

Rimozione privilegi amministrativi / Administrative privileges removal

De Group Information Security Office <Security@eng.it>

Data Qua, 27/08/2025 13:06

Cc Group Information Office <GroupCIO@eng.it>; Group Information Security Office <Security@eng.it>



Aggiornamento modalità operative

Gentile Collega,

ti comunichiamo che, in ottemperanza al piano di **potenziamento della postura di cybersecurity** del Gruppo, è in corso un processo per la **revoca**, da tutte le postazioni di lavoro Windows, **dei privilegi di amministratori locali** e per l'**inibizione dell'utilizzo dei dispositivi di mass storage USB** (pendrive e altri supporti di archiviazione esterna diversi da stampanti, scanner, hub, etc.).

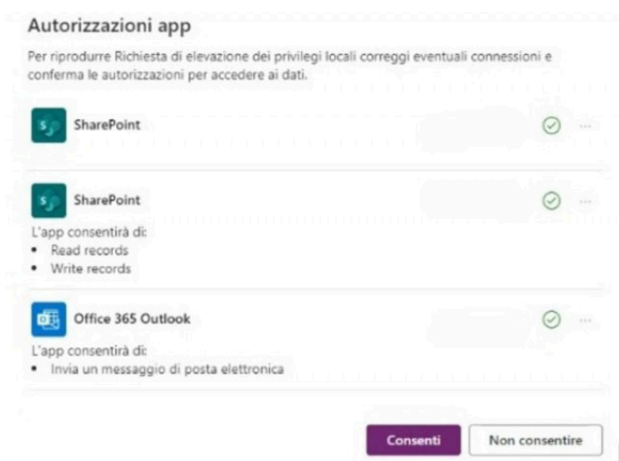
Questa è una misura imprescindibile per salvaguardare i dati sensibili e le risorse informatiche da potenziali aggressioni o sottrazioni. Le aziende che adottano questo tipo di soluzioni riducono significativamente il rischio di incidenti di sicurezza e si conformano alle normative vigenti, come la DORA (Directive on Operational Resilience for the Financial Sector) e la NIS2 (Directive on Security of Network and Information Systems).

Tale processo è in corso per gruppi di utenti che vengono avvisati per e-mail prima della rimozione.

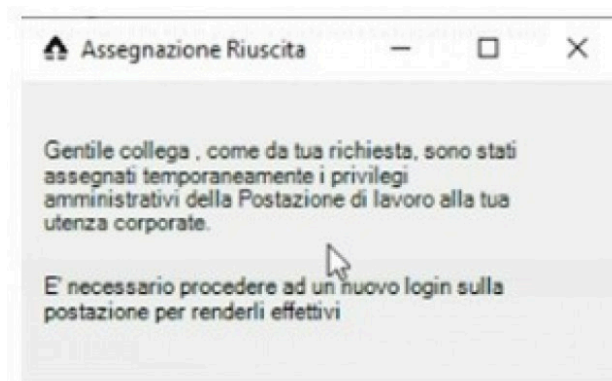
Per le postazioni di lavoro Windows dei neoassunti e per quelle che vanno a sostituire quelle obsolete le restrizioni saranno già attive al momento della consegna dell'asset.

Se per comprovate esigenze lavorative hai bisogno di installare software, cambiare le configurazioni del PC o attivare una porta USB per usare una pendrive, dovrai seguire il processo di **richiesta di deroga tramite Form** - vedi banner in calce.

Al primo utilizzo del Form sarà necessario, attraverso il tasto “Consenti”, approvare i permessi di accesso alla propria utenza corporate (vedi immagine a lato).



Una volta compilato il form dovrai attendere la comparsa di questo pop-up:



Dopo la comparsa del pop-up e il conseguente riavvio della postazione la tua utenza avrà un profilo amministrativo per il tempo indicato nella compilazione del form.

Novità

Potrai richiedere l’abilitazione per la password amministrativa con tempistiche diverse in base alla motivazione della richiesta:

- **password amministrativa da 2 a 4 ore** – verrà assegnata d’ufficio
- **password amministrativa da 5 a 10 ore** – verrà assegnata d’ufficio e notificata al responsabile
- **password amministrativa da 2 a 5 giorni** – verrà sottoposta ad approvazione del responsabile e processata solo a seguito di ricevuta approvazione.

Resta invariata la durata della validità dell’autorizzazione per l’accesso ai dispositivi di mass storage:

- **USB:** il giorno della richiesta (disabilitazione alle 2:00 AM)

Tutte le richieste verranno centralmente loggate per eventuali audit successivi.

Con il nuovo rilascio non sarà quindi necessario contattare il Service Desk in quanto l’elevazione temporanea dei diritti amministrativi è stata completamente automatizzata.

In caso di estrema urgenza o indisponibilità del Form, potrai contattare il Service Desk via e-mail servicedesk_internalit@eng.it o tramite telefono +39 0125 853 080, avendo cura di informare della richiesta la tua/il tuo responsabile che potrà essere contattata/o per verifiche.

Per maggiori dettagli visita la [pagina su Engage](#).

