

# Installazione del plug-in Cisco Email Security con file di configurazione personalizzati

## Sommario

[Introduzione](#)

[Installazione del plug-in Cisco Email Security con file di configurazione personalizzati](#)

[Installare il plug-in Cisco Email Security](#)

[Costruire una directory di configurazione personalizzata](#)

[Modificare il file CommonComponentsConfig.xml](#)

[Distribuire i file di configurazione personalizzati](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritto il processo per utilizzare i file di configurazione personalizzati per installare il plug-in Cisco Email Security.

## Installazione del plug-in Cisco Email Security con file di configurazione personalizzati

### Installare il plug-in Cisco Email Security

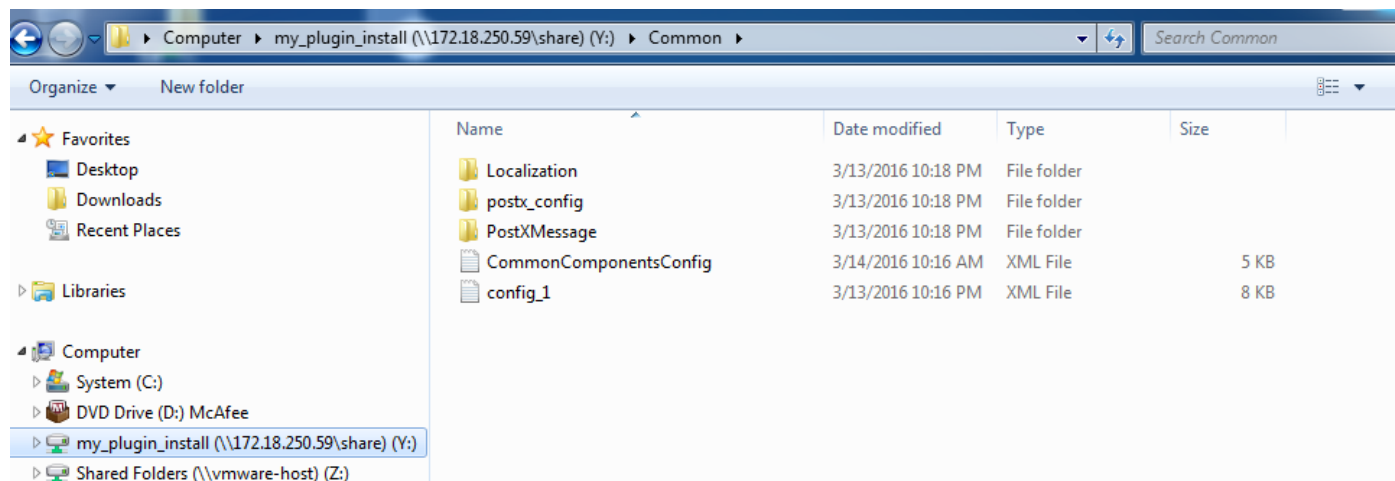
1. Scaricare e installare la versione più recente del plug-in. (i file da [scaricare](#) sono disponibili nella pagina dei prodotti).
2. Installare il plug-in tramite l'installazione standard. Per ulteriori informazioni, vedere [il Manuale dell'amministratore del plug-in Cisco Email Security](#).
3. Caricare il file di configurazione XML firmato di Business Class Email (BCE).
4. Verificare che il plug-in funzioni come previsto per la crittografia. In questo modo è possibile garantire configurazioni personalizzate all'XML BCE per la decrittografia/contrassegno/crittografia, nonché ulteriori configurazioni personalizzate per l'XML CommonComponentsConfiguration.

### Costruire una directory di configurazione personalizzata

1. Su un host Windows o un server di rete, creare una directory di installazione personalizzata. (Per questo esempio, utilizzando una condivisione di rete:  
\\172.18.250.59\share\installazione\_plug\_in\_utente)
2. Nell'host Windows, passare alla directory di installazione standard:  
C:\ProgramData\Cisco\Cisco IronPort Email Security Plug-In\
3. Copiare la directory 'Common' dalla directory di installazione standard alla directory di installazione personalizzata.
4. Nell'host Windows, dalla directory di installazione standard, aprire la directory *user\_id*:  
C:\ProgramData\Cisco\Cisco IronPort Email Security Plug-In\*<user\_id>*

5. Copiare i file *config\_1.xml* e *CommonComponentsConfig.xml* esistenti nella directory di installazione personalizzata, nella directory 'Common'.
6. Dalla directory di installazione personalizzata, eliminare i file *used\_configs.bin* e *cachedFolders.xml* nella directory 'Common' creata per l'installazione personalizzata, se presente.

