sistemi operativi

Nella tabella seguente, sono elencati i sistemi operativi supportati.

Sistemi operativi Mac

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.6
- macOS Mojave 10.14.4 - 10.14.5

Provider di archiviazione cloud

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

Provider di archiviazione cloud

- Dropbox
- Box
- Google Drive

  N.B.:
  La funzione *Backup e sincronizzazione di Google* non è supportata.

- OneDrive
- OneDrive for Business

Microsoft Office

Data Guardian per Mac supporta le seguenti versioni di Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	GUID-70934847-A1D7-4AD3-8822-A1E474D4ECD6
Status	In Translation

Applicazione Data Guardian for Mobile

Di seguito sono elencati i sistemi operativi supportati con l'applicazione Data Guardian for Mobile.

Sistemi operativi Android

- 5.0—5.1.1 Lollipop
- 6.0—6.0.1 Marshmallow
- 7.0—7.1.2 Nougat
- 8.0—8.1 Oreo
- 9.0 Pie

Sistemi operativi iOS

- iOS 10.x—10.3
- iOS 11.x—11.4.1
- iOS 12.x-12.1.4

Sistema operativo Chromebook

Per eseguire le applicazioni Android su Chrome OS, è necessaria la versione M53 o successiva di Chrome OS. Questi dispositivi sono convalidati per l'esecuzione di app Android su Chrome OS, ma confermano l'opzione con il proprio agente di vendita:

- https://www.chromium.org/chromium-os/chrome-os-systems-supporting-android-apps

Microsoft Office

L'applicazione Data Guardian for Mobile può aprire i file creati con le seguenti versioni di Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	GUID-E0E57A65-225C-46FB-9E51-60FAC92BA57A
Status	In Translation

Data Guardian per il Web

Per abilitare il client Web Data Guardian, l'amministratore imposta una macchina virtuale che ospita il client Web e comunica con Dell Server v9.8 o versione successiva.

Per distribuire il client Web Data Guardian è possibile utilizzare i seguenti ambienti virtualizzati.

Ambienti virtualizzati

- **VMware ESXi 6.7**
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - Non sono richiesti sistemi operativi
  - Visitare http://www.vmware.com/resources/compatibility/search.php per un elenco completo di sistemi operativi host supportati
  - L'hardware deve essere conforme ai requisiti minimi VMware
  - Almeno 4 GB di RAM per la risorsa immagine dedicata
  - Per maggiori informazioni, visitare il sito http://pubs.vmware.com/vsphere-67/index.jsp

- **VMware ESXi 5.5**
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - Non sono richiesti sistemi operativi
  - Visitare http://www.vmware.com/resources/compatibility/search.php per un elenco completo di sistemi operativi host supportati
  - L'hardware deve essere conforme ai requisiti minimi VMware
  - Almeno 4 GB di RAM per la risorsa immagine dedicata
  - Per maggiori informazioni, visitare il sito http://pubs.vmware.com/vsphere-55/index.jsp

- **Microsoft Hyper-V**
  - Processore a 64 bit con SLAT (Second Level Address Translation)
  - Almeno 8 GB di RAM consigliati
  - L'hardware deve essere conforme ai requisiti minimi Hyper-V
  - Vedere https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements per maggiori informazioni.

N.B.:
Questi requisiti minimi rappresentano fino a venticinque connessioni simultanee a un singolo portale Web.

Provider di archiviazione cloud

In base alle impostazioni dei criteri, il portale Web di Data Guardian è in grado di accedere a questi provider di cloud storage.

Provider di archiviazione cloud

- OneDrive for Business

Microsoft Office

Data Guardian per il Web può aprire i file creati con le seguenti versioni di Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	**GUID-F414365D-DE5B-4703-88AB-FCB73F3BD14D**
Status	**Translation Validated**

Altri requisiti

Attualmente, l'autenticazione a più fattori di Amazon Cognito non è supportata su nessuna piattaforma Data Guardian.

Identifier	**GUID-E2815EA1-85AF-4049-B317-DF016FBA39EE**
Status	**Translation Validated**

Browser Web

È possibile utilizzare Data Guardian con Internet Explorer, Mozilla Firefox, Google Chrome e Microsoft Edge.

Per Mac, è supportato anche Safari.

Identifier	**GUID-582A5665-D2A2-4B98-A51D-5F14376D98BA**
Status	**Translation Validated**

Adobe Acrobat

Nel caso di computer Windows e Mac, i file .pdf protetti possono essere aperti con Adobe Acrobat Reader DC.

N.B.:
I seguenti programmi non sono supportati: Adobe Acrobat *Standard* DC, Adobe Acrobat *Pro* DC e Adobe Acrobat DC.

Identifier	GUID-36045ECC-D303-4A63-9ABA
Status	In Translation

Installare o disinstallare Data Guardian su Windows

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

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

Identifier	GUID-D0717325-F700-400C-BC03-5FD8190A81A9
Status	In Translation

Panoramica delle attività di installazione per Windows

Questa panoramica riepiloga la sequenza per l'installazione 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 in modo interattivo 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. **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.

Opzioni per Windows

Attività	Descrizione	Per maggiori informazioni
Visualizzare il menu dell'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

Identifier	GUID-B54EDFCA-AFBB-4BD0-8427-515A3E052962
Status	In Translation

Cartelle preesistenti con file non crittografati

Al momento di distribuire Data Guardian, è consigliabile non configurare account di archiviazione cloud nei dispositivi di destinazione.

Se un provider di archiviazione cloud è configurato con cartelle che sono sincronizzate con il computer locale prima dell'installazione di 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

Identifier	GUID-7BBFA9B6-C19E-44E8-908C-F5AF181462C8
Status	In Translation

Installare Data Guardian in modo interattivo su Windows

Per installare Data Guardian, è necessario essere amministratore locale. Se gli utenti non potranno installare il prodotto, informarli della posizione dei supporti di installazione.

Prima di iniziare

Stabilire i componenti necessari in base all'ambiente di utilizzo e al prodotto Data Guardian:

Dell Security Center Hosted	Dell Management Server On-premises
Se l'ambiente hosted è un ambiente multi-tenant, è necessario un ID di installazione.	Accertarsi di conoscere il nome di Dell Server.

Installare Data Guardian

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 e copiarlo sul computer locale. Ecco i nomi dei programmi di installazione di esempio:
   - Dell Security Center Hosted - I nomi dei programmi di installazione hanno estensione .exe
   - on-premises - I nomi dei programmi di installazione hanno:
     - Estensione .exe
     - Estensione .msi per Workspace ONE e un'installazione MSI
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++ 2015 Redistributable Package o Microsoft .NET Framework 4.5.2 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 \Data Guardian\.**

Non installare Data Guardian nelle cartelle **C:\Users** o **C:\Windows** o nella radice di qualsiasi unità.

10 Selezionare una delle seguenti azioni:

Dell Security Center Hosted	Dell Management Server On-premises
Una soluzione SaaS (Software-as-a-Service) hosted per la gestione del software Dell Data Security.	Un server on-premises che si trova all'interno della rete aziendale per la gestione del software Dell Data Security.
a Selezionare **Dell Security Center Hosted**. b Se l'azienda è multi-tenant, è anche possibile inserire un ID di installazione. **N.B.:** Se l'azienda è multi-tenant e non si inserisce un ID di installazione, l'amministratore può aggiungerlo nel registro di sistema in un secondo momento. c Fare clic su **Continua.** d Continuare con il passaggio 11.	a Selezionare Dell Management Server On-premises. b Nel campo *`Nome Dell Management Server:`*, immettere il nome del Dell 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. **N.B.:** Non deselezionare la casella di controllo *Abilita verifica trust SSL*, a meno che l'amministratore non lo richieda. c Fare clic su **Avanti**. d Nella schermata Informazioni di Conferma Dell Management Server, confermare che l'indirizzo URL del Dell Server è corretto. Il programma di installazione aggiunge www o http(s), e la porta. Fare clic su **Avanti**. e Continuare con il passaggio 11.

11 Nella finestra Tipo di gestione, selezionare questa opzione:

- Utente interno - Un utente con un indirizzo e-mail nel dominio dell'azienda.

12 Fare clic su **Installa** per avviare l'installazione.

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

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

14 Fare clic su **Sì** per riavviare il sistema.

L'installazione di Data Guardian è completata.

15 Gli utenti devono confermare l'attivazione. L'icona dell'area di notifica di Data Guardian dovrebbe presentare un segno di spunta verde  .

N.B.:

A seconda del modo in cui Data Guardian viene distribuito all'interno dell'azienda, l'attivazione può non essere immediata. Tuttavia, se l'attivazione non viene eseguita, l'utente deve eseguirla manualmente.

Identifier	**GUID-AF4BEC71-F3FB-43E9-A588-FA2C2BC7E4BD**
Status	**Translation Validated**

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:

Opzione Data Guardian	Possibile problema
Office protetto	• 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.
Crittografia cloud	• 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

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.

Identifier	**GUID-10DDD78A-61B2-4AE9-9DF4-0527FEE42D0D**
Status	**In Translation**

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 notifica viene visualizzato un segno di spunta verde.

4 Confermare lo stato della modalità utente. Fare clic sull'icona area di notifica 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 Utilizzare Data Guardian come utente esterno.

N.B.:
Se per Modalità utente viene visualizzato **Non registrato**, Data Guardian non è stato ancora attivato.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center Hosted e tenant sospeso

Con Dell Security Center Hosted, se un tenant non riesce a effettuare pagamenti per un periodo di tempo specificato, il tenant può essere sospeso. Si applica a Windows, Mac, dispositivi mobili e portale web.

Gli utenti interni ed esterni di Data Guardian possono riscontrare le seguenti condizioni:

- Tutte le piattaforme - Se si tenta di installare Data Guardian, eseguire l'attivazione e l'accesso, viene visualizzata una finestra di dialogo indicante che il tenant è sospeso.
- Mac - Se il tenant è sospeso mentre Data Guardian è aperto, viene visualizzata la relativa finestra di dialogo dopo aver chiuso Esplora file e tutti i file e l'utente tenta di aprire un file protetto.
- Portale web:
  - Se è già stato effettuato l'accesso e si carica un file crittografato, appare il messaggio Caricamento non riuscito.
  - Se un file crittografato o non crittografato è stato caricato e quindi il tenant viene sospeso, appare il messaggio Download non riuscito.
  - Se si esegue la disconnessione e si tenta di accedere nuovamente, appare una finestra di dialogo che indica che il tenant è sospeso.

Contattare l'amministratore.

Identifier	**GUID-43BA606D-3F31-4E67-97B4-039DE9CEBC65**
Status	**In Translation**

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

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 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 con il pulsante destro del mouse 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 interno all'indirizzo di dominio
- **Utente esterno** - Un utente con indirizzo all'esterno di questo dominio

- **Non registrato** - Un utente interno o esterno il cui Data Guardian non è attivato

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: Dell Server che comunica con il client.

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

Versione criteri: Versione dei criteri generata da Dell Server.

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

Nome: nome del file

Cloud: questa funzione è stata disabilitata e non dispone più di dati.

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: questa funzione è stata disabilitata.

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

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

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

In precedenza, la Crittografia cloud di Data Guardian aveva un'area **Cartelle** della schermata Dettagli. Attualmente, la Crittografia cloud è stata disabilitata.

Identifier	**GUID-5726752F-D15C-479E-8E8E-6BBE27B23F90**
Status	**Translation Validated**

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 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.

Identifier	**GUID-62C18A73-A619-46BF-BE3A-76911412C43A**
Status	**Translation Validated**

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.

Identifier	**GUID-E67381E8-70C7-46BE-A822-9B5C48B0FFC3**
Status	**Translation Validated**

Aggiornare Data Guardian

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

Identifier	**GUID-CC8C1B76-3E85-415F-AAE0-3C20521D70A6**
Status	**In Translation**

Disinstallare Data Guardian su Windows

Se Data Guardian è stato installato dall'amministratore, solo l'amministratore dovrebbe 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.

Identifier	**GUID-FB8AEF07-F76C-4E52-9920-B56A973DB1E6**
Status	**In Translation**

Disinstallazione di 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 quei file nell'unità locale.

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. Oppure, è possibile visualizzarli nel portale Web di Data Guardian.

Disinstallazione di Data Guardian

1 Utilizzare il pannello di controllo di Windows per disinstallare il programma.
2 Selezionare **Dell 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 per confermare la disinstallazione di Dell 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 Se una finestra di dialogo segnala che è aperto un documento Office, fare clic su **OK**, chiudere il documento Office e avviare nuovamente la disinstallazione.
9 Fare clic su **Fine** quando viene visualizzata la schermata Operazione completata.
10 Fare clic su **Sì** per riavviare il sistema.

La disinstallazione di Data Guardian è completata.

Identifier	**GUID-05F5667F-C3BE-4C5E-B64D-5629C60C049D**
Status	**Translation Validated**

Fornire un feedback a Dell

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

Per accedere, 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.

Identifier	GUID-E68E0B8D-7519-4C11-A918-
Status	In Translation

Utilizzare Data Guardian con Windows

L'amministratore ha già configurato una serie di criteri per proteggere i documenti e indicherà all'utente quale di queste opzioni si applicano alla propria azienda.

Identifier	GUID-162A20CF-D1AD-4701-9A28-1000DB2FE1D4
Status	In Translation

Panoramica delle opzioni

Questa panoramica riepiloga le possibili opzioni per Data Guardian in base al criterio impostato dall'amministratore. Questi documenti saranno protetti durante la condivisione con altri o l'archiviazione su un supporto rimovibile.

Opzione	Descrizione	Per maggiori informazioni
Documenti Office e con attivazione macro	Sono inclusi i formati .docx, .pptx, .xlsx, .pdf, .docm, .pptm, .xlsm e .pdf.	Vedere Osservare le opzioni del menu File per determinare il livello di sicurezza per i documenti Office. Sarà disponibile una di queste modalità: • Consenso esplicito • Protezione forzata
Protezione di base dei file	Si tratta di applicazioni e tipi di file aggiuntivi che l'azienda desidera crittografare e che l'amministratore ha configurato.	Vedere Proteggere applicazioni e tipi di file aggiuntivi con la protezione di base dei file.
Opzioni aggiuntive	Queste possono applicarsi ai documenti Office, ai file base o a entrambi.	Vedere Opzioni aggiuntive per Data Guardian.
Condividere un file con un utente esterno	Un utente con un indirizzo e-mail che non fa parte del dominio (un utente di un'altra azienda o un utente interno che desidera accedere a file protetti da un indirizzo email che non fa parte del dominio).	Vedere Utilizzare Data Guardian come utente esterno.

Lavorare online con documenti protetti

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

Proprietà file > scheda Dell Data Guardian

Con i documenti di Office protetti, è possibile fare clic con il pulsante destro del mouse e selezionare **Proprietà**. Viene visualizzata una scheda **Dell Data Guardian** con informazioni, come ad esempio l'ID chiave del file e i dati di accesso ed embargo.

Icone di sovrapposizione per Windows

Per Data Guardian 2.2 e versioni successive, vengono visualizzate icone di sovrapposizione sui file protetti in Esplora file. Se si fa clic con il pulsante destro del mouse sul file protetto, una scheda Dell Data Guardian fornisce ulteriori informazioni.

Filigrana nascosta

A seconda dei criteri impostati dall'amministratore, i documenti di Office protetti potrebbero essere dotati di una filigrana nascosta che identifica l'utente. Se si stampa o si condivide il documento, la filigrana persiste.

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.

Identifier	**GUID-E88C0771-29BE-4292-AD26-F913747EE0FC**
Status	**Translation Validated**

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
- .pdf

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 di 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.

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* è attivato.
  - 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 di 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* 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.
  - Cartella **Documenti >** <2>Documento non protetto </2>- Se consentito dal criterio in modalità Protezione forzata (e non in modalità Consenso esplicito), una cartella Documento non protetto viene aggiunta alla radice della cartella Documenti. I documenti Office in questa cartella sono decrittografati. Se si elimina la cartella, la stessa viene ricreata.

- 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.