EPM - Microsoft Intune Endpoint Privilege Management

Ricordiamo che nel caso di **utilizzi frequenti** è possibile utilizzare il tool **EPM** che permette di avviare eseguibili .exe con privilegi elevati, utilizzando il tasto destro del mouse e specificando la motivazione dell'esigenza in una casella a testo libero.

Riportiamo per comodità il link a Engage dove è possibile reperire il [Manuale EPM](#).

Se EPM non è attivo nella postazione di lavoro (assenza della voce "Esecuzione con accesso con privilegi elevati" visibile con il tasto destro del mouse su un file .exe), è necessario richiederne licenza tramite RdA secondo la procedura standard descritta [QUI](#).

Grazie per la collaborazione

Group Information Security Office
Group Information Office

FORM: Richiesta di elevazione temporanea dei privilegi locali

Operating Mode Update

Dear Colleague,

we inform you that, in compliance with the plan to **strengthen the Group's cybersecurity posture**, a process is underway for the **revocation**, from all Windows workstations, **of the privileges of local administrators** and for the **inhibition of the use of USB mass storage devices** (pendrives and other external storage media other than printers, scanners, hubs, etc.).

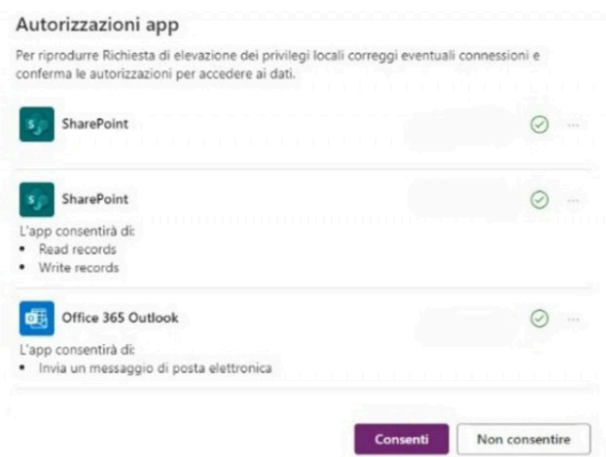
This is an essential measure to safeguard sensitive data and IT assets from potential aggression or theft. Companies that adopt this type of solution significantly reduce the risk of security incidents and comply with current regulations, such as DORA (Directive on Operational Resilience for the Financial Sector) and NIS2 (Directive on Security of Network and Information Systems).

This process is ongoing for groups of users who are notified by email before removal.

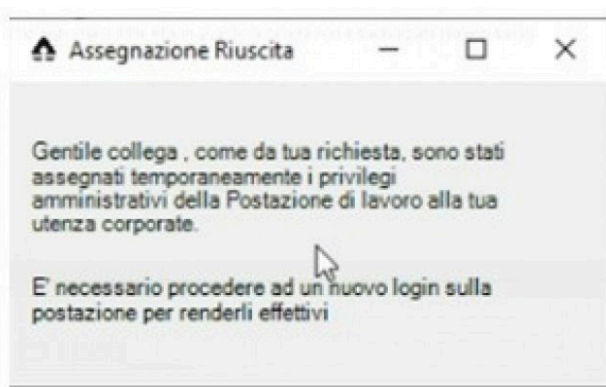
For the Windows workstations of new hires and those that replace the obsolete ones, the restrictions will already be in place at the time of delivery of the asset.

If for proven work needs you need to install software, change PC configurations or activate a USB port to use a pendrive, you will have to follow the **exemption request process using the form** - see banner below.

On first use of the form, you will need to approve access permissions to your corporate account by clicking the “Allow” button (see image on the side).



Once you have filled out the form, you will have to wait for this pop-up:



After the pop-up appears and the subsequent restart of the workstation, your user will have an administrative profile for the period of time requested in the form.

What's New

You can now request administrative password access for different durations, depending on the reason for your request:

- **Administrative password for 2 to 4 hours** – automatically granted
- **Administrative password for 5 to 10 hours** – automatically granted and notified to your manager
- **Administrative password for 2 to 5 days** – subject to your manager’s approval and processed only after approval is received.

The duration for USB mass storage devices access remains unchanged:

- **USB access:** granted on the day of the request, with deactivation scheduled at **2:00 AM**.

All requests will be centrally logged for possible future audits.

With this new release, **there is no need to contact the Service Desk**, as the temporary elevation of administrative rights is now fully automated.

In cases of extreme urgency or unavailability of the form, you may contact the Service Desk by email at servicedesk_internalit@eng.it or by phone at **+39 0125 853 080**. Please ensure your manager is informed of the request, as they may be contacted for verification.

For more details, visit the relevant [page on Engage](#).

EPM – Microsoft Intune Endpoint Privilege Management

For **frequent needs**, we remind you that you can use the **EPM** tool. It allows you to run .exe executables with elevated privileges by right-clicking and entering the reason in a free-text field.

For your convenience, here is the [EPM Manual](#) on Engage.

If EPM is not active on your workstation (i.e. the “**Run with elevated access**” option is missing when right-clicking a .exe file), you need to request a license via a Purchase Request (RdA), following the standard procedure described [HERE](#).

Thank you for your cooperation

Group Information Security Office
Group Information Office

FORM: Request for temporary elevation of local privileges

© ENGINEERING - All Rights Reserved