A questo punto, la struttura della directory di installazione personalizzata dovrebbe essere simile alla seguente:



## Modificare il file CommonComponentsConfig.xml

Modificare il file CommonComponentsConfig.xml in modo che sia indipendente dall'utente, consentendo a qualsiasi utente di caricare la configurazione nel proprio profilo di Outlook.

1. Utilizzando un editor di testo dalla directory di installazione personalizzata, modificare il file CommonComponentsConfig.xml nella directory 'Common' che viene creata per l'installazione personalizzata.

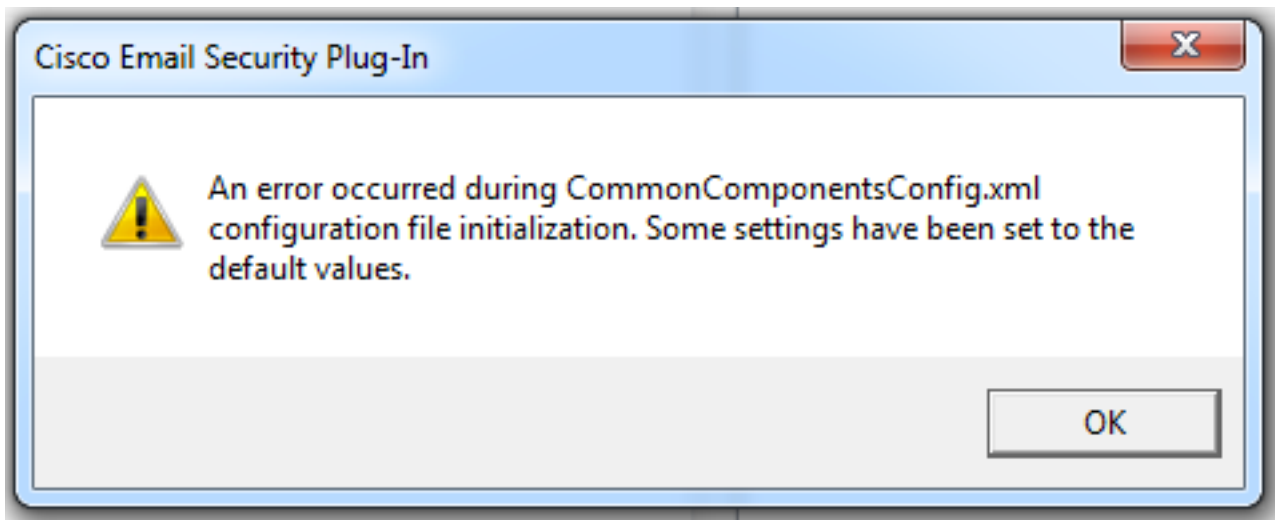
2. Trovare il tag *accountFileNames*:

```
<accountFileNames>
<accountFileName filePath="config_1.xml" emailAddressAndKeyServer="user@domain.com
res.cisco.com" defaultReportAccount="true" defaultEncryptAccount="true" profileName="[Cisco
Enterprise Exchange]" />
</accountFileNames>
```

3. Modificare la sezione *accountFileNames*, rimuovendo le voci *emailAddress* e *profileName* preesistenti:

```
<accountFileNames>
<accountFileName filePath="config_1.xml" emailAddressAndKeyServer="*"
defaultReportAccount="true" defaultEncryptAccount="true" />
</accountFileNames>
```

**Nota:** Verificare che la sintassi *accountFileName* sia formattata correttamente. Se la riga di configurazione *accountFileName* non è corretta, Outlook imposterà il plug-in sui valori predefiniti e lo contrassegnerà come Inattivo per i componenti aggiuntivi di Outlook:



## Distribuire i file di configurazione personalizzati

Disinstalla l'installazione standard del plug-in eseguita dall'inizio di questo articolo. Questa operazione può essere eseguita mediante la normale disinstallazione da Windows: **Pannello di controllo > Programmi e funzionalità > Plug-in Cisco Email Security**, quindi selezionare **Disinstalla/Cambia**. Completare i passaggi come richiesto.