Identifier	GUID-077EC2B6-61AD-4F13-95D0-CF91EF0143AF
Status	In Translation

Utilizzare la modalità Consenso esplicito per proteggere i documenti Office

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

- Utilizzare le opzioni del menu File per la modalità Consenso esplicito
- Opzioni aggiuntive per Data Guardian

Utilizzare le opzioni del menu File per la modalità Consenso esplicito

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
Aprire	I file vengono aperti come di consueto
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.
Salva con nome	Presenta le opzioni standard (ma non la modalità protetta)
Salva con nome protetto	L'unica opzione nel campo Salva come è Documento Office protetto
Stampa	**Abilitata** Tuttavia, per i documenti Office protetti, se l'amministratore disattiva la Stampa tramite criterio, è ancora possibile selezionare Stampa, ma un avviso popup informa che il documento protetto non può essere stampato. Se l'amministratore consente Stampa, un altro criterio potrebbe applicare una filigrana, contenente il nome utente, il nome di dominio e l'ID del computer, su ogni pagina stampata.
Condividi	**Abilitato** per documenti Office protetti. **Disabilitato** per i documenti non protetti.
Esporta (Office 2013 e versioni successive)	Può essere attivato o disattivato in base ai criteri impostati dall'amministratore.

Menu File	Modalità di consenso esplicito e documenti Office protetti
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. 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 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.

Classificazione TITUS e modalità Consenso esplicito

Se è attivato un criterio, l'amministratore configura alcune classificazioni TITUS con cui crittografare i documenti. È possibile fare clic con il pulsante destro del mouse su un documento Office non protetto e selezionare la classificazione TITUS. Ciò offre un altro modo per proteggere un documento Office.

Classificazione dati e modalità Consenso esplicito

Se questo criterio è abilitato, l'amministratore può impostare classificazioni per contenuti specifici, come numero di previdenza sociale, numero di carta di credito o altre informazioni sensibili. L'amministratore comunicherà quali informazioni sono state classificate. Quando si salva un documento che contiene informazioni basate su tali regole di classificazione, il documento viene crittografato.

Se si utilizzano i tag in un documento di Office per attivare una classificazione dei dati utilizzati nel tag di metadati del file del criterio, il tag utilizzato nel documento di Office è dotato di distinzione tra maiuscole e minuscole e deve corrispondere alla combinazione di maiuscole e minuscole utilizzata dall'amministratore nel criterio.

N.B.:

Se questo criterio è abilitato, uno sweep farà sì che i file che soddisfano le regole di classificazione siano criptati. Tuttavia, quando si crea il file, è possibile fare clic con il pulsante destro del mouse e selezionare **Proteggi file**.

Vedere anche Outlook Email Encryption con Data Guardian.

Risoluzione dei problemi per la modalità di consenso esplicito

Se il criterio di Data Guardian ha disattivato la stampa per i documenti di Office protetti, è ancora possibile selezionare Stampa accedendo a **File > Info** oppure facendo clic con il pulsante destro del mouse su un file Office protetto in Windows Explorer. 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 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.

N.B.:

Se si utilizza la modalità di protezione forzata, tutti i documenti Office vengono protetti.

Identifier	GUID-5E368002-F3BB-48A7-9A30-B4591019B21F
Status	In Translation

Utilizzare la modalità Protezione forzata per proteggere i documenti Office

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

- Utilizzare le opzioni del menu File per la modalità Protezione forzata
- Opzioni aggiuntive per Data Guardian

Utilizzare le opzioni del menu File per la modalità Protezione forzata

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 protezione forzata per documenti protetti e non protetti
Aprire	I documenti non protetti vengono aperti in modalità di sola lettura.
Salva	• 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).
Salva con nome	**Disabilitato**
Salva con nome protetto	L'unica opzione nel campo Salva come è Documento Office protetto
Stampa	**Abilitata** Tuttavia, per i documenti di Office protetti, se l'amministratore disattiva la Stampa tramite criterio, è ancora possibile selezionare Stampa, ma un avviso popup informa che il documento protetto non può essere stampato. Se l'amministratore consente Stampa, un altro criterio potrebbe applicare una filigrana, contenente il nome utente, il nome di dominio e l'ID del computer, su ogni pagina stampata.
Condividi	**Disabilitato**
Esporta	Può essere attivato o disattivato in base ai criteri impostati dall'amministratore.

Menu File	Modalità di protezione forzata per documenti protetti e non protetti
(Office 2013 e versioni successive)	
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.

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.

Identifier	GUID-669244A9-0658-46A3-A9EB-A5D349D7EDBC
Status	In Translation

Opzioni aggiuntive per Data Guardian

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.

Incolla

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

- È possibile copiare e incollare i dati protetti e non protetti nel documento protetto originale o in un file PDF protetto. Tuttavia, nessun file PDF non protetto può essere aperto in Adobe Acrobat Reader DC.
- 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.

Apertura e modifica di un PDF protetto con Adobe Acrobat Reader DC

Quando si utilizza Acrobat Reader DC:

- È possibile aggiungere annotazioni su un file .pdf protetto o completare un modulo. Quando si salva il file, viene creato un nuovo file .pdf protetto che include le modifiche. Questa è una funzionalità di Acrobat Reader DC.
- Per migliorare la sicurezza, quando un file .pdf protetto viene aperto con Acrobat Reader DC, l'accesso a Internet è bloccato fino a quando Acrobat Reader DC non viene chiuso.
- Per migliorare la sicurezza, se un .pdf protetto è aperto, l'utente non può inviare e-mail da tale istanza.

N.B.:
Non è possibile aprire un file .pdf protetto dalla rete. Per aprire un file .pdf protetto dalla rete, è possibile utilizzare Word.

Stampa per buste ed etichette

Se l'amministratore ha impostato un criterio per aggiungere una filigrana durante la stampa di un documento di 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.

Opzioni aggiuntive

Processi bloccati

Sulla base dei criteri impostati dall'amministratore, alcuni processi (ad es., lo strumento di cattura) potrebbero venire bloccati. L'amministratore può informare l'utente circa tali processi. Inoltre, viene visualizzata una finestra di dialogo in cui si comunica che il processo è bloccato.

- **Modalità Protezione forzata** - Se l'amministratore imposta un criterio per bloccare il pulsante *PrtScr*, potrebbe non essere possibile utilizzare il touchscreen o i tablet per stampare gli schermi.
- In Windows con RS5 è disponibile l'app Note su schermo (precedentemente strumento di cattura). Con Data Guardian, l'amministratore può attivare un criterio che blocca quest'app per aumentare la sicurezza.

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

Per allegare un documento 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.

È possibile allegare un file documento di Office protetto, un tipo di file protetto aggiuntivo basato su policy o un file .xen.

Per Windows con Data Guardian, se si allega un documento, Data Guardian aggiunge informazioni per accedere al file crittografato all'interno del messaggio email.

- Utenti interni - Vengono visualizzate informazioni con un link per scaricare un client.
- Utenti esterni - Vengono visualizzate informazioni con un link per registrare e scaricare un client.

N.B.:
Per le informazioni aggiunte da visualizzare, è necessario inviare il messaggio email da Microsoft Office Outlook, non dalla versione web-based di Outlook.

Outlook Email Encryption con Data Guardian

In base alla policy con Data Guardian v2.0.1 e versioni successive, gli utenti interni hanno un'opzione *Protezione* in alto a sinistra di Outlook per crittografare sia le e-mail sia gli allegati. Mittente e ricevente devono entrambi avere Data Guardian installato e attivato.

La crittografia dei messaggi di posta elettronica Outlook di Data Guardian è supportata solo con Office 2013 e versioni successive, ma non con la web mail.

Per utilizzarla:

1 In alto a sinistra, fare clic su **Proteggi**.
2 Per un indirizzo email esterno, fare clic su **Sì** per confermare la condivisione chiave o su **No** se si decide di non inviare l'email.

La best practice consiste nell'avere un messaggio di posta elettronica aperto per volta. Se si hanno più messaggi aperti, fare clic sull'email per portarla in primo piano prima di fare clic sul pulsante Protezione. Il pulsante Protezione deve essere grigio quando non vi si posiziona il puntatore.

I dati in movimento sono protetti. In questa versione di anteprima, la prevenzione della perdita dei dati per i dati inattivi è supportata solo parzialmente. Nelle versioni successive, la sicurezza verrà progressivamente migliorata.

Per ridurre al minimo l'effetto della prevenzione della perdita dei dati quando si apre un'email crittografata, alcune operazioni sono disabilitate o bloccate:

- *Azioni rapide* di Outlook
- *Sposta*, *Sposta nella cartella* e altre operazioni con le cartelle
- Frecce *Successivo* e *Precedente*
- *Inoltra*
- Alcune opzioni attivabili con il clic del pulsante destro del mouse

Per ridurre al minimo l'effetto della prevenzione della perdita dei dati quando si apre un'email crittografata, le seguenti operazioni sono controllate:

- *Copia/Incolla*
- *Stampa* ed *esportazione* di dati
- Alcune opzioni attivabili con il clic del pulsante destro del mouse
- Cartella Bozze e *Salvataggio automatico*

Destinatari di email Outlook

Quando si apre un'email di Outlook crittografata, viene visualizzato un messaggio di avvertenza indicante che il documento è protetto e l'utente deve fare doppio clic per aprire il file. Nell'anteprima viene visualizzata solo una pagina di copertina, ma non il contenuto dell'email. Nella pagina di copertina è riportato il nome del Dell Server, se il server è di tipo on-premises, o un ID di installazione, se Dell Security Center Hosted è multi-tenant. La pagina di copertina contiene anche i link per scaricare il client di Data Guardian.

Classificazione e-mail

Report locale per documenti di Office protetti crittografati con la classificazione dei dati (modalità Consenso esplicito)

Per proteggere le informazioni sensibili nei documenti di Office e PDF, l'amministratore può impostare un criterio che richiede la ricerca e la successiva crittografia dei file in base alla classificazione dei dati. Le informazioni sensibili possono includere numeri di previdenza sociale, numeri di carta di credito, indirizzi negli Stati Uniti o dati specifici dell'azienda. L'amministratore dovrà informare l'utente delle informazioni sensibili che causano la crittografia dei file.

Per visualizzare un report locale dei file crittografati a causa della classificazione dei dati e della motivazione per la crittografia:

1 Andare a **C:\Utenti\<nomeutente>\AppData\Local\Dell\Data Guardian**.
2 Aprire **Classification Report.log**.

N.B.:
Se è in corso la crittografia di un file, la relativa voce può presentare più linee prima del completamento dell'operazione.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Proteggere applicazioni e tipi di file aggiuntivi con la protezione di base dei file

L'amministratore comunicherà se i criteri consentono la crittografia di applicazioni e tipi di file aggiuntivi. Se qualcuno apre un file crittografato con protezione di base dei file ma non ha installato Data Guardian, i contenuti sono illeggibili.

Panoramica della protezione di base dei file

Applicazioni

Di seguito sono riportati alcuni esempi di applicazioni che l'amministratore potrebbe crittografare:

- Blocco note
- WordPad
- Visio
- MS Paint

N.B.:
Alcune applicazioni sono solo parzialmente supportate con Data Guardian e l'amministratore le indicherà all'utente.

Tipi di file

Di seguito sono riportati alcuni esempi di tipi di file aggiuntivi che possono essere configurati: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e Mobile

Quando il criterio Protezione di base dei file è configurato, Data Guardian cerca nei computer degli utenti e crittografa tutti i file locali con queste estensioni. I file crittografati con Protezione di base dei file possono essere visualizzati e modificati solo con l'applicazione associata alla relativa estensione.

N.B.:
I file nelle cartelle di sistema specifiche non vengono crittografati, ad esempio AppData, così come le cartelle che si riferiscono a documenti di Office protetti, ad esempio la cartella Documenti sicuri.

Icone di sovrapposizione per Windows

Per Data Guardian 2.2 e versioni successive, vengono visualizzate icone di sovrapposizione sui file protetti in Esplora file. Se si fa clic con il pulsante destro del mouse sul file protetto, una scheda Dell Data Guardian fornisce ulteriori informazioni.

Escludere alcuni file dalla scansione in Windows o Mac (prima che la ricerca venga abilitata)

Se l'azienda decide di crittografare un tipo di file aggiuntivo, ad esempio. txt, potrebbe non essere necessario che tutti i file con tale estensione vengano scansionati e crittografati.

Prima di abilitare la Protezione di base dei file per tale estensione, l'amministratore può impostare un altro criterio che consente di aggiungere una cartella al computer locale e i file in tale cartella non vengono scansionati. L'amministratore può impostare un criterio, creare un nome di cartella, fornire il nome della cartella e suggerire dove è possibile aggiungere la cartella. Questi potrebbero essere file necessari al sistema o i file che non richiedono protezione.

IMPORTANTE:

È necessario creare la cartella prima che l'amministratore abiliti il criterio Protezione di base dei file.

1 Utilizzare il nome e il percorso della cartella forniti dall'amministratore.
   - Per Mac, passare al **riquadro Preferenze > Esclusioni della protezione di base dei file**. Qui viene visualizzato il nome della cartella da creare e il percorso.

2 Aggiungere i file con l'estensione specificata, ad esempio. txt, che non devono essere crittografati. Facoltativamente, è possibile aggiungere sottocartelle con nomi creati dall'utente.

   N.B.:

   Se si dispone di file con una data estensione, crittografati in precedenza, non saranno decrittografati una volta inseriti in quella cartella. Resteranno crittografati. Se si dispone di una cartella **Documenti non protetti**, che l'amministratore può creare tramite un altro criterio, è possibile collocare i tipi Protezione di base dei file in questa cartella per decrittografarli.

3 Una volta abilitata la Protezione di base dei file, se si dispone di file non protetti con tale estensione su una rete o su un'unità esterna, è possibile copiarli nella cartella esclusa. Resteranno non crittografati. In caso contrario, saranno crittografati.

Se il proprio computer dispone di più utenti, solo l'utente attualmente connesso può collocare i file nella cartella ed escluderli dalla scansione. Tutti i file che un altro utente colloca in quella cartella verranno scansionati e crittografati.

Rimozione di un'estensione di file in Windows o Mac

L'amministratore può decidere di rimuovere un'estensione di file. In tal caso, il computer è sottoposto a ricerca al fine di decrittografare i file di questo tipo.

- La scheda *Properties* > *Dell Data Guardian* del file crittografato non viene più visualizzata.
- Se esistevano icone di sovrapposizione dei file, non vengono più visualizzate.
- Possono essere necessari diversi minuti per completare la decrittografia dei file. Se un file con l'estensione in questione è ancora crittografato, potrebbe essere stato aperto durante la ricerca oppure archiviato su un file server o in un'altra posizione.

Rivolgersi all'amministratore per richiedere il ripristino di tutti i file con l'estensione desiderata che non vengono decrittografati.

Applicazioni Office

È possibile utilizzare un'applicazione Office per aprire un file crittografato con Protezione di base dei file, ma i contenuti sono di sola lettura.

Portale Web

In Impostazioni > Criteri, se la protezione di base dei file è attivata, l'amministratore ha aggiunto tipi di file non Office che Data Guardian crittograferà in seguito al download dal portale web. L'amministratore deve indicare i tipi di file.

N.B.:

Se si carica un tipo di file non ancora supportato, non sarà possibile leggerne il contenuto nel portale Web.

È possibile caricare tipi di file non Office crittografati o non crittografati. Tuttavia, quando si scarica il file non Office , l'estensione varia.

File non Office (ad esempio, .txt o .png)	Descrizione download
Crittografati prima di eseguire il caricamento Esempio: file non Office già crittografati da Windows o Mac.	Una volta scaricati dal portale web, l'estensione file viene mantenuta, ad esempio .txt o .png.
File non crittografati	Una volta scaricati dal portale web, l'estensione del file varia a seconda del fatto che l'amministratore abbia aggiunto l'estensione a una policy. Tuttavia, sono crittografati. Esempi di un file in formato .txt scaricato dal portale web: • **nomefile.txt** - L'amministratore ha aggiunto il tipo di file .txt a una policy. • **nomefile.txt.xen** - Il file .txt non è incluso nella policy. Il file viene crittografato ma aggiunge un'estensione .xen.

Se la policy *Modifica* è attivata per il portale web, gli utenti possono modificare i file non Office.

