

Esercizio_S9_L5_WinServer_2022

Consegna

Lo scopo di questo esercizio è di familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022.

Preparazione:

- ☐ Accedi al tuo ambiente Windows Server 2022.
- ☐ Assicurati di avere i permessi amministrativi necessari per creare e gestire gruppi.

Creazione dei Gruppi:

- ☐ Crea due gruppi distinti. Puoi scegliere i nomi che preferisci per questi gruppi, ma assicurati che i nomi siano significativi per riflettere la loro funzione o ruolo all'interno dell'organizzazione (ad esempio, "Amministratori", "UtentiStandard", "MarketingTeam", "Sviluppatori", ecc.).

Assegnazione dei Permessi:

- ☐ Per ogni gruppo, assegna permessi specifici.

Puoi scegliere quali permessi concedere, ma assicurati di considerare i seguenti aspetti:

- Accesso ai file e alle cartelle.
- Esecuzione di programmi specifici.
- Modifiche alle impostazioni di sistema.
- Accesso remoto al server.

- ☐ Documenta i permessi assegnati a ciascun gruppo, spiegando perché hai scelto tali permessi.

Verifica:

- ☐ Una volta creati i gruppi e assegnati i permessi, verifica che le impostazioni siano corrette. Puoi farlo:
 - Creando utenti di prova e aggiungendoli ai gruppi.
 - Verificando che gli utenti abbiano i permessi assegnati in base al proprio gruppo.

Documentazione:

○ Scrivi un breve report che includa:

- I nomi dei gruppi creati.
- I permessi assegnati a ciascun gruppo.
- I passaggi seguiti per creare e configurare i gruppi.
- Eventuali problemi riscontrati e come li hai risolti.

Svolgimento

Per lo svolgimento di questo progetto ho deciso di creare “ex novo” un server da utilizzare per simulare quello di un’azienda di servizi IT fittizia chiamata SecureIT.

Alla creazione del dominio seguirà poi la creazione di gruppi dei vari dipartimenti:

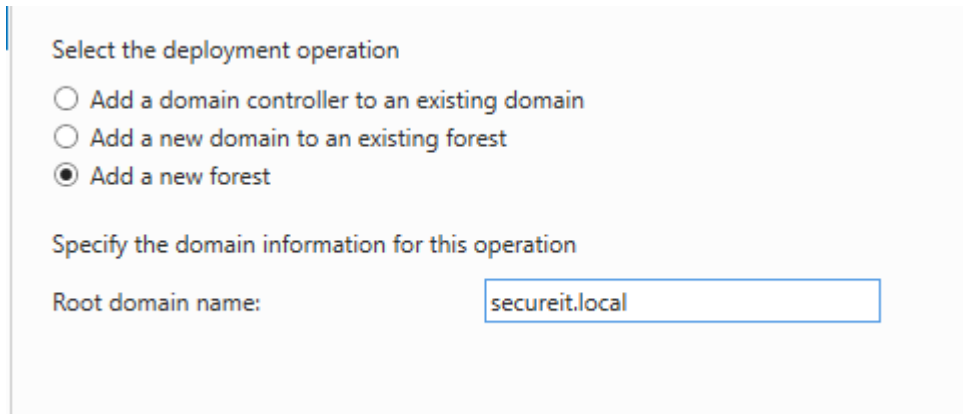
- HelpDesk
- RicercaSicurezza
- Amministrazione
- Sviluppo
- Sales
- HR (Risorse Umane)
- Marketing

Ogni dipartimento avrà i suoi users e i permessi verranno personalizzati sulla base dei ruoli all’interno dell’azienda RBAC.

Verranno infine scritte alcune regole GPO per gestire in maniera più sicura l’intera infrastruttura.

Creazione Server

Tutto comincia ovviamente con la creazione di un nuovo dominio denominato **secureit.local**:



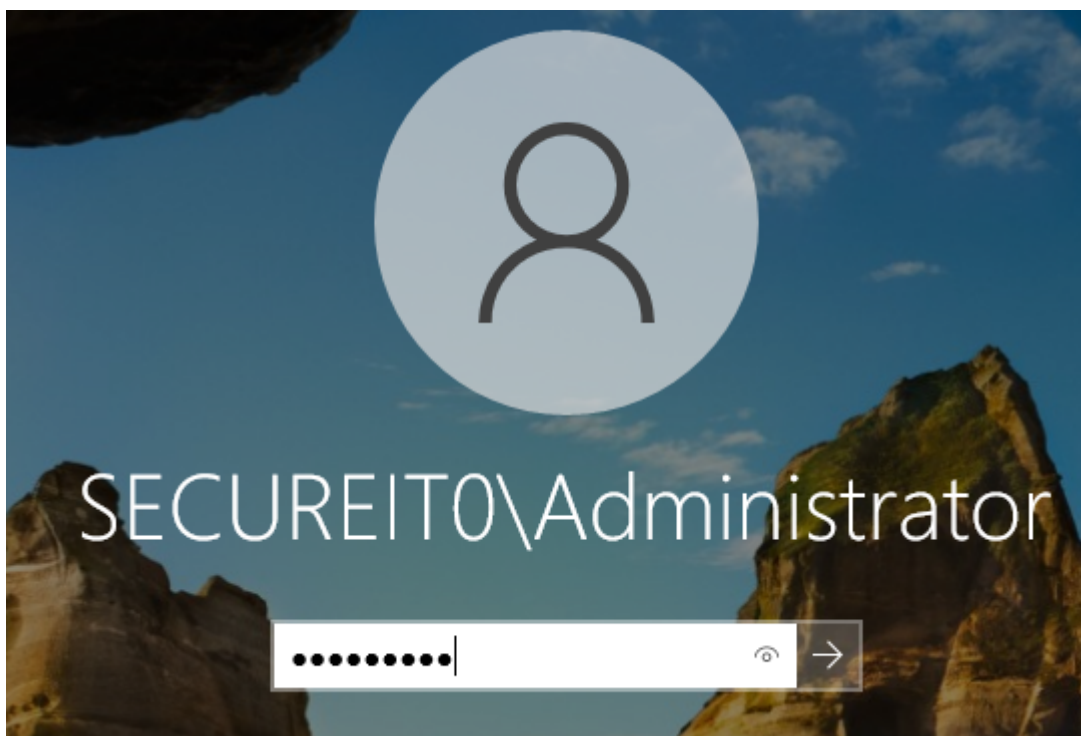
Select the deployment operation

- ☐ Add a domain controller to an existing domain
- ☐ Add a new domain to an existing forest
- ☒ Add a new forest

Specify the domain information for this operation

Root domain name:

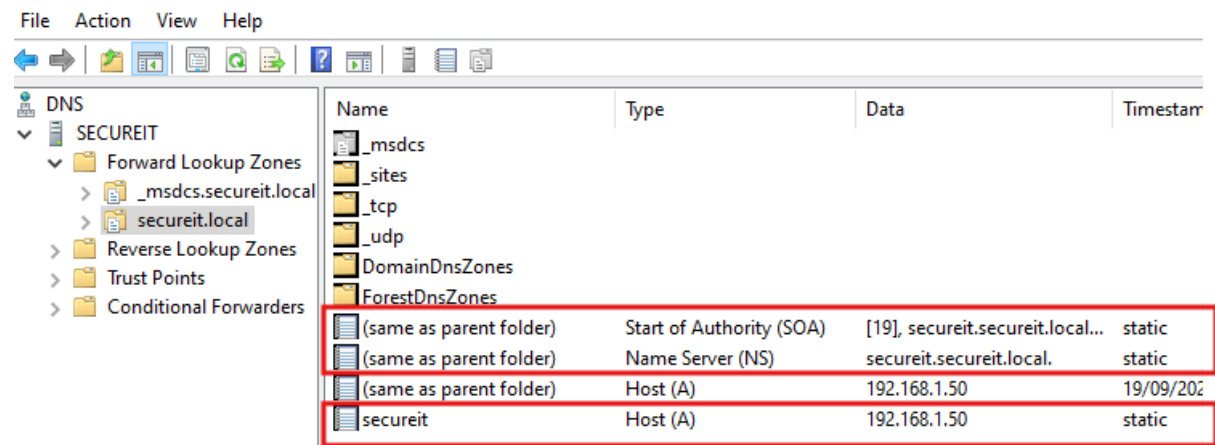
Una volta impostato correttamente possiamo accedervi grazie alle credenziali scelte al momento della registrazione:



Creazione Server DNS

Un altro passo generalmente importante da effettuare è quello di configurare il server DNS tramite [Tools → DNS → SecureIT → Forward Lookup Zones → secureit.local](#)

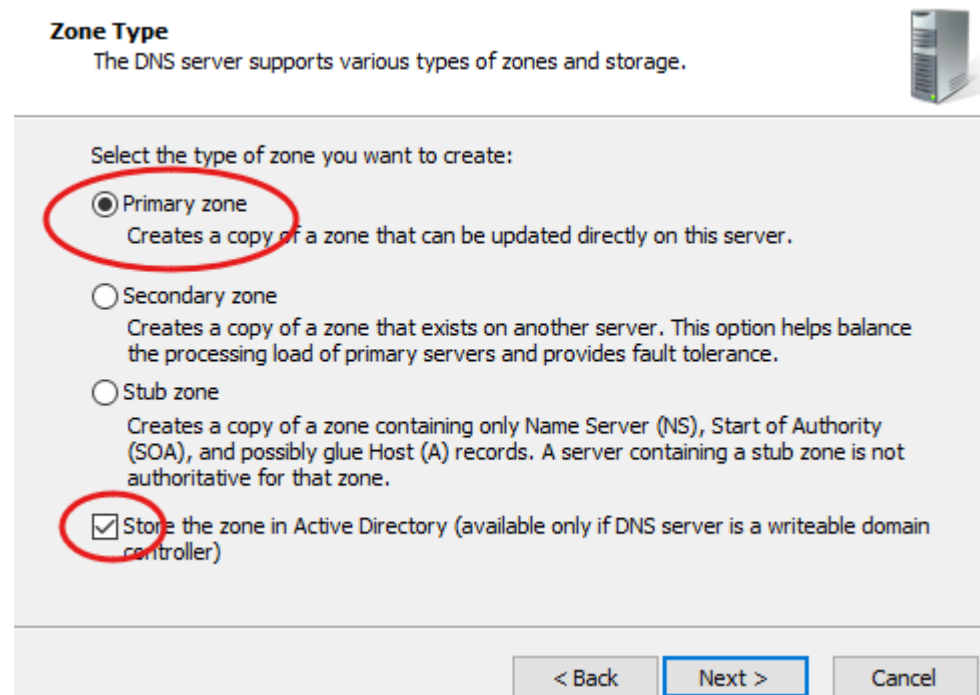
Giunti a questo punto è necessario assicurarsi che il Domain Lookup sia settato correttamente nei campi **SOA, NS ed Host**:



Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[19], secureit.secureit.local...	static
(same as parent folder)	Name Server (NS)	secureit.secureit.local.	static
(same as parent folder)	Host (A)	192.168.1.50	19/09/202
secureit	Host (A)	192.168.1.50	static

Va poi