A questo punto, i file di configurazione personalizzati sono pronti per l'installazione. Dalla CLI di Windows, eseguire la sintassi seguente per installare:

```
Cisco Email Security Plugin.exe /exenoui /qn UseCustomConfig="\\{SHARED_DIR}\{CONFIG_FOLDER}"
```

Dove la directory che segue "=" specifica la directory dei file di configurazione personalizzati.

Altri parametri di switch utilizzati durante l'installazione con estensione exe:

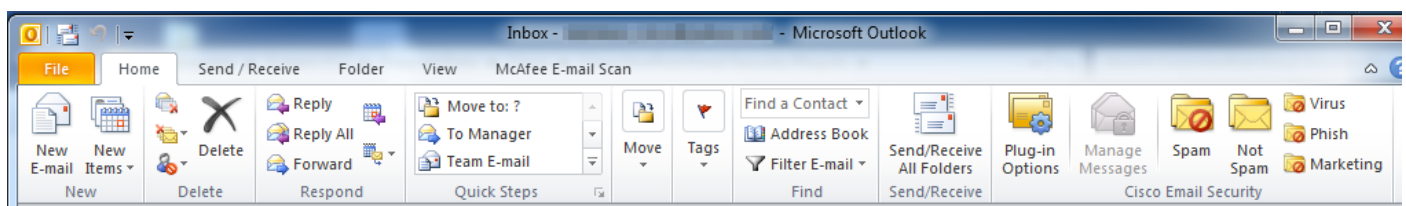
### Switch Descrizione

/exenoui Avvia l'installazione EXE senza interfaccia utente  
/qn q, qn - nessuna interfaccia utente

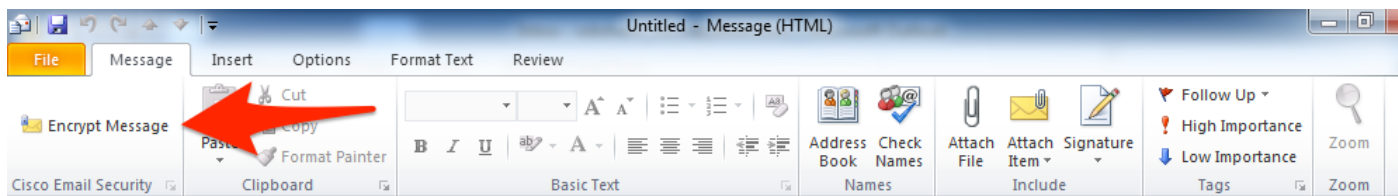
Continuando con l'esempio costruito sopra, usando quanto segue:

```
C:\>CiscoEmailSecurity-7-5-2-009.exe /exenoui /qn  
UseCustomConfig="\\172.18.250.59\share\my_plugin_install"
```

L'installazione richiede in genere circa 30 secondi. Al termine dell'installazione, dopo l'apertura di Outlook l'installazione del prodotto finale nella barra multifunzione di Outlook sarà simile a:



Nel campo *New E-mail* (Nuovo messaggio), evidenziare l'opzione *Encryption* (Crittografia) e tenerla pronta per l'uso:



L'opzione di crittografia verrà impostata in base alla configurazione originale di BCE XML:

```
<!--  
Plugin related configuration. Valid type edition values are:  
decrypt - Plugin can only decrypt PXE envelopes.  
flag - Plugin can decrypt and flag a message for encryption.  
encrypt - Plugin can decrypt and encrypt a message on the device.  
-->  
<plugin edition="flag">
```

## Risoluzione dei problemi

- *UseCustomConfig* deve essere in lettere maiuscole corrette e non plurale. *UseCustomConfigs* non funzionerà e causerà la lettura non corretta della configurazione di Outlook.
- Non terminare il comando di installazione della configurazione personalizzata che fa riferimento alla directory del file di configurazione personalizzata con "\".
- Per consentire all'utente finale che esegue Outlook di leggere/scrivere i file, è necessario che per la directory e i file di configurazione personalizzati siano impostate le autorizzazioni appropriate. In caso contrario, è possibile che la configurazione non venga letta correttamente e che all'utente finale vengano visualizzati errori durante l'avvio di Outlook.
- Esaminare il file *CiscoEmailSecurity.log* nella directory dell'utente finale per ulteriori dettagli sugli errori generati e associarlo all'operazione del plug-in:

```
C:\ProgramData\Cisco\Cisco IronPort Email Security Plug-In\<>user_id>\CiscoEmailSecurity.log
```