Identifier	**GUID-801B897D-9A0F-48C0-B46C-A3726B8BD9E4**
Status	**Translation Validated**

Manomissione e documenti Office protetti

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

Se un utente interno manomette un documento di 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 di 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.

Identifier	**GUID-A8209D75-E380-4809-A55A-CF89E3FBE29A**
Status	**In Translation**

Visualizzare cartelle e file del client di sincronizzazione nel cloud

Se si dispone di una cartella del client di sincronizzazione sul computer e Data Guardian la crittografa, tali file verranno crittografati nel cloud.

Se si utilizza il portale Web di Data Guardian per crittografare i file, questi potrebbero essere crittografati come file .xen. Non è possibile aprire i file .xen crittografati in Windows. È possibile visualizzarli su un dispositivo mobile con Data Guardian o sul portale Web.

Identifier	**GUID-7A2816C4-2882-4B5B-B2C6-A8032B1C4508**
Status	**Translation Validated**

Condividere i documenti Office protetti con utenti esterni

Con Data Guardian, è possibile condividere un documento di Office protetto tramite email, supporto rimovibile o share di rete oppure caricandolo nel cloud:

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

Quando si allega il documento e si seleziona *Invia*, viene visualizzata una finestra di dialogo per ricordare che la chiave per questo documento protetto verrà condivisa con l'utente esterno.

Migliorare la sicurezza aggiungendo restrizioni alla data

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 di 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 infine 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 di 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 visualizzato un messaggio che spiega che il file non può essere aperto fino alla data e all'ora indicate a causa di restrizioni di accesso.

Identifier	GUID-FFED5E16-B72A-4858-A64D-
Status	Translation Validated

Installare e utilizzare Data Guardian con Mac

Data Guardian per Mac è dotato di una guida integrata per schermate specifiche che forniscono informazioni su:

- Interfaccia Dell Data Guardian in cui gli utenti possono caricare i file per crittografarli
- Crittografia cloud
- Utenti esterni e restrizioni di accesso
- Manomissioni

Nell'interfaccia Dell Data Guardian per Mac, fare clic sull'icona della Guida.

Identifier	GUID-0DB59561-F614-4FEB-9265-6F2711737741
Status	Translated

Installare il client per Mac

Se l'amministratore ha aggiunto l'utente all'elenco di utenti consentiti dell'azienda, è possibile registrarsi all'indirizzo: https://nomesecurityserver.dominio.com:8443/cloudweb/register.

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

È necessario essere un amministratore locale.

Per installare Data Guardian per Mac:

1 Per il client di Data Guardian, individuare il programma di installazione in **Dell-Data-Guardian-Mac-0.x.x.xxxx.dmg.**
2 Utilizzare il file **.pkg** in Dell-Data-Guardian-0.x.x.xxxx.dmg per l'installazione o l'aggiornamento.
3 Fare doppio clic sul pacchetto **Dell-Data-Guardian-x.x.x**.
4 Fare clic su **Continua.**
5 Nella finestra Introduzione, fare clic su **Continua**.
6 Nella finestra Contratto di licenza software, fare clic su **Continua**.
7 Fare clic su **Accetto**per continuare.
8 Nella finestra Tipo di configurazione, selezionare una delle seguenti opzioni:

Dell Security Center Hosted	Dell Management Server On-premises
Una soluzione SaaS (Software-as-a-Service) hosted per la gestione del software Dell Data Security. a Selezionare **Dell Security Center Hosted**. b Fare clic su **Continua.** c Continuare con il passaggio 9.	Un server on-premises che si trova all'interno della rete aziendale per la gestione del software Dell Data Security. a Selezionare Dell Management Server On-premises. b Nel campo *Nome Dell Management Server*, immettere il nome del Dell 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.

Dell Security Center Hosted	Dell Management Server On-premises
	c Fare clic su **Continua.** d Continuare con il passaggio 9.

9 Nella finestra Tipo di installazione, effettuare una delle seguenti operazioni:
- Fare clic su **Installa**, quindi andare al passaggio 10.
- Fare clic su **Modifica posizione di installazione**.
  1 Nella finestra Selezione destinazione, selezionare tutti gli utenti. Attualmente, questa è l'unica opzione.
  2 Fare clic su **Continua.**
  3 Fare clic su **Installa**, quindi andare al passaggio 10.

10 Nella finestra di dialogo, immettere nome e password e fare clic su **Installa software**.

11 Nella finestra Riepilogo, fare clic su **Chiudi**.

12 Quando richiesto, mantenere il file .pkg o spostarlo nel *Cestino*.

13 Eseguire una delle azioni seguenti:

Dell Security Center Hosted	Dell Management Server On-premises
La finestra Credenziali si apre automaticamente al termine dell'installazione. Se l'azienda è multi-tenant, è necessario un ID di installazione. 1 Nella finestra Credenziali, immettere l'email dell'account di accesso e fare clic su **Continua**. 2 Eseguire una delle azioni seguenti: • Se l'azienda è multi-tenant, immettere un ID di installazione e fare clic su **Continua**. Procedere al punto 3. **N.B.:** Se viene visualizzato un errore, controllare le proprie credenziali. Se si notano un indirizzo e-mail o ID di installazione non corretti, fare clic su **Riavvia inizializzazione** per inserire nuovamente le credenziali. • Per singoli tenant, procedere al punto 3. 3 Nella finestra Microsoft, immettere la password e fare clic su **Accedi**. 4 Nella finestra Azure, immettere la password. 5 Fare clic su **Accedi**. **N.B.:** Se viene visualizzato un errore, controllare le proprie credenziali. Se si nota un indirizzo e-mail non corretto, fare clic su **Riavvia inizializzazione** per inserire nuovamente le credenziali. 6 Si apre l'interfaccia di Dell Data Guardian. Vedere Applicazione Dell Data Guardian.	1 Chiudere la finestra .dmg per aprire Finder. 2 Vedere Attivazione dell'utente finale.

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

Identifier	**GUID-839E9A73-4125-4A28-84A6-4F5CC4D734AC**
Status	**In Translation**

Attivazione dell'utente finale (on-premises)

Attivazione per Dell Management Server On-premises

Con un server on-premises, dopo aver aperto Dell Data Guardian per la prima volta, è necessario eseguire l'accesso per attivarlo:

1 Nel Finder, selezionare **Applicazioni**, e fare doppio clic su **Dell Data Guardian**.

2 Quando viene visualizzata la finestra Credenziali, inserire l'indirizzo del Dell Server, ad esempio azienda.server.com. Queste informazioni sono fornite dall'amministratore. Per impostazione predefinita, il numero di porta è 8443. Se la propria azienda modifica la porta predefinita con un numero di porta personalizzato, l'amministratore informerà l'utente.

> **N.B.:**
> Non deselezionare la casella di controllo Errori SSL, a meno che l'amministratore non lo richieda.

3 Inserire il proprio indirizzo e-mail e la password.

4 Fare clic su **Accedi** per attivare Data Guardian.

5 Vedere *Applicazione Dell Data Guardian* qui di seguito.

Per maggiori informazioni sull'autenticazione, consultare la Guida di Dell Data Guardian online.

Applicazione Dell Data Guardian

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

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

Se l'autenticazione di Data Guardian è stata revocata o è scaduta, anche il nome del provider di archiviazione cloud è disattivato.

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

2 Si apre una finestra che richiede le credenziali dell'utente. Immettere le proprie credenziali.

Una volta eseguita l'autenticazione, il nome del provider di archiviazione cloud risulterà attivo.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center Hosted e tenant sospeso

Con Dell Security Center Hosted, se un tenant non riesce a effettuare pagamenti per un periodo di tempo specificato, il tenant può essere sospeso. Si applica a Windows, Mac, dispositivi mobili e portale web.

Gli utenti interni ed esterni di Data Guardian possono riscontrare le seguenti condizioni:

- Tutte le piattaforme - Se si tenta di installare Data Guardian, eseguire l'attivazione e l'accesso, viene visualizzata una finestra di dialogo indicante che il tenant è sospeso.

- Mac - Se il tenant è sospeso mentre Data Guardian è aperto, viene visualizzata la relativa finestra di dialogo dopo aver chiuso Esplora file e tutti i file e l'utente tenta di aprire un file protetto.
- Portale web:
  - Se è già stato effettuato l'accesso e si carica un file crittografato, appare il messaggio Caricamento non riuscito.
  - Se un file crittografato o non crittografato è stato caricato e quindi il tenant viene sospeso, appare il messaggio Download non riuscito.
  - Se si esegue la disconnessione e si tenta di accedere nuovamente, appare una finestra di dialogo che indica che il tenant è sospeso.

Contattare l'amministratore.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Proteggere applicazioni e tipi di file aggiuntivi con la protezione di base dei file

L'amministratore comunicherà se i criteri consentono la crittografia di applicazioni e tipi di file aggiuntivi. Se qualcuno apre un file crittografato con protezione di base dei file ma non ha installato Data Guardian, i contenuti sono illeggibili.

Panoramica della protezione di base dei file

Applicazioni

Di seguito sono riportati alcuni esempi di applicazioni che l'amministratore potrebbe crittografare:

- Blocco note
- WordPad
- Visio
- MS Paint

> **N.B.:**
> Alcune applicazioni sono solo parzialmente supportate con Data Guardian e l'amministratore le indicherà all'utente.

Tipi di file

Di seguito sono riportati alcuni esempi di tipi di file aggiuntivi che possono essere configurati: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e Mobile

Quando il criterio Protezione di base dei file è configurato, Data Guardian cerca nei computer degli utenti e crittografa tutti i file locali con queste estensioni. I file crittografati con Protezione di base dei file possono essere visualizzati e modificati solo con l'applicazione associata alla relativa estensione.

> **N.B.:**
> I file nelle cartelle di sistema specifiche non vengono crittografati, ad esempio AppData, così come le cartelle che si riferiscono a documenti di Office protetti, ad esempio la cartella Documenti sicuri.

Icone di sovrapposizione per Windows

Per Data Guardian 2.2 e versioni successive, vengono visualizzate icone di sovrapposizione sui file protetti in Esplora file. Se si fa clic con il pulsante destro del mouse sul file protetto, una scheda Dell Data Guardian fornisce ulteriori informazioni.

Escludere alcuni file dalla scansione in Windows o Mac (prima che la ricerca venga abilitata)

Se l'azienda decide di crittografare un tipo di file aggiuntivo, ad esempio. txt, potrebbe non essere necessario che tutti i file con tale estensione vengano scansionati e crittografati.

Prima di abilitare la Protezione di base dei file per tale estensione, l'amministratore può impostare un altro criterio che consente di aggiungere una cartella al computer locale e i file in tale cartella non vengono scansionati. L'amministratore può impostare un criterio, creare un nome di cartella, fornire il nome della cartella e suggerire dove è possibile aggiungere la cartella. Questi potrebbero essere file necessari al sistema o i file che non richiedono protezione.

IMPORTANTE:

È necessario creare la cartella prima che l'amministratore abiliti il criterio Protezione di base dei file.

1 Utilizzare il nome e il percorso della cartella forniti dall'amministratore.
   - Per Mac, passare al **riquadro Preferenze > Esclusioni della protezione di base dei file**. Qui viene visualizzato il nome della cartella da creare e il percorso.

2 Aggiungere i file con l'estensione specificata, ad esempio. txt, che non devono essere crittografati. Facoltativamente, è possibile aggiungere sottocartelle con nomi creati dall'utente.

   N.B.:

   Se si dispone di file con una data estensione, crittografati in precedenza, non saranno decrittografati una volta inseriti in quella cartella. Resteranno crittografati. Se si dispone di una cartella **Documenti non protetti**, che l'amministratore può creare tramite un altro criterio, è possibile collocare i tipi Protezione di base dei file in questa cartella per decrittografarli.

3 Una volta abilitata la Protezione di base dei file, se si dispone di file non protetti con tale estensione su una rete o su un'unità esterna, è possibile copiarli nella cartella esclusa. Resteranno non crittografati. In caso contrario, saranno crittografati.

Se il proprio computer dispone di più utenti, solo l'utente attualmente connesso può collocare i file nella cartella ed escluderli dalla scansione. Tutti i file che un altro utente colloca in quella cartella verranno scansionati e crittografati.

Rimozione di un'estensione di file in Windows o Mac

L'amministratore può decidere di rimuovere un'estensione di file. In tal caso, il computer è sottoposto a ricerca al fine di decrittografare i file di questo tipo.

- La scheda *Properties* > *Dell Data Guardian* del file crittografato non viene più visualizzata.
- Se esistevano icone di sovrapposizione dei file, non vengono più visualizzate.
- Possono essere necessari diversi minuti per completare la decrittografia dei file. Se un file con l'estensione in questione è ancora crittografato, potrebbe essere stato aperto durante la ricerca oppure archiviato su un file server o in un'altra posizione.

Rivolgersi all'amministratore per richiedere il ripristino di tutti i file con l'estensione desiderata che non vengono decrittografati.

Applicazioni Office

È possibile utilizzare un'applicazione Office per aprire un file crittografato con Protezione di base dei file, ma i contenuti sono di sola lettura.

Portale Web

In Impostazioni > Criteri, se la protezione di base dei file è attivata, l'amministratore ha aggiunto tipi di file non Office che Data Guardian crittograferà in seguito al download dal portale web. L'amministratore deve indicare i tipi di file.

N.B.:

Se si carica un tipo di file non ancora supportato, non sarà possibile leggerne il contenuto nel portale Web.

È possibile caricare tipi di file non Office crittografati o non crittografati. Tuttavia, quando si scarica il file non Office , l'estensione varia.

File non Office (ad esempio, .txt o .png)	Descrizione download
Crittografati prima di eseguire il caricamento Esempio: file non Office già crittografati da Windows o Mac.	Una volta scaricati dal portale web, l'estensione file viene mantenuta, ad esempio .txt o .png.
File non crittografati	Una volta scaricati dal portale web, l'estensione del file varia a seconda del fatto che l'amministratore abbia aggiunto l'estensione a una policy. Tuttavia, sono crittografati. Esempi di un file in formato .txt scaricato dal portale web: • **nomefile.txt** - L'amministratore ha aggiunto il tipo di file .txt a una policy. • **nomefile.txt.xen** - Il file .txt non è incluso nella policy. Il file viene crittografato ma aggiunge un'estensione .xen.

Se la policy *Modifica* è attivata per il portale web, gli utenti possono modificare i file non Office.

Identifier	**GUID-FC539BCB-1939-4E0A-8A36-**
Status	**Translation Validated**

Installare e utilizzare 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. L'app Data Guardian deve essere installata sul dispositivo mobile per visualizzare o utilizzare i file crittografati.

Identifier	**GUID-116F412E-15BE-4E29-A886-5A308BA693ED**
Status	**Translated**

Prerequisito

Prima di utilizzare l'app Data Guardian, determinare il sistema necessario in base al proprio ambiente:

Dell Security Center Hosted	Dell Management Server On-premises
Se l'ambiente hosted è un ambiente multi-tenant, è necessario un ID di installazione.	Accertarsi di conoscere il nome del Dell Server, ad esempio server.dominio.com. Queste informazioni sono fornite dall'amministratore.

Identifier	**GUID-A802F8F9-1B8F-47DD-8525-518A4C004221**
Status	**Translation Validated**

Guida introduttiva a Data Guardian Mobile

Seguire questa procedura per utilizzare Data Guardian Mobile.

Attività	Descrizione	Consultare questa sezione
Installare Data Guardian - Scegliere un'opzione:	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
Individuare i criteri che si applicano al dispositivo mobile	L'amministratore indicherà all'utente quali criteri si applicano.	È possibile disporre di: • Documenti di Office protetti • Protezione cloud • Opzioni aggiuntive

Attività	Descrizione	Consultare questa sezione
Esplorazione in File Manager	Vedere le opzioni di Data Guardian.	Esplorazione in File Manager
Se il criterio Protezione cloud è abilitato, accedere al proprio account del provider di archiviazione cloud	Sul dispositivo, passare alla schermata File Manager dell'app Data Guardian e toccare il provider di archiviazione cloud.	Vedere Accedere all'account del provider di archiviazione cloud.

In base ai criteri di Data Guardian, è possibile avere:

- File Office protetti (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) che mantengono le loro estensioni di file.
- Altre applicazioni e tipi di file, ad esempio .txt.
- I file non di Office nel cloud hanno un'estensione .xen.

Sui dispositivi mobili con Data Guardian è possibile:

- Creare cartelle e file
- Eliminare cartelle e file
- Condividere un documento con un utente esterno (se è abilitato il criterio per visualizzatori esterni)

Identifier	**GUID-618A6EAF-794D-4077-A675-AC9ACA624CC3**
Status	**In Translation**

Installare o disinstallare Data Guardian su un dispositivo iOS tramite l'App Store

Installazione su un dispositivo iOS

Prerequisito: se il dispositivo supporta uno scanner di impronte digitali ID Touch e si desidera utilizzarlo al posto del PIN, è necessario configurare il dispositivo per l'ID Touch prima di installare Data Guardian.

1 Sul dispositivo, toccare **App Store** e cercare Data Guardian.
2 Selezionare e installare l'app **Data Guardian**.
3 Toccare la casella di controllo per accettare il contratto di licenza.
4 Selezionare una delle seguenti opzioni:

Dell Security Center Hosted	On-premises
Una soluzione SaaS (Software-as-a-Service) hosted per la gestione del software Dell Data Security. a Toccare **Dell Security Center Hosted**. b Immettere il proprio indirizzo email. c Toccare **Invia**. **N.B.:** Se l'indirizzo email immesso viene trovato su più tenant, digitare l'ID di installazione. d Nella finestra Microsoft Azure, immettere la password. e Toccare **Accedi**.	Un server on-premises che si trova all'interno della rete aziendale per la gestione del software Dell Data Security. a Toccare **On-premises**. b Nel campo Server della schermata di accesso, immettere il nome del Dell Server dell'azienda, ad esempio: server.domain.com. c Immettere nome utente e password. d Toccare **Accedi**.

5 Quando richiesto, toccare il sensore per le impronte digitali o creare un PIN.

L'account è ora attivo e viene visualizzata la schermata File Manager di Data Guardian.

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**.

Identifier	GUID-7247F5B1-D730-4DE6-97BA-7E88AD40B7E4
Status	In Translation

Installare o disinstallare Data Guardian su un dispositivo iOS con Workspace ONE

Se è installato Workspace ONE, è possibile eseguire l'autenticazione in Data Guardian con single sign-on. Questa procedura è la stessa per Dell Security Center Hosted o Dell Management Server On-premises.

L'amministratore eseguirà il push dell'app Data Guardian sul dispositivo.

1 Quando viene richiesto se si desidera installare l'app **Data Guardian**, toccare **OK**.
2 Avviare l'app Data Guardian.
3 Quando viene visualizzato il contratto di licenza, toccare **Accetto**.
4 Quando viene richiesto di selezionare Workspace ONE o Data Guardian, toccare **Workspace ONE** per ottenere il single sign-on.
5 Inserire la password.
6 Quando richiesto, creare un PIN.

> **N.B.:**
> Se si esegue l'accesso a Workspace ONE, è sufficiente inserire il PIN per Data Guardian.

L'account è ora attivo e viene visualizzata la schermata File Manager di Data Guardian.

Identifier	GUID-D045F8A7-9124-4843-BAF6-E0BB27CE1046
Status	In Translation

Installare o disinstallare Data Guardian su un dispositivo Android tramite Google Play

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 Toccare la casella di controllo per accettare il contratto di licenza.
4 Selezionare una delle seguenti opzioni:

Dell Security Center Hosted	Dell Management Server On-premises
Una soluzione SaaS (Software-as-a-Service) hosted per la gestione del software Dell Data Security. a Toccare **Hosted**. b Immettere il proprio indirizzo email. c Toccare **Invia**.	Un server on-premises che si trova all'interno della rete aziendale per la gestione del software Dell Data Security. a Toccare **On-premises**. b Nel campo Server della schermata di accesso, immettere il nome del Dell Server dell'azienda, ad esempio: server.domain.com.

Dell Security Center Hosted	Dell Management Server On-premises
N.B.: Se l'indirizzo email immesso viene trovato su più tenant, digitare l'ID di installazione.	c Immettere nome utente e password. d Toccare **Accedi**.

d Nella finestra Microsoft Azure, immettere la password.

e Toccare **Accedi**.

5 Quando richiesto, creare un PIN.

L'account è ora attivo e viene visualizzata la schermata File Manager di Data Guardian.

Disinstallare l'app Data Guardian

1 Nel drawer delle app di Android, toccare **Impostazioni**.
2 In **Impostazioni**, toccare **App**.
3 Toccare e tenere premuto l'icona **Data Guardian**.
4 Trascinare l'icona sull'opzione Disinstalla.
5 Toccare **OK**.

Identifier	GUID-37A6FDB2-CD4D-4EB3-BDE1-EC151BC08814
Status	In Translation

Installare o disinstallare Data Guardian su un dispositivo Android con Workspace ONE

Se è installato Workspace ONE, è possibile eseguire l'autenticazione in Data Guardian con single sign-on. Questa procedura è la stessa per Dell Security Center Hosted o Dell Management Server On-premises.

1 Nel dispositivo, toccare **Hub**.
2 Toccare **Catalogo app**.
3 Nell'app Dell Data Guardian, toccare **Installa**.
4 Nella finestra *Conferma installazione*, toccare **Installa**.
5 Nella finestra *Google Play Protect*, toccare **Consenti**.
6 Quando viene visualizzato il messaggio di installazione dell'app, toccare **Fine**.
7 Toccare **Apri** per aprire l'app Data Guardian.
8 Quando viene richiesto di autenticare Workspace ONE o Data Guardian, toccare **Workspace ONE** per ottenere il single sign-on.
9 Quando viene visualizzato il contratto di licenza, toccare la casella di controllo.
10 Toccare **Single Sign-On**.
11 Quando richiesto, creare un PIN.

N.B.: Se si esegue l'accesso a Workspace ONE, è sufficiente inserire il PIN per Data Guardian.

L'account è ora attivo e viene visualizzata la schermata File Manager di Data Guardian.

Disinstallare l'app Data Guardian

1 Nel drawer delle app di Android, toccare **Impostazioni**.
2 In **Impostazioni**, toccare **App**.
3 Tenere premuta l'icona **Data Guardian**.

4 Trascinare l'icona sull'opzione Disinstalla.
5 Toccare **OK**.

Identifier	GUID-5B8DFEFC-DC7C-42AE-A662-627068964BC8
Status	In Translation

Esplorazione di File Manager

In File Manager di Data Guardian, è possibile utilizzare l'archiviazione locale o il cloud. File Manager viene aperto quando si apre Data Guardian.

Schermata File Manager

Le cartelle predefinite per la schermata File Manager includono:

- Documents
- Download
- Foto

Schermata Crea nuovo

Toccando l'icona Aggiungi (**+**) viene visualizzata la schermata *Crea nuovo* con le seguenti opzioni:

- Documento
- Foglio di calcolo
- Presentazione (PowerPoint)
- Foto
- Cartella
- Servizio cloud

Opzioni del drawer di navigazione

Toccare l'icona del drawer di navigazione. Le opzioni includono:

- **Browser**
- **File Manager**
- Icona **Impostazioni**:
  - Pulsante **Modifica PIN** (se attivato dal criterio)
  - **Browser**
  - **File Manager (Impostazioni)** - Utilizzare queste opzioni
    - **Intervallo aggiornamento** - La frequenza con cui Data Guardian sincronizza i servizi cloud. Dell consiglia di utilizzare l'impostazione *Manuale* o *Ogni giorno*. Le altre opzioni disponibili sono *Ogni ora* e *Ogni settimana*.
    - **Avviso download 10 MB** - Attivare o disattivare. Utilizzare questa impostazione se non si utilizza una rete Wi-Fi e le dimensioni del download superano i 10 MB.
    - **Cancella cache** - Cancella i file temporanei.
  - (iOS)- **ID Touch** o **ID faccia**, a seconda della versione iOS e se si dispone di un'impronta o riconoscimento facciale preconfigurati. Toccare per abilitare o disabilitare durante l'uso di Data Guardian.
  - **Informazioni su** - Vedere Criteri e versione di Data Guardian

  - Pulsante **Chiudi Data Guardian**
  - **Account cloud** - Indica se gli account sono Collegati o Scollegati.
- **Browser**
- **File Manager** - Consente di tornare alla schermata File Manager.
- **Blocca Data Guardian**

Opzioni aggiuntive

- Aggiungere un file ai Preferiti
  - Per iOS, consultare il drawer di navigazione.
  - Per Android, tenere premuto il nome del file.

Identifier	**GUID-8826272C-679E-40FF-B0A9-D1C9888AF6E5**
Status	**Translation Validated**

Individuare i criteri per Data Guardian Mobile

L'amministratore indicherà all'utente quali criteri sono impostati per la propria azienda.

Identifier	**GUID-4C1E2DAD-C0CA-4E6F-96D4-0297C01CE8B2**
Status	**Translation Validated**

Visualizzare i criteri e la versione di Data Guardian

Alcuni criteri di Data Guardian sono elencati in **Informazioni su**. Per visualizzare questi criteri o la versione di Data Guardian:

1 Nel drawer di navigazione di Data Guardian, toccare **Impostazioni > Informazioni**.
2 Toccare **Criteri**.
Sulla base dei criteri impostati dall'amministratore, l'elenco potrebbe includere:
- Lunghezza PIN
- Timeout inattività
- Errore di accesso
- Copia e incolla - Consente di copiare contenuti da un documento protetto a un altro.

Versione
3 Determinare opzioni aggiuntive dei criteri.
Queste possono includere:
- Documenti di Office protetti
- Protezione cloud
- Criteri aggiuntivi

Identifier	**GUID-3613C9F0-10DE-4A67-9158-1964C8D2D77E**
Status	**Translation Validated**

Utilizzare i documenti Office protetti con dispositivi mobili

L'amministratore indicherà all'utente quali opzioni sono abilitate per la propria azienda. Quando Data Guardian è installato e si apre un documento di Office protetto, compare un messaggio che indica che è in corso la decrittografia del documento.

Opzioni di Data Guardian per i documenti Office

Vengono visualizzate le seguenti opzioni di Data Guardian.

- **Crea** - In base all'impostazione dei criteri, il documento viene protetto al momento della creazione. L'intestazione di questo file è *Documento protetto*.
- **Copia/Incolla** - Con un documento di Office protetto è possibile copiare contenuti solo in un altro documento di Office protetto.
- **Stampa** - In base alle altre impostazioni dei criteri, è possibile avere una filigrana quando si esegue la stampa.
- **Esporta** - In base alle altre impostazioni dei criteri, è possibile avere una filigrana quando si esegue l'esportazione.

Quando un documento Office viene aperto, toccare l'icona in alto a sinistra per visualizzare queste opzioni:

- **Salva**
- **Salva con nome**
- **Esporta**
- **Esci**

Opzioni aggiuntive di Office in base al criterio:

- **Modifica** - È possibile modificare file Office con estensione .docx e .ppt.

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

- **Filigrana nascosta** - In base al criterio applicato, i documenti di Office protetti possono avere una filigrana nascosta che identifica l'utente. Se si stampa o si condivide il documento, la filigrana persiste.
- **Filigrana su schermo** - Quando un qualsiasi documento di Office protetto viene aperto, una filigrana viene visualizzata sullo schermo del client.

Ulteriori informazioni per i documenti Office

Documenti Office protetti nella modalità offline

Quando si crea un documento di 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.

Risoluzione dei problemi con i documenti di Office protetti

Su un dispositivo iOS, se si apre un documento di 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.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Proteggere applicazioni e tipi di file aggiuntivi con la protezione di base dei file

L'amministratore comunicherà se i criteri consentono la crittografia di applicazioni e tipi di file aggiuntivi. Se qualcuno apre un file crittografato con protezione di base dei file ma non ha installato Data Guardian, i contenuti sono illeggibili.

Panoramica della protezione di base dei file

Applicazioni

Di seguito sono riportati alcuni esempi di applicazioni che l'amministratore potrebbe crittografare:

- Blocco note
- WordPad
- Visio
- MS Paint

> **N.B.:**
> Alcune applicazioni sono solo parzialmente supportate con Data Guardian e l'amministratore le indicherà all'utente.

Tipi di file

Di seguito sono riportati alcuni esempi di tipi di file aggiuntivi che possono essere configurati: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e Mobile

Quando il criterio Protezione di base dei file è configurato, Data Guardian cerca nei computer degli utenti e crittografa tutti i file locali con queste estensioni. I file crittografati con Protezione di base dei file possono essere visualizzati e modificati solo con l'applicazione associata alla relativa estensione.

> **N.B.:**
> I file nelle cartelle di sistema specifiche non vengono crittografati, ad esempio AppData, così come le cartelle che si riferiscono a documenti di Office protetti, ad esempio la cartella Documenti sicuri.

Icone di sovrapposizione per Windows

Per Data Guardian 2.2 e versioni successive, vengono visualizzate icone di sovrapposizione sui file protetti in Esplora file. Se si fa clic con il pulsante destro del mouse sul file protetto, una scheda Dell Data Guardian fornisce ulteriori informazioni.

Escludere alcuni file dalla scansione in Windows o Mac (prima che la ricerca venga abilitata)

Se l'azienda decide di crittografare un tipo di file aggiuntivo, ad esempio. txt, potrebbe non essere necessario che tutti i file con tale estensione vengano scansionati e crittografati.

Prima di abilitare la Protezione di base dei file per tale estensione, l'amministratore può impostare un altro criterio che consente di aggiungere una cartella al computer locale e i file in tale cartella non vengono scansionati. L'amministratore può impostare un criterio, creare

un nome di cartella, fornire il nome della cartella e suggerire dove è possibile aggiungere la cartella. Questi potrebbero essere file necessari al sistema o i file che non richiedono protezione.

IMPORTANTE:

È necessario creare la cartella prima che l'amministratore abiliti il criterio Protezione di base dei file.

1 Utilizzare il nome e il percorso della cartella forniti dall'amministratore.
   - Per Mac, passare al **riquadro Preferenze > Esclusioni della protezione di base dei file**. Qui viene visualizzato il nome della cartella da creare e il percorso.

2 Aggiungere i file con l'estensione specificata, ad esempio. txt, che non devono essere crittografati. Facoltativamente, è possibile aggiungere sottocartelle con nomi creati dall'utente.

   N.B.:

   Se si dispone di file con una data estensione, crittografati in precedenza, non saranno decrittografati una volta inseriti in quella cartella. Resteranno crittografati. Se si dispone di una cartella **Documenti non protetti**, che l'amministratore può creare tramite un altro criterio, è possibile collocare i tipi Protezione di base dei file in questa cartella per decrittografarli.

3 Una volta abilitata la Protezione di base dei file, se si dispone di file non protetti con tale estensione su una rete o su un'unità esterna, è possibile copiarli nella cartella esclusa. Resteranno non crittografati. In caso contrario, saranno crittografati.

Se il proprio computer dispone di più utenti, solo l'utente attualmente connesso può collocare i file nella cartella ed escluderli dalla scansione. Tutti i file che un altro utente colloca in quella cartella verranno scansionati e crittografati.

Rimozione di un'estensione di file in Windows o Mac

L'amministratore può decidere di rimuovere un'estensione di file. In tal caso, il computer è sottoposto a ricerca al fine di decrittografare i file di questo tipo.

- La scheda *Properties* > *Dell Data Guardian* del file crittografato non viene più visualizzata.
- Se esistevano icone di sovrapposizione dei file, non vengono più visualizzate.
- Possono essere necessari diversi minuti per completare la decrittografia dei file. Se un file con l'estensione in questione è ancora crittografato, potrebbe essere stato aperto durante la ricerca oppure archiviato su un file server o in un'altra posizione.

Rivolgersi all'amministratore per richiedere il ripristino di tutti i file con l'estensione desiderata che non vengono decrittografati.

Applicazioni Office

È possibile utilizzare un'applicazione Office per aprire un file crittografato con Protezione di base dei file, ma i contenuti sono di sola lettura.

Portale Web

In Impostazioni > Criteri, se la protezione di base dei file è attivata, l'amministratore ha aggiunto tipi di file non Office che Data Guardian crittograferà in seguito al download dal portale web. L'amministratore deve indicare i tipi di file.

N.B.:

Se si carica un tipo di file non ancora supportato, non sarà possibile leggerne il contenuto nel portale Web.

È possibile caricare tipi di file non Office crittografati o non crittografati. Tuttavia, quando si scarica il file non Office , l'estensione varia.

File non Office (ad esempio, .txt o .png)	Descrizione download
Crittografati prima di eseguire il caricamento	Una volta scaricati dal portale web, l'estensione file viene mantenuta, ad esempio .txt o .png.

File non Office (ad esempio, .txt o .png)	Descrizione download
Esempio: file non Office già crittografati da Windows o Mac.	
File non crittografati	Una volta scaricati dal portale web, l'estensione del file varia a seconda del fatto che l'amministratore abbia aggiunto l'estensione a una policy. Tuttavia, sono crittografati. Esempi di un file in formato .txt scaricato dal portale web: • **nomefile.txt** - L'amministratore ha aggiunto il tipo di file .txt a una policy. • **nomefile.txt.xen** - Il file .txt non è incluso nella policy. Il file viene crittografato ma aggiunge un'estensione .xen.

Se la policy *Modifica* è attivata per il portale web, gli utenti possono modificare i file non Office.

Identifier	**GUID-36644E42-9324-479F-8128-F89D438E8F17**
Status	**Translation Validated**

Utilizzare Protezione cloud con i dispositivi mobili

Se l'amministratore abilita Protezione cloud, sono necessarie due applicazioni:

- App del client di sincronizzazione cloud - Vedere la guida online per ulteriori informazioni sul client di sincronizzazione cloud.
- L'app Data Guardian Mobile indica il client di sincronizzazione cloud utilizzato dall'azienda e consente di scaricarlo.

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 documento di 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.

Accedere all'account del provider di archiviazione cloud

Per accedere all'account del provider di archiviazione cloud:

1. Nella schermata File Manager, toccare l'icona Aggiungi (+).
2. Toccare **Servizio cloud**.
   Un criterio di Data Guardian determina quali provider di archiviazione cloud visualizzare. L'amministratore può designare uno o più provider di archiviazione cloud specifici da utilizzare all'interno dell'azienda e può bloccarne altri.
3. 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.

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.

Utilizzare Protezione cloud

Sui dispositivi mobili con Data Guardian 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.

- 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.

- **File > Copia** - In base al criterio impostato dall'amministratore, è possibile copiare un file da un provider cloud all'altro.
- Per Android con OneDrive o 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.

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 > File Manager > Servizio cloud**. Quando si ottiene l'accesso a un provider di archiviazione cloud, un segno di spunta viene visualizzato nella casella di controllo.

2 Eseguire una delle azioni seguenti:

Android

a Toccare **Collegato**.

b Toccare **Sì**.

iOS

a Toccare **Scollegato**.

L'accesso e i file vengono rimossi da Data Guardian. I file non vengono rimossi dal cloud.

Risoluzione dei problemi relativi a Protezione cloud

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.

Identifier	**GUID-19337C15-12E9-4E8D-B908-29416128B500**
Status	**Translation Validated**

Utilizzare criteri aggiuntivi con i dispositivi mobili

L'amministratore indicherà all'utente quali di questi criteri sono stati impostati per la propria azienda.

Utilizzare un PIN

L'amministratore può impostare un criterio per richiedere un PIN e specificarne la lunghezza.

Manomissioni

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

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 di 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.

Identifier	**GUID-21086952-1999-4F9B-A47C-C57073C7C715**
Status	**Translation Validated**

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 in un server Google non nel Dell 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.

N.B.:
La funzione *Backup e sincronizzazione di Google* non è supportata.

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.

Identifier	**GUID-46C6144D-AF30-4559-96AC-39DB1738D2D8**
Status	**Translation Validated**

Registri

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

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center Hosted e tenant sospeso

Con Dell Security Center Hosted, se un tenant non riesce a effettuare pagamenti per un periodo di tempo specificato, il tenant può essere sospeso. Si applica a Windows, Mac, dispositivi mobili e portale web.

Gli utenti interni ed esterni di Data Guardian possono riscontrare le seguenti condizioni:

- Tutte le piattaforme - Se si tenta di installare Data Guardian, eseguire l'attivazione e l'accesso, viene visualizzata una finestra di dialogo indicante che il tenant è sospeso.
- Mac - Se il tenant è sospeso mentre Data Guardian è aperto, viene visualizzata la relativa finestra di dialogo dopo aver chiuso Esplora file e tutti i file e l'utente tenta di aprire un file protetto.
- Portale web:
  - Se è già stato effettuato l'accesso e si carica un file crittografato, appare il messaggio Caricamento non riuscito.
  - Se un file crittografato o non crittografato è stato caricato e quindi il tenant viene sospeso, appare il messaggio Download non riuscito.
  - Se si esegue la disconnessione e si tenta di accedere nuovamente, appare una finestra di dialogo che indica che il tenant è sospeso.

Contattare l'amministratore.

Identifier	**GUID-66FB1CE0-6669-4DDD-80E8-BCBAA27D4E13**
Status	**Translation Validated**

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.

Identifier	GUID-BDAC1DD8-21C2-4ED1-B0A
Status	In Translation

Visualizzare o modificare i file protetti su un client Web

Se l'amministratore imposta un portale Web di Data Guardian, è possibile collegarsi a un URL per questo client Web e visualizzare i file crittografati senza dover installare un client Data Guardian. A seconda dei criteri, è anche possibile modificare un file.

In base al criterio impostato dall'amministratore, è possibile visualizzare quanto segue:

- Documenti Office protetti: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- File .xen: file Office o non Office crittografati da Data Guardian durante il caricamento nel cloud.
- Altri tipi di file, come Blocco note.

In base al criterio impostato dall'amministratore, è possibile accedere a un provider di cloud storage.

Identifier	GUID-C468D78F-0ADF-45FC-B5A2-44B933EB2497
Status	Translation Validated

Accedere al portale Web per Data Guardian

La procedura varia leggermente a seconda del browser utilizzato.

1 Richiedere all'amministratore l'URL per accedere al portale Web.
2 Fare clic sull'URL.
Se si riceve un avviso, fare clic su **Continua** o **Procedi**.
3 Nella schermata del contratto di licenza, fare clic su **Accetto**.
Se si riceve un avviso, fare clic su **Continua** o **Procedi**.
4 Immettere le credenziali di dominio.
5 Fare clic su **Accedi**.
6 Se viene richiesto di registrare la propria posizione, selezionare un'opzione.
7 Per visualizzare o modificare i file, consultare la guida online disponibile nel portale Web di Data Guardian.

N.B.:
Per Mac è necessario configurare Safari in modo da consentire i pop-up.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Proteggere applicazioni e tipi di file aggiuntivi con la protezione di base dei file

L'amministratore comunicherà se i criteri consentono la crittografia di applicazioni e tipi di file aggiuntivi. Se qualcuno apre un file crittografato con protezione di base dei file ma non ha installato Data Guardian, i contenuti sono illeggibili.

Panoramica della protezione di base dei file

Applicazioni

Di seguito sono riportati alcuni esempi di applicazioni che l'amministratore potrebbe crittografare:

- Blocco note
- WordPad
- Visio
- MS Paint

> **N.B.:**
> Alcune applicazioni sono solo parzialmente supportate con Data Guardian e l'amministratore le indicherà all'utente.

Tipi di file

Di seguito sono riportati alcuni esempi di tipi di file aggiuntivi che possono essere configurati: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac e Mobile

Quando il criterio Protezione di base dei file è configurato, Data Guardian cerca nei computer degli utenti e crittografa tutti i file locali con queste estensioni. I file crittografati con Protezione di base dei file possono essere visualizzati e modificati solo con l'applicazione associata alla relativa estensione.

> **N.B.:**
> I file nelle cartelle di sistema specifiche non vengono crittografati, ad esempio AppData, così come le cartelle che si riferiscono a documenti di Office protetti, ad esempio la cartella Documenti sicuri.

Icone di sovrapposizione per Windows

Per Data Guardian 2.2 e versioni successive, vengono visualizzate icone di sovrapposizione sui file protetti in Esplora file. Se si fa clic con il pulsante destro del mouse sul file protetto, una scheda Dell Data Guardian fornisce ulteriori informazioni.

Escludere alcuni file dalla scansione in Windows o Mac (prima che la ricerca venga abilitata)

Se l'azienda decide di crittografare un tipo di file aggiuntivo, ad esempio. txt, potrebbe non essere necessario che tutti i file con tale estensione vengano scansionati e crittografati.

Prima di abilitare la Protezione di base dei file per tale estensione, l'amministratore può impostare un altro criterio che consente di aggiungere una cartella al computer locale e i file in tale cartella non vengono scansionati. L'amministratore può impostare un criterio, creare

un nome di cartella, fornire il nome della cartella e suggerire dove è possibile aggiungere la cartella. Questi potrebbero essere file necessari al sistema o i file che non richiedono protezione.

IMPORTANTE:

È necessario creare la cartella prima che l'amministratore abiliti il criterio Protezione di base dei file.

1 Utilizzare il nome e il percorso della cartella forniti dall'amministratore.
   - Per Mac, passare al **riquadro Preferenze > Esclusioni della protezione di base dei file**. Qui viene visualizzato il nome della cartella da creare e il percorso.

2 Aggiungere i file con l'estensione specificata, ad esempio. txt, che non devono essere crittografati. Facoltativamente, è possibile aggiungere sottocartelle con nomi creati dall'utente.

   N.B.:

   Se si dispone di file con una data estensione, crittografati in precedenza, non saranno decrittografati una volta inseriti in quella cartella. Resteranno crittografati. Se si dispone di una cartella **Documenti non protetti**, che l'amministratore può creare tramite un altro criterio, è possibile collocare i tipi Protezione di base dei file in questa cartella per decrittografarli.

3 Una volta abilitata la Protezione di base dei file, se si dispone di file non protetti con tale estensione su una rete o su un'unità esterna, è possibile copiarli nella cartella esclusa. Resteranno non crittografati. In caso contrario, saranno crittografati.

Se il proprio computer dispone di più utenti, solo l'utente attualmente connesso può collocare i file nella cartella ed escluderli dalla scansione. Tutti i file che un altro utente colloca in quella cartella verranno scansionati e crittografati.

Rimozione di un'estensione di file in Windows o Mac

L'amministratore può decidere di rimuovere un'estensione di file. In tal caso, il computer è sottoposto a ricerca al fine di decrittografare i file di questo tipo.

- La scheda *Properties* > *Dell Data Guardian* del file crittografato non viene più visualizzata.
- Se esistevano icone di sovrapposizione dei file, non vengono più visualizzate.
- Possono essere necessari diversi minuti per completare la decrittografia dei file. Se un file con l'estensione in questione è ancora crittografato, potrebbe essere stato aperto durante la ricerca oppure archiviato su un file server o in un'altra posizione.

Rivolgersi all'amministratore per richiedere il ripristino di tutti i file con l'estensione desiderata che non vengono decrittografati.

Applicazioni Office

È possibile utilizzare un'applicazione Office per aprire un file crittografato con Protezione di base dei file, ma i contenuti sono di sola lettura.

Portale Web

In Impostazioni > Criteri, se la protezione di base dei file è attivata, l'amministratore ha aggiunto tipi di file non Office che Data Guardian crittograferà in seguito al download dal portale web. L'amministratore deve indicare i tipi di file.

N.B.:

Se si carica un tipo di file non ancora supportato, non sarà possibile leggerne il contenuto nel portale Web.

È possibile caricare tipi di file non Office crittografati o non crittografati. Tuttavia, quando si scarica il file non Office , l'estensione varia.

File non Office (ad esempio, .txt o .png)	Descrizione download
Crittografati prima di eseguire il caricamento	Una volta scaricati dal portale web, l'estensione file viene mantenuta, ad esempio .txt o .png.

File non Office (ad esempio, .txt o .png)	Descrizione download
Esempio: file non Office già crittografati da Windows o Mac.	
File non crittografati	Una volta scaricati dal portale web, l'estensione del file varia a seconda del fatto che l'amministratore abbia aggiunto l'estensione a una policy. Tuttavia, sono crittografati. Esempi di un file in formato .txt scaricato dal portale web: • **nomefile.txt** - L'amministratore ha aggiunto il tipo di file .txt a una policy. • **nomefile.txt.xen** - Il file .txt non è incluso nella policy. Il file viene crittografato ma aggiunge un'estensione .xen.

Se la policy *Modifica* è attivata per il portale web, gli utenti possono modificare i file non Office.

Identifier	**GUID-932E973E-B2CD-4305-B50F-F85231243FA4**
Status	**In Translation**

Utilizzare un provider di cloud storage

In base al criterio, il portale Web può accedere a un provider di cloud storage. Per maggiori informazioni, consultare la Guida in linea per il portale Web.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center Hosted e tenant sospeso

Con Dell Security Center Hosted, se un tenant non riesce a effettuare pagamenti per un periodo di tempo specificato, il tenant può essere sospeso. Si applica a Windows, Mac, dispositivi mobili e portale web.

Gli utenti interni ed esterni di Data Guardian possono riscontrare le seguenti condizioni:

- Tutte le piattaforme - Se si tenta di installare Data Guardian, eseguire l'attivazione e l'accesso, viene visualizzata una finestra di dialogo indicante che il tenant è sospeso.
- Mac - Se il tenant è sospeso mentre Data Guardian è aperto, viene visualizzata la relativa finestra di dialogo dopo aver chiuso Esplora file e tutti i file e l'utente tenta di aprire un file protetto.
- Portale web:
  - Se è già stato effettuato l'accesso e si carica un file crittografato, appare il messaggio Caricamento non riuscito.
  - Se un file crittografato o non crittografato è stato caricato e quindi il tenant viene sospeso, appare il messaggio Download non riuscito.
  - Se si esegue la disconnessione e si tenta di accedere nuovamente, appare una finestra di dialogo che indica che il tenant è sospeso.

Contattare l'amministratore.

Identifier	GUID-FF3D5442-1632-454D-8787-1
Status	Translation Validated

Utilizzare 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.

Gli utenti esterni devono soddisfare i requisiti del server. Inoltre, il dominio o l'utente non devono trovarsi nella blacklist dell'azienda.

In un ambiente hosted, gli utenti esterni possono attivarsi con un solo tenant.

Le opzioni per gli utenti esterni includono:

- **Windows** - Scaricare e installare un client Data Guardian. Consultare le sezioni Attività dell'utente interno in Windows e Attività dell'utente esterno.
- **Mac** - Consultare la sezione Utente esterno e Mac.
- **Mobile**
- **Portale Web** - Invece di scaricare un client Data Guardian, utilizzare il portale Web Data Guardian. Gli utenti esterni possono visualizzare un documento di Office protetto, un file .pdf o .xen. Sulla base dei criteri impostati, l'utente esterno può modificare il file. Consultare la sezione Utente esterno e portale Web.

Identifier	GUID-EBDBAE23-A90F-4603-934B-6B40EE93C248
Status	In Translation

Attività dell'utente interno in Windows

Per condividere file protetti con un utente esterno, è possibile:

- Utilizzare l'opzione *Accesso ai file protetti* con documenti di Office protetti
- Approvare o rifiutare l'accesso quando un utente esterno richiede l'accesso
- Inviare un documento di Office protetto tramite un messaggio e-mail di Outlook.

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 protetto e selezionare **Accesso ai file protetti**. È possibile selezionare uno o più file, fino a 50. Viene visualizzata la finestra Condivisione accesso a documenti protetti. I file possono trovarsi nelle seguenti posizioni:
   - Unità di rete o cartella locale

- E-mail
- Supporto rimovibile
- Condivisione di rete

2 Nel campo *Indirizzo e-mail per condivisione*, nell'angolo in alto a destra, immettere l'indirizzo email 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 gli utenti esterni non ancora registrati che riceveranno un messaggio email con le istruzioni per registrarsi su un Dell Server, scaricare e attivare 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.

Inviare un file protetto tramite un messaggio email di Outlook

Quando si allega un file protetto e si fa clic su *Invia*, 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.

Identifier	GUID-967BF32F-F6F1-4C5A-BA0B-34CA9F73A438
Status	In Translation

Attività dell'utente esterno in Windows

Un utente interno può decidere di autorizzare l'accesso a file protetti. L'utente autorizzato può ricevere:

- Un'email contenente le istruzioni per la registrazione
- Un file protetto con una pagina di copertina su cui è riportato un collegamento per registrare un indirizzo email valido

N.B.:
Nella pagina di copertina è riportato il nome del Dell Server, se il server è di tipo on-premises, o un ID di installazione, se Dell Security Center Hosted è multi-tenant. La pagina di copertina contiene anche i link per scaricare il client di Data Guardian.

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

- Registrarsi in Data Guardian
- Scaricare e installare Data Guardian - L'utente esterno deve disporre dei diritti di amministratore sul suo computer.

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 Eseguire una delle azioni seguenti:
   - Email - Fare clic su **Accetta**.
   - Documento protetto che visualizza un avviso sulla pagina di copertina - Fare clic sul link fornito per registrare un indirizzo email valido.

2 Seguire una procedura in base all'ambiente dell'azienda:

Dell Security Center Hosted

Una soluzione SaaS (Software-as-a-Service) hosted per la gestione del software Dell Data Security.

a Quando si apre il portale Web Dell Data Guardian, immettere il proprio indirizzo di posta elettronica.

b Scorrere in basso e fare clic su **Accetto**.

c Nella finestra Dell Security Center, scorrere in basso fino a *Vuoi registrare un account?* e fare clic su **Registra**.

d Nella pagina del nuovo account, immettere un indirizzo email, nome, cognome e password. La password deve essere lunga almeno otto caratteri e deve contenere una lettera minuscola, una lettera maiuscola, un carattere speciale e un numero.

e Fare clic su **Registra**.

f Spostarsi all'indirizzo email utilizzato per la registrazione per recuperare il codice di verifica e immetterlo.

> **N.B.:**
> Se non viene visualizzato un messaggio e-mail, controllare la cartella della posta indesiderata (spam).

g Fare clic su **Conferma account**. Se l'indirizzo viene verificato, il portale Web si apre.

h Trascinare il file protetto nel portale web e fare clic su **Carica ora**.

i Si riceverà un messaggio di benvenuto dopo aver effettuato la registrazione. Questo messaggio contiene un link per scaricare un client Windows.

> **N.B.:**
> Se il Dell Security Center Hosted è multi-tenant, il messaggio email elenca anche un ID di installazione necessario.

Dell Management Server On-premises

Un server on-premises che si trova all'interno della rete aziendale per la gestione del software Dell Data Security.

> **N.B.:**
> Per un ambiente on-premises è possibile installare Data Guardian prima di effettuare la registrazione. Per eseguire l'attivazione, fare clic sul link **Registra**.

a Quando si apre la finestra Dell Data Guardian, immettere il proprio indirizzo di posta elettronica.

b Fare clic su **Registra**.

c Nella pagina di registrazione, immettere e confermare la password, quindi fare clic su **Accedi**.

Viene visualizzata una finestra di dialogo di conferma della registrazione e viene inviato un messaggio e-mail all'indirizzo immesso dall'utente interno. Se non viene visualizzato il messaggio e-mail, controllare la cartella della posta indesiderata (spam).

d Nel messaggio e-mail di verifica dell'account inviato dal Dell Server, fare clic sul collegamento ipertestuale.

> **N.B.:**
> Se non viene visualizzato un messaggio e-mail, controllare la cartella della posta indesiderata (spam).

e Passare alla pagina Web.

f Nella pagina di conferma, fare clic su **Continua per effettuare l'accesso**.

g Nella pagina di accesso, fare clic su **Password dimenticata**.

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

h 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.

i Aprire il messaggio e-mail di attivazione dell'account e fare clic sul collegamento.

Nel messaggio e-mail è indicato anche il nome del Dell Server da utilizzare durante l'installazione di Data Guardian.

j Nella pagina Accedi, immettere l'indirizzo di posta elettronica e la password usati per registrarsi.

k Fare clic su **Accedi**.

Dell Security Center Hosted	Dell Management Server On-premises
	Viene visualizzata una pagina Scarica Data Guardian.

Scaricare e installare Data Guardian per Windows

Dopo la registrazione, è possibile fare clic su un link per scaricare un client Windows. A seconda di quanto fornito inizialmente dall'utente interno, i collegamenti potrebbero essere disponibili qui:

- Per un Security Management Server viene visualizzata la pagina Download con opzioni per il client Windows.
- Per un Security Management Server Virtual, facendo clic su Windows l'utente viene reindirizzato al sito dell.com/support.
- Se l'utente ha ricevuto un file protetto, la pagina di copertina contiene i collegamenti per il download di un client.
- Si potrebbe ricevere un messaggio email di benvenuto con i link per scaricare un client.

In questa procedura è descritta l'installazione di Data Guardian su Windows.

1 In Windows, fare clic su **Scarica (32 bit)** o **Scarica (64-bit)**, a seconda del sistema operativo del computer.
2 Scaricare il file di installazione in una directory del computer.
3 Fare doppio clic sul file di installazione per avviare il programma di installazione.
4 Selezionare una lingua e fare clic su **OK**.
5 Se viene richiesto di installare Microsoft Visual C++ 2010 Redistributable Package, fare clic su **OK**.
6 Nella schermata iniziale, fare clic su **Avanti**.
7 Leggere il contratto di licenza, accettare i termini, e fare clic su **Avanti**.
8 Nella schermata Cartella di destinazione, fare clic su **Avanti** per eseguire l'installazione nel percorso predefinito: **C:\Program Files\Dell \Dell Data Guardian\.**
9 Nella schermata Tipo di configurazione, selezionare una delle seguenti opzioni:

Dell Security Center Hosted	Dell Management Server On-premises
a Selezionare Dell Security Center Hosted. b Se l'azienda è multi-tenant, immettere l'ID di installazione riportato sulla pagina di copertina o nell'email di benvenuto. c Fare clic su **Avanti**. d Continuare con il passaggio 10.	a Selezionare Dell Management Server On-premises. b Nel campo *Nome server:*, immettere il nome del Dell 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. c Fare clic su **Avanti**. d Nella schermata Conferma server di attivazione, verificare l'esattezza dell'indirizzo URL del Dell Server. Il programma di installazione aggiunge www o http(s), e la porta. Fare clic su **Avanti**. e Continuare con il passaggio 10.

10 Nella finestra Tipo di gestione, selezionare questa opzione:
- Utente esterno - Un utente con un indirizzo e-mail non appartenente al dominio aziendale.

11 Fare clic su **Installa** per avviare l'installazione.
Viene visualizzata una finestra di stato che mostra l'avanzamento dell'installazione.
12 Fare clic su **Fine** quando viene visualizzata la schermata Installazione completata.
13 Fare clic su **Sì** per riavviare il sistema.
L'installazione di Data Guardian è completata.
14 Vedere Attivare Data Guardian.

N.B.:
Assicurarsi di vedere le note e le eccezioni in Utilizzare Data Guardian con Windows; ad esempio, non è possibile aprire un file .pdf protetto dalla rete. Per aprire un file .pdf protetto dalla rete, è possibile utilizzare Word.

Identifier	GUID-92B941BF-52D2-4302-AFA1-3D348E260E03
Status	In Translation

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**.

> **N.B.:**
> In un ambiente hosted, gli utenti esterni possono attivarsi con un solo tenant per volta. Se un utente si è già registrato con un tenant, deve disinstallare Data Guardian e reinstallarlo con l'altro ID di installazione. È anche possibile utilizzare il portale Web per caricare e visualizzare documenti protetti.

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

> **N.B.:**
> Per on-premises, se è stato installato Data Guardian prima di effettuare la registrazione, all'attivazione fare clic sul link **Registra**.

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

4 Confermare lo stato della modalità utente. Fare clic sulla scheda icona area di notifica e selezionare **Dettagli**.

In alto, la Modalità utente è:

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

Identifier	GUID-55AD51F6-9437-4B64-9A9F-E598A3BBDC74
Status	Translation Validated

Richiesta di accesso da parte di un utente interno

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

1 Se si apre un file documento di 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.

Identifier	**GUID-1DB6F793-018B-4F14-AA95-63980FCDD713**
Status	**Translation Validated**

Utente esterno e attività Mac

Attività per utente interno per Mac

Eseguire una delle azioni seguenti:

- Documenti protetti - Inviare all'utente esterno tramite email, share di rete o archiviazione rimovibile.
- Se è stata attivata la crittografia cloud di Data Guardian - Nell'interfaccia di Dell Data Guardian, trascinare i file protetti nella colonna accanto a quella del provider di archiviazione cloud.

Attività per utente esterno per Mac

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 Quando si apre un documento protetto che visualizza un avviso sulla pagina di copertina, fare clic sul collegamento fornito per registrare un indirizzo email valido.

> **N.B.:**
> Nella pagina di copertina è riportato il nome del Dell Server, se il server è di tipo on-premises, o un ID di installazione, se Dell Security Center Hosted è multi-tenant. La pagina di copertina contiene i link per scaricare il client di Data Guardian.

2 Effettuare una delle seguenti operazioni in base all'ambiente di utilizzo:

Dell Security Center Hosted

Una soluzione SaaS (Software-as-a-Service) hosted per la gestione del software Dell Data Security.

a Quando si apre il portale Web Dell Data Guardian, immettere il proprio indirizzo di posta elettronica.

b Scorrere in basso e fare clic su **Accetto**.

c Nella finestra Dell Security Center, scorrere in basso fino a *Vuoi registrare un account?* e fare clic su **Registra**.

d Nella pagina del nuovo account, immettere un indirizzo email, nome, cognome e password. La password deve essere lunga almeno otto caratteri e deve contenere una lettera minuscola, una lettera maiuscola, un carattere speciale e un numero.

e Fare clic su **Registra**.

f Spostarsi all'indirizzo email utilizzato per la registrazione per recuperare il codice di verifica e immetterlo.

> **N.B.:**
> Se non viene visualizzato un messaggio e-mail, controllare la cartella della posta indesiderata (spam).

g Fare clic su **Conferma account**. Se l'indirizzo viene verificato, il portale Web si apre.

Dell Management Server On-premises

Un server on-premises che si trova all'interno della rete aziendale per la gestione del software Dell Data Security.

a Quando si apre la finestra Dell Data Guardian, immettere il proprio indirizzo di posta elettronica.

b Fare clic su **Registra**.

c Nella pagina di registrazione, immettere e confermare la password, quindi fare clic su **Accedi**.

Viene visualizzata una finestra di dialogo di conferma della registrazione e viene inviato un messaggio e-mail all'indirizzo immesso dall'utente interno. Se non viene visualizzato il messaggio e-mail, controllare la cartella della posta indesiderata (spam).

d Aprire il messaggio e-mail di verifica dell'account e fare clic sul collegamento.

Nel messaggio e-mail è indicato anche il nome del Dell Server da utilizzare durante l'installazione di Data Guardian.

e Nella pagina di conferma della registrazione, fare clic su **Ritorna alla pagina di accesso**.

È possibile fare clic su un collegamento nella pagina di copertina per scaricare e installare un client. Vedere qui di seguito.

Dell Security Center Hosted	Dell Management Server On-premises
h Caricare il file protetto per visualizzarlo. Si riceve un'email con il collegamento per scaricare il client Mac. In alternativa, è possibile fare clic sul collegamento contenuto nella pagina di copertina. Vedere qui di seguito.	

Scaricare e installare un client Data Guardian (facoltativo)

1 Nella pagina Dell Data Guardian, immettere l'indirizzo di posta elettronica e la password usati per registrarsi.
2 Fare clic su **Accedi**.
Viene visualizzata una pagina Download del Data Guardian con le opzioni per Windows, iOS, Android e Mac OS X.
3 Sotto Mac OS X, fare clic su **Download**.
4 Nella pagina *Driver & download*, selezionare **Apple Mac OS** e fare clic su **Download**.
5 Scaricare il file .dmg in una directory sul computer ed eseguire .pkg.
6 Per eseguire l'accesso/l'attivazione, effettuare una delle seguenti operazioni:

Dell Security Center Hosted	Dell Management Server On-premises
a Immettere l'indirizzo email utilizzato per la registrazione. b Le informazioni di accesso sono quelle utilizzate per effettuare l'accesso al .dmg. c Fare clic su **Accedi**.	a Consultare la Guida online integrata di Data Guardian e immettere il nome del Dell Server riportato nell'email di verifica dell'account. b Immettere anche il proprio indirizzo email e la password. Le informazioni di accesso sono quelle utilizzate per la registrazione. c Fare clic su **Accedi**.

Identifier	**GUID-B2D2A78A-86B7-4D46-A530-C531CE3B706A**
Status	**Translation Validated**

Utente esterno e mobile

Se un utente interno condivide un link tramite il cloud a un file protetto, il file visualizza una pagina di copertina che contiene un link per la registrazione di un indirizzo email valido.

N.B.:
Nella pagina di copertina è riportato il nome del Dell Server, se il server è di tipo on-premises, o un ID di installazione, se Dell Security Center Hosted è multi-tenant. La pagina di copertina contiene anche i link per scaricare il client di Data Guardian.

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

- Registrarsi in Data Guardian
- Scaricare e installare Data Guardian - L'utente esterno deve disporre dei diritti di amministratore sul suo computer.

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 Nell'avviso sulla pagina di copertina fare clic sul link fornito per registrare un indirizzo email valido.
2 Seguire una procedura in base all'ambiente dell'azienda:

Dell Security Center Hosted

Una soluzione SaaS (Software-as-a-Service) hosted per la gestione del software Dell Data Security.

a Quando si apre il portale Web Dell Data Guardian, immettere il proprio indirizzo di posta elettronica.

b Scorrere in basso e fare clic su **Accetto**.

c Nella finestra Dell Security Center, scorrere in basso fino a *Vuoi registrare un account?* e fare clic su **Registra**.

d Nella pagina del nuovo account, immettere un indirizzo email, nome, cognome e password. La password deve essere lunga almeno otto caratteri e deve contenere una lettera minuscola, una lettera maiuscola, un carattere speciale e un numero.

e Fare clic su **Registra**.

f Spostarsi all'indirizzo email utilizzato per la registrazione per recuperare il codice di verifica e immetterlo.

> **N.B.:**
> Se non viene visualizzato un messaggio e-mail, controllare la cartella della posta indesiderata (spam).

g Fare clic su **Conferma account**. Se l'indirizzo viene verificato, il portale Web si apre.

h Trascinare il file protetto nel portale web e fare clic su **Carica ora**.

i Si riceverà un messaggio di benvenuto dopo aver effettuato la registrazione. Questo messaggio contiene un link per scaricare un client Windows.

> **N.B.:**
> Se il Dell Security Center Hosted è multi-tenant, il messaggio email elenca anche un ID di installazione necessario.

Dell Management Server On-premises

Un server on-premises che si trova all'interno della rete aziendale per la gestione del software Dell Data Security.

> **N.B.:**
> Per un ambiente on-premises è possibile installare Data Guardian prima di effettuare la registrazione. Per eseguire l'attivazione, fare clic sul link **Registra**.

a Quando si apre la finestra Dell Data Guardian, immettere il proprio indirizzo di posta elettronica.

b Fare clic su **Registra**.

c Nella pagina di registrazione, immettere e confermare la password, quindi fare clic su **Accedi**.

Viene visualizzata una finestra di dialogo di conferma della registrazione e viene inviato un messaggio e-mail all'indirizzo immesso dall'utente interno. Se non viene visualizzato il messaggio e-mail, controllare la cartella della posta indesiderata (spam).

d Nel messaggio e-mail di verifica dell'account inviato dal Dell Server, fare clic sul collegamento ipertestuale.

> **N.B.:**
> Se non viene visualizzato un messaggio e-mail, controllare la cartella della posta indesiderata (spam).

e Passare alla pagina Web.

f Nella pagina di conferma, fare clic su **Continua per effettuare l'accesso**.

g Nella pagina di accesso, fare clic su **Password dimenticata**.

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

h 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.

i Aprire il messaggio e-mail di attivazione dell'account e fare clic sul collegamento.

Nel messaggio e-mail è indicato anche il nome del Dell Server da utilizzare durante l'installazione di Data Guardian.

j Nella pagina Accedi, immettere l'indirizzo di posta elettronica e la password usati per registrarsi.

k Fare clic su **Accedi**.

Viene visualizzata una pagina Scarica Data Guardian.

Scaricare e installare Data Guardian for Mobile

Eseguire una delle azioni seguenti:

- Installare o disinstallare Data Guardian su un dispositivo Android
- Installare o disinstallare Data Guardian su un dispositivo iOS

Identifier	**GUID-FE0A7159-E0F3-4E21-9FE6-008C831F7D44**
Status	**Translation Validated**

Utente esterno e portale Web

Attività dell'utente interno

Un utente interno può effettuare una delle seguenti opzioni:

- Inviare all'utente esterno l'URL aziendale per accedere al portale Web di Data Guardian.
- Inviare un file protetto all'utente esterno. Nel momento in cui l'utente apre il file, viene visualizzata una pagina di copertina.

L'utente esterno può visualizzare solo i file .pdf di documento di Office protetto e i file .xen o di modifica sulla base dei criteri impostati. Tuttavia, all'utente esterno non è richiesto di scaricare e installare un client Data Guardian.

Attività dell'utente esterno per il portale Web

Per registrarsi sul portale Web Data Guardian:

1 Fare clic sull'URL del portale Web, ricevuto da un utente interno o riportato sulla pagina di copertina di un file protetto.

2 Nella schermata del contratto di licenza, scorrere in basso e fare clic su **Accetto**.

3 Utilizzare uno di questi metodi, a seconda che l'ambiente sia hosted oppure On-premises.

Dell Security Center Hosted	**Dell Management Server On-premises**
Una soluzione SaaS (Software-as-a-Service) hosted per la gestione del software Dell Data Security.	Un server on-premises che si trova all'interno della rete aziendale per la gestione del software Dell Data Security.
a Immettere un indirizzo email e una password. b Fare clic su **Accedi**. c Immettere indirizzo email, nome, cognome e password. La password deve essere lunga almeno otto caratteri e deve contenere una lettera minuscola, una lettera maiuscola, un carattere speciale e un numero. d Fare clic su **Registra**. e Spostarsi all'indirizzo email utilizzato per la registrazione per recuperare il codice di verifica e immetterlo. f Immettere il codice di verifica e fare clic su **Conferma account**. Viene visualizzato il portale Web.	a b Fare clic su **Non si dispone ancora di un account?** c Immettere un indirizzo e-mail e fare clic su **Registra**. **N.B.:** Per gli utenti interni che desiderano registrarsi come esterni, si tratta di un indirizzo e-mail non di dominio. d Sulla pagina Registra, immettere e confermare la password, quindi fare clic su **Registra**. La pagina Conferma indica che un messaggio e-mail di conferma è stato inviato all'indirizzo e-mail fornito. e Per completare l'attivazione dell'account, aprire il messaggio e-mail intitolato *Verifica dell'account*, quindi fare clic sul collegamento. f Nella schermata di conferma della registrazione, fare clic su **Ritorna alla pagina di accesso**. g Immettere l'indirizzo e-mail e la password utilizzati per registrarsi.

Se un utente interno non dispone della chiave, è possibile accedere al portale web ma non aprire il file.

4 Si apre la pagina di caricamento di Dell Data Guardian.

5 Fare clic su **Sfoglia** per selezionare il file e caricarlo oppure trascinare il file nel portale Web.

6 Fare clic sull'icona **?** per visualizzare la Guida in linea per ogni pagina.

Per modificare i file, l'amministratore deve modificare il criterio per quell'utente. Se l'operazione viene concessa dopo la registrazione, l'utente deve disconnettersi dal portale Web e quindi accedere nuovamente.

È opzionalmente possibile scaricare un client Data Guardian. La pagina di copertina contiene i link per scaricare il client di Data Guardian. Nella pagina di copertina è riportato anche il nome del Dell Server, se il server è di tipo on-premises, o un ID di installazione, se Dell Security Center Hosted è multi-tenant.

Richiesta di accesso da parte di un utente interno

Se si carica un file documento di Office protetto o un file .pdf e la finestra d dialogo *Caricamento non riuscito* indica che l'accesso non è disponibile, è possibile richiedere l'accesso all'autore del file:

1 Nella finestra di dialogo *Caricamento non riuscito* fare clic su **Sì**.
2 Attendere un messaggio email dell'utente interno che informa se l'accesso è stato concesso o negato.

N.B.:
Se non si riceve un messaggio email dall'utente interno, è necessario attendere 48 ore prima di richiedere nuovamente l'accesso. Se si apre il file protetto prima che l'utente interno approvi l'accesso, viene visualizzato un messaggio che indica che la richiesta è in sospeso.

Identifier	**GUID-01B874EC-88D4-4264-803C-472B65D1180F**
Status	**Translation Validated**

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 Dell Server e riaprire il documento protetto.

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

- Stampa
- Esporta
- Salva con nome
- Condividi

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center Hosted e tenant sospeso

Con Dell Security Center Hosted, se un tenant non riesce a effettuare pagamenti per un periodo di tempo specificato, il tenant può essere sospeso. Si applica a Windows, Mac, dispositivi mobili e portale web.

Gli utenti interni ed esterni di Data Guardian possono riscontrare le seguenti condizioni:

- Tutte le piattaforme - Se si tenta di installare Data Guardian, eseguire l'attivazione e l'accesso, viene visualizzata una finestra di dialogo indicante che il tenant è sospeso.
- Mac - Se il tenant è sospeso mentre Data Guardian è aperto, viene visualizzata la relativa finestra di dialogo dopo aver chiuso Esplora file e tutti i file e l'utente tenta di aprire un file protetto.

- Portale web:
  - Se è già stato effettuato l'accesso e si carica un file crittografato, appare il messaggio Caricamento non riuscito.
  - Se un file crittografato o non crittografato è stato caricato e quindi il tenant viene sospeso, appare il messaggio Download non riuscito.
  - Se si esegue la disconnessione e si tenta di accedere nuovamente, appare una finestra di dialogo che indica che il tenant è sospeso.

Contattare l'amministratore.

Identifier	GUID-EF1D5890-EB47-482E-AF29-
Status	In Translation

Aumentare la sicurezza con i Gruppi di accesso di Data Guardian (on-premises)

In Data Guardian i Gruppi di accesso migliorano la sicurezza mediante la creazione di gruppi di utenti che possono collaborare sui dati crittografati. Gli utenti che si trovano all'esterno di un gruppo non possono accedere o visualizzare i dati, a meno che il proprietario del file non conceda l'accesso. I Gruppi di accesso possono includere utenti interni ed esterni. È possibile utilizzare i Gruppi di accesso con Windows, Mac, dispositivi mobili e portale Web.

Selezionare una delle seguenti opzioni a seconda dell'azienda:

- L'azienda ha installato Data Guardian con la modalità Consenso esplicito
- L'azienda ha installato Data Guardian con la modalità Protezione forzata
- L'azienda non ha ancora Data Guardian e la modalità Consenso esplicito
- L'azienda non ha ancora Data Guardian e la modalità Protezione forzata

È inoltre possibile effettuare le seguenti operazioni:

- Cambiare il proprietario di un file crittografato
- Revocare l'accesso a una chiave

Identifier	GUID-F71ADE66-5107-4796-B57E-FC00340C788C
Status	In Translation

L'azienda ha installato Data Guardian con la modalità Consenso esplicito

Se l'azienda utilizza i gruppi di accesso per migliorare la sicurezza dei dati sensibili, è necessario sapere chi sono i componenti del proprio gruppo di accesso. Inizialmente, per assicurare una transizione graduale, l'azienda può concedere un breve periodo per l'elaborazione dei file condivisi e crittografati esistenti. Al termine del periodo di transizione, i componenti del gruppo di accesso possono visualizzare qualsiasi file condiviso e crittografato creato. È possibile concedere l'accesso anche a utenti esterni al proprio gruppo di accesso.

Identificare le persone che si trovano nel proprio gruppo di accesso

L'amministratore dovrà informare l'utente di chi si trova in uno o più gruppi di accesso, a seconda di chi richiede l'accesso a file specifici. I gruppi di accesso possono includere utenti interni ed esterni. Se si lavora su dati sensibili con specifici utenti, si può richiedere che l'amministratore crei un gruppo di accesso per quei contenuti.

Utilizzare un periodo di transizione per elaborare i file condivisi e crittografati

Se Data Guardian è installato e i file esistenti sono crittografati, la best practice per l'azienda prevede un breve periodo di transizione per i file crittografati che vengono condivisi. Per facilitare una transizione graduale, tenere presente quanto segue per i file condivisi e crittografati:

- Il proprietario o autore del file, sia esso interno che esterno, continuerà ad avere accesso al file.
- Gli utenti interni o esterni all'interno del gruppo di accesso avranno accesso alla maggior parte dei file condivisi. In base al tipo di chiave associato ad alcuni file, è possibile che si perda l'accesso ad alcuni.
- Utenti interni all'esterno del gruppo di accesso: gli utenti devono aprire un file condiviso nel periodo di transizione per ottenere l'accesso alla chiave. Se in questo breve periodo non aprono un file condiviso e crittografato, perdono l'accesso al file.
- Utenti esterni non nel gruppo di accesso: se è già stato concesso l'accesso a un file crittografato, l'utente esterno continuerà ad avere accesso durante e dopo il periodo di transizione.

Se si perde l'accesso a un file dopo il periodo di transizione, è possibile richiedere l'accesso al proprietario.

Accedere nuovamente ai file condivisi e crittografati dopo il periodo di transizione

Per Windows e Mac in modalità Consenso esplicito, è possibile effettuare le seguenti operazioni per eseguire nuovamente l'accesso:

- Documenti di Office protetti - Una finestra di dialogo chiede l'accesso a utenti interni ed esterni e il proprietario del file può decidere se concederlo.
- Altri tipi di file crittografati tramite la protezione di base dei file - nessuna richiesta dopo la condivisione. L'utente deve conoscere il proprietario del file e fare clic con il pulsante destro del mouse sul file crittografato per trovare l'ID chiave nella scheda Data Guardian. L'utente può inviare tali informazioni al proprietario e richiedere l'accesso.

Collaborare con i nuovi file crittografati dopo il periodo di transizione

Per i nuovi file che vengono creati e crittografati dopo il periodo di transizione:

- Utenti interni o esterni all'interno del gruppo di accesso: hanno accesso a tutti i file condivisi e crittografati.
  - Chiunque venga rimosso dal gruppo di accesso perde l'accesso.
  - Se il proprietario di un file viene rimosso dal gruppo, gli altri utenti continueranno ad avere l'accesso.
- Utenti interni o esterni all'esterno del gruppo di accesso: non possono visualizzare un file crittografato.
  - Un utente interno all'interno del gruppo di accesso può concedere l'accesso.
  - Se un utente esterno è il proprietario di un file crittografato, può concedere l'accesso a un'altra persona.
  - Se un utente interno o esterno all'esterno del gruppo riceve un documento di Office protetto e tenta di aprirlo, viene visualizzata una finestra di dialogo indicante che è necessario richiedere l'accesso.
  - Se un utente interno o esterno al gruppo riceve e tenta di aprire un tipo di file da Protezione di base dei file, l'utente può fare clic con il pulsante destro del mouse sul file crittografato per trovare l'ID chiave nella scheda Data Guardian e inviare tali informazioni al proprietario.

Identifier	GUID-18DE070B-862D-4CAF-8CDE-DA86552E6C57
Status	In Translation

L'azienda ha installato Data Guardian con la modalità Protezione forzata

Se l'azienda utilizza i gruppi di accesso per migliorare la sicurezza dei dati sensibili, è necessario sapere chi sono i componenti del proprio gruppo di accesso. Inizialmente, per assicurare una transizione graduale, l'azienda può concedere un breve periodo per l'elaborazione dei file condivisi e crittografati esistenti. Al termine del periodo di transizione, i componenti del gruppo di accesso possono visualizzare qualsiasi file condiviso e crittografato creato. È possibile concedere l'accesso anche a utenti esterni al proprio gruppo di accesso.

Identificare le persone che si trovano nel proprio gruppo di accesso

L'amministratore dovrà informare l'utente di chi si trova in uno o più gruppi di accesso, a seconda di chi richiede l'accesso a file specifici. I gruppi di accesso possono includere utenti interni ed esterni. Se si lavora su dati sensibili con specifici utenti, si può richiedere che l'amministratore crei un gruppo di accesso per quei contenuti.

Utilizzare un periodo di transizione per elaborare i file condivisi e crittografati

Se Data Guardian è installato e i file esistenti sono crittografati, la best practice per l'azienda prevede un breve periodo di transizione per i file crittografati che vengono condivisi. Per facilitare una transizione graduale, tenere presente quanto segue per i file condivisi e crittografati:

- Il proprietario o autore del file, sia esso interno che esterno, continuerà ad avere accesso al file.
- Gli utenti interni o esterni all'interno del gruppo di accesso avranno accesso alla maggior parte dei file condivisi. In base al tipo di chiave associato ad alcuni file, è possibile che si perda l'accesso ad alcuni.
- Utenti interni all'esterno del gruppo di accesso: gli utenti devono aprire un file condiviso nel periodo di transizione per ottenere l'accesso alla chiave. Se in questo breve periodo non aprono un file condiviso e crittografato, perdono l'accesso al file.
- Utenti esterni non nel gruppo di accesso: se è già stato concesso l'accesso a un file crittografato, l'utente esterno continuerà ad avere accesso dopo il periodo di transizione.

Se si perde l'accesso a un file dopo il periodo di transizione, è possibile richiedere l'accesso al proprietario.

Accedere nuovamente ai file condivisi e crittografati dopo il periodo di transizione

Per Windows e Mac, in modalità Protezione forzata, è possibile effettuare le operazioni riportate di seguito per ripristinare l'accesso:

- Documenti di Office protetti - Una finestra di dialogo chiede l'accesso a utenti interni ed esterni e il proprietario del file può decidere se concederlo.
- Altri tipi di file crittografati tramite la protezione di base dei file - nessuna richiesta dopo la condivisione. L'utente deve conoscere il proprietario del file e fare clic con il pulsante destro del mouse sul file crittografato per trovare l'ID chiave nella scheda Data Guardian. L'utente può inviare tali informazioni al proprietario e richiedere l'accesso.

Collaborare con i file creati dopo il periodo di transizione

Per i nuovi file che vengono creati e crittografati dopo il periodo di transizione:

- Utenti interni o esterni all'interno del gruppo di accesso: hanno accesso a tutti i file condivisi e crittografati.
  - Chiunque venga rimosso dal gruppo di accesso perde l'accesso.
  - Se il proprietario di un file viene rimosso dal gruppo, gli altri utenti continueranno ad avere l'accesso.
- Utenti interni o esterni all'esterno del gruppo di accesso: non possono visualizzare un file crittografato.
  - Un utente interno all'interno del gruppo di accesso può concedere l'accesso.
  - Se un utente esterno è il proprietario di un file crittografato, può concedere l'accesso a un'altra persona.
  - Se un utente interno o esterno all'esterno del gruppo riceve un file crittografato e tenta di aprirlo, viene visualizzata una finestra di dialogo indicante che è necessario richiedere l'accesso.

Identifier	**GUID-BDD3EF46-A9A1-48C2-BB76-B9D874BC37E4**
Status	**In Translation**

L'azienda non ha ancora Data Guardian e la modalità Consenso esplicito

Se l'azienda ha intenzione di utilizzare Data Guardian con i gruppi di accesso per migliorare la sicurezza dei dati sensibili, la best practice prevede di identificare i file che si condividono con utenti interni o esterni e scoprire se tali utenti saranno in qualsiasi gruppo di accesso creato per l'utente dall'amministratore. Inizialmente, per assicurare una transizione graduale, l'azienda può concedere un breve periodo per l'elaborazione dei file condivisi esistenti. Al termine del periodo di transizione, i componenti del gruppo di accesso possono visualizzare qualsiasi file condiviso e crittografato creato. È possibile concedere l'accesso a persone all'esterno del proprio gruppo di accesso in modo che sia possibile collaborare con loro, ma con una maggiore sicurezza.

Identificare le persone che si trovano nel proprio gruppo di accesso

L'amministratore dovrà informare l'utente di chi si trova in uno o più gruppi di accesso, a seconda di chi richiede l'accesso a file specifici. I gruppi di accesso possono includere utenti interni ed esterni. Se si lavora su dati sensibili con specifici utenti, si può richiedere che l'amministratore crei un gruppo di accesso per quei contenuti.

Utilizzare un periodo di transizione per elaborare i file condivisi

Quando Data Guardian è installato, viene eseguita una scansione su Windows o Mac e vengono crittografati i seguenti file, se l'amministratore ha attivato una policy per tali file.

- Altri tipi di file, come i file .txt o .png, configurati per la Protezione di base dei file
- File di classificazione dei dati (Windows)
- File di classificazione TITUS (Windows)

Se già si collabora su file o essi vengono condivisi con utenti interni o esterni, tali utenti possono far parte o meno del gruppo di accesso. La best practice per un passaggio graduale prevede un breve periodo di transizione per elaborare questi file crittografati che vengono condivisi con altri utenti. È necessario accedere al computer durante questo periodo di transizione.

Tenere presente quanto riportato di seguito se si desidera continuare la condivisione o la collaborazione su questi file:

- Per i file condivisi riportati sopra, la proprietà viene attribuita al primo utente che accede e il cui computer viene sottoposto a ricerca.

- Se un'altra persona diventa proprietario del file e l'autore originale non è nel suo gruppo di accesso, il proprietario originale deve richiedere l'accesso al nuovo proprietario. Il proprietario originale può anche richiedere che l'amministratore modifichi la proprietà.
- I 'computer degli utenti esterni non vengono sottoposti a ricerca, quindi i file condivisi non protetti non vengono ricercati e crittografati.
- Se la Crittografia cloud di Data Guardian è attivata e gli utenti condividono cartelle o file su un provider di cloud storage, verranno ricercati anche questi file.

Collaborare con i file creati dopo il periodo di transizione

Per i nuovi file che vengono creati e crittografati dopo il periodo di transizione:

- Utenti interni o esterni all'interno del gruppo di accesso: hanno accesso a tutti i file condivisi e crittografati.
  - Chiunque venga rimosso dal gruppo di accesso perde l'accesso.
  - Se il proprietario di un file viene rimosso dal gruppo, gli altri utenti continueranno ad avere l'accesso.
- Utenti interni o esterni all'esterno del gruppo di accesso: non possono visualizzare un file crittografato.
  - Un utente interno all'interno del gruppo di accesso può concedere l'accesso.
  - Se un utente esterno è il proprietario di un file crittografato, può concedere l'accesso a un'altra persona.
  - Se un utente interno o esterno all'esterno del gruppo riceve un file crittografato e tenta di aprirlo, viene visualizzata una finestra di dialogo indicante che è necessario richiedere l'accesso.

Identifier	**GUID-16B7D77E-57D2-47D9-B2CC-39DB65B223E2**
Status	**In Translation**

L'azienda non ha ancora Data Guardian e la modalità Protezione forzata

Se l'azienda ha intenzione di utilizzare Data Guardian con i gruppi di accesso per migliorare la sicurezza dei dati sensibili, la best practice prevede di identificare i file che si condividono con utenti interni o esterni e scoprire se tali utenti saranno in qualsiasi gruppo di accesso creato per l'utente dall'amministratore. Inizialmente, per assicurare una transizione graduale, l'azienda può concedere un breve periodo per l'elaborazione dei file condivisi esistenti. Al termine del periodo di transizione, i componenti del gruppo di accesso possono visualizzare qualsiasi file condiviso e crittografato creato. È possibile concedere l'accesso a persone all'esterno del proprio gruppo di accesso in modo che sia possibile collaborare con loro, ma con una maggiore sicurezza.

Identificare le persone che si trovano nel proprio gruppo di accesso

L'amministratore dovrà informare l'utente di chi si trova in uno o più gruppi di accesso, a seconda di chi richiede l'accesso a file specifici. I gruppi di accesso possono includere utenti interni ed esterni. Se si lavora su dati sensibili con specifici utenti, si può richiedere che l'amministratore crei un gruppo di accesso per quei contenuti.

Utilizzare un periodo di transizione per elaborare i file condivisi

Quando Data Guardian è installato, viene eseguita una scansione su Windows o Mac e vengono crittografati i seguenti file, se l'amministratore ha attivato una policy per tali file.

- Documenti Office
- PDF
- Altri tipi di file, come i file .txt o .png, configurati per la Protezione di base dei file

La best practice per un passaggio graduale prevede un breve periodo di transizione per elaborare questi file crittografati che vengono condivisi con altri utenti. È necessario accedere al computer durante questo periodo di transizione.

Tenere presente quanto riportato di seguito se si desidera continuare la condivisione o la collaborazione su questi file:

- Per i file condivisi riportati sopra, la proprietà viene attribuita al primo utente che accede e il cui computer viene sottoposto a ricerca.
- Se un'altra persona diventa proprietario del file e l'autore originale non è nel suo gruppo di accesso, il proprietario originale deve richiedere l'accesso al nuovo proprietario. Il proprietario originale può anche richiedere che l'amministratore modifichi la proprietà.
- I 'computer degli utenti esterni non vengono sottoposti a ricerca, quindi i file condivisi non protetti non vengono ricercati e crittografati.
- Se la Crittografia cloud di Data Guardian è attivata e gli utenti condividono cartelle o file su un provider di cloud storage, verranno ricercati anche questi file.

Collaborare con i file creati dopo il periodo di transizione

Per i nuovi file che vengono creati e crittografati dopo il periodo di transizione:

- Utenti interni o esterni all'interno del gruppo di accesso: hanno accesso a tutti i file condivisi e crittografati.
  - Chiunque venga rimosso dal gruppo di accesso perde l'accesso.
  - Se il proprietario di un file viene rimosso dal gruppo, gli altri utenti continueranno ad avere l'accesso.
- Utenti interni o esterni all'esterno del gruppo di accesso: non possono visualizzare un file crittografato.
  - Un utente interno all'interno del gruppo di accesso può concedere l'accesso.
  - Se un utente esterno è il proprietario di un file crittografato, può concedere l'accesso a un'altra persona.
  - Se un utente interno o esterno all'esterno del gruppo riceve un file crittografato e tenta di aprirlo, viene visualizzata una finestra di dialogo indicante che è necessario richiedere l'accesso.

Identifier	**GUID-2627974A-3D0D-4075-81BC-86DFD31CF90B**
Status	**Translated**

Cambiare il proprietario di un file crittografato

Durante il periodo di transizione per i gruppi di accesso, è possibile richiedere all'amministratore la proprietà di un file crittografato e condiviso di cui si è autore originale se questa è stata attribuita a un altro utente.

Identifier	**GUID-0ED28BBC-3A7C-48F3-A1AE-A5039C39C392**
Status	**In Translation**

Revocare l'accesso a una chiave

Se si concede l'accesso di un file crittografato a un utente esterno, l'utente ha la chiave per aprire il file.

Facoltativamente, se non si desidera più che l'utente esterno abbia accesso al file, è possibile chiedere all'amministratore di revocare la chiave. Ciò si applica solo agli utenti esterni.

Identifier	**GUID-8B76A529-19A6-4107-983B-707F5AB1D09C**
Status	**In Translation**

Precondividere file protetti su Windows

È necessario che sia installato Data Guardian, assegnato a uno o più gruppi di accesso.
Se un utente interno o esterno non si trova nel gruppo di accesso, è possibile precondividere un file protetto.

1 Fare clic con il pulsante destro del mouse su un file protetto e selezionare **Accesso ai file protetti**.

Nell'interfaccia utente di *Condivisione accesso a file protetti*, il nome del documento viene visualizzato in File selezionato.

2 In *Indirizzo e-mail per la condivisione*, fare clic su **Aggiungi** e inserire un indirizzo e-mail valido per un utente esterno o un utente interno che non si trovi nel proprio gruppo di accesso.

È possibile aggiungere fino a dieci singoli indirizzi alla volta.

3 Per modificare un indirizzo e-mail, fare clic su **Modifica**.

4 Per eliminare un indirizzo e-mail, selezionare una voce e fare clic su **Elimina**.

> **N.B.:**
> Viene indicato il nome del proprietario del file e non può essere selezionato o eliminato.

5 I gruppi di accesso vengono visualizzati in Gruppi disponibili. Selezionare uno o più gruppi e utilizzare le frecce da aggiungere ai *Gruppi condivisi*.

6 Fare clic su **OK**. Viene visualizzato il messaggio di completamento dell'operazione.

> **N.B.:**
> Gli utenti esterni non possono condividere il documento protetto con un altro utente esterno.

Se è la prima volta che un utente esterno riceve un file protetto di Data Guardian, l'utente deve installare Data Guardian o utilizzare il portale Web per visualizzare il file protetto.

Identifier	**GUID-C67795A0-FA20-4E32-9A2B-89654D67DFB2**
Status	**In Translation**

Precondividere file protetti su Mac

È necessario che sia installato Data Guardian, assegnato a uno o più gruppi di accesso.
Se un utente interno o esterno non si trova nel gruppo di accesso, è possibile precondividere un file protetto.

1 Fare clic con il pulsante destro del mouse su un file protetto e selezionare **Accesso ai file protetti**.

Nell'interfaccia utente di *Condivisione accesso a file protetti*, il nome del documento viene visualizzato in File selezionato.

2 In *Indirizzo e-mail per la condivisione*, fare clic su **Aggiungi** e inserire un indirizzo e-mail valido per un utente esterno o un utente interno che non si trovi nel proprio gruppo di accesso.

È possibile aggiungere fino a dieci singoli indirizzi alla volta.

3 Per eliminare un indirizzo e-mail, selezionare una voce e fare clic su **Elimina**.

> **N.B.:**
> Viene indicato il nome del proprietario del file e non può essere selezionato o eliminato.

4 I gruppi di accesso vengono visualizzati in Gruppi disponibili. Selezionare uno o più gruppi e utilizzare le frecce da aggiungere ai *Gruppi condivisi*.

5 Fare clic su **OK**. Viene visualizzato il messaggio di completamento dell'operazione.

> **N.B.:**
> Gli utenti esterni non possono condividere il documento protetto con un altro utente esterno.

Se è la prima volta che un utente esterno riceve un file protetto di Data Guardian, l'utente deve installare Data Guardian o utilizzare il portale Web per visualizzare il file protetto.

Identifier	GUID-FAF997A4-8E8E-4DCB-BA76-575F951F0799
Status	In Translation

Precondividere file protetti su iOS o Android

Se un utente interno o esterno non si trova nel gruppo di accesso, è possibile precondividere un file protetto.

1 Toccare un file protetto.

2

N.B.:

Nella scheda *Utenti*, il nome del proprietario del file viene visualizzato, ma non può essere selezionato o eliminato. Se il file è stato già condiviso con utenti interni o esterni, tali nomi vengono visualizzati.

3 Nella scheda *Utenti*, per aggiungere l'indirizzo e-mail di un utente esterno o di un utente interno che non si trova nel proprio gruppo di accesso, fare clic sull'icona più (+) in basso a destra.

4 Per eliminare un indirizzo e-mail, scorrere e toccare **Elimina**.

5 Toccare la scheda **Gruppi** per visualizzare i propri gruppi di accesso.

6 Toccare un gruppo per condividere un file protetto.

N.B.:

Un segno di spunta indica un gruppo con il quale si sceglie di condividere il file protetto.

7 In alto a destra, toccare **Condividi**.

Viene visualizzato il messaggio di completamento dell'operazione. Gli utenti esterni non possono condividere il documento protetto con un altro utente esterno.

Se è la prima volta che un utente esterno riceve un file protetto di Data Guardian, l'utente deve installare Data Guardian o utilizzare il portale Web per visualizzare il file protetto.

Identifier	GUID-455BE40E-83D4-4C42-890C-18067EE3CFD5
Status	In Translation

Precondividere file protetti sul portale Web

Se un utente interno o esterno non si trova nel gruppo di accesso, è possibile precondividere un file protetto.

1 Caricare un documento protetto sul portale web.

Se l'amministratore ha aggiunto l'utente a uno o più gruppi di accesso, viene visualizzata l'icona *Accesso a file protetto* accanto all'icona Download.

2 Fare clic sull'icona **Accesso a file protetto**.

Nell'interfaccia utente di *Condivisione accesso a file protetti*, il nome del documento viene visualizzato in File selezionato.

3 In *Indirizzo e-mail per la condivisione*, fare clic su **Aggiungi nuovo**.

4 Inserire un indirizzo e-mail valido per un utente esterno o un utente interno che non si trovi nel gruppo di accesso e fare clic sul segno di spunta per salvarlo. È possibile aggiungere fino a dieci singoli indirizzi alla volta.

N.B.:

Per eliminare un indirizzo e-mail, fare clic su **X**. Il nome della persona che condivide il documento è evidenziato e non può essere selezionato o eliminato.

5 I gruppi di accesso vengono visualizzati in Gruppi disponibili. Fare clic su **Seleziona tutto** oppure sull'icona a forma di freccia accanto a un'opzione per aggiungerla ai *Gruppi condivisi* o rimuoverla.

6 Fare clic su **OK**.

N.B.:
Gli utenti esterni non possono condividere il documento protetto con un altro utente esterno.

Se è la prima volta che un utente esterno riceve un file protetto di Data Guardian, l'utente deve installare il portale Web.

Identifier	**GUID-5BE95524-98D7-476C-9790-CA2298568418**
Status	**In Translation**

Precondividere file protetti come utente esterno

È necessario che sia installato Data Guardian, assegnato a uno o più gruppi di accesso.
Se si è l'autore o il proprietario di un file protetto, è possibile precondividere il file con un utente interno. Non è possibile condividere il documento protetto con un altro utente esterno. Se non si è proprietari del file, non è possibile condividerlo.

- L'*Indirizzo e-mail per la condivisione* non elenca i nomi degli altri utenti con cui è stato condiviso il documento protetto.
- Nessun gruppo viene visualizzato in Gruppi disponibili. È possibile condividere solo con singoli utenti.

1 Fare clic con il pulsante destro del mouse su un file protetto e selezionare **Accesso ai file protetti**.
Nell'interfaccia utente di *Condivisione accesso a file protetti*, il nome del documento viene visualizzato in File selezionato.
2 In *Indirizzo e-mail per la condivisione*, fare clic su **Aggiungi** e inserire un indirizzo e-mail valido per un utente esterno o un utente interno che non si trovi nel proprio gruppo di accesso.
È possibile aggiungere fino a dieci singoli indirizzi alla volta.
3 Per modificare un indirizzo e-mail, fare clic su **Modifica**.
4 Per eliminare un indirizzo e-mail, selezionare una voce e fare clic su **Elimina**.

N.B.:
In quanto proprietario del file, non è possibile selezionare o eliminare il proprio nome.

5 Fare clic su **OK**. Viene visualizzato il messaggio di completamento dell'operazione.

Se è la prima volta che un utente riceve un file protetto di Data Guardian, l'utente deve installare Data Guardian o utilizzare il portale Web per visualizzare il file protetto.

Identifier	**GUID-F97CE528-0A49-4763-80D0-0F5937EAE934**
Status	**In Translation**

Modificare chi ha accesso alle e-mail protette

In base al criterio impostato dall'amministratore, è possibile fare clic con il pulsante destro del mouse su un'e-mail protetta e inviata agli utenti nel proprio gruppo di accesso. È possibile modificare chi ha accesso a quella e-mail.

1 In Outlook, fare clic con il pulsante destro del mouse su un'e-mail con etichetta [PROTETTO].
2 In basso, selezionare **Accesso e-mail protetta**.
Viene visualizzato un elenco di utenti con cui è stato condiviso l'accesso.
3 Rimuovere i singoli utenti se non si desidera più che abbiano accesso all'e-mail protetta.

Identifier	GUID-F553E0C3-FCF3-4782-8FD4-
Status	Translation Validated

FAQ - Domande frequenti

Identifier	GUID-D70F8E30-C205-474A-BC17-DB3867AE07AE
Status	In Translation

FAQ varie

Domanda

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

Soluzione

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

Identifier	GUID-36E78894-7902-4034-8BFA-6D63A1743855
Status	Translation Validated

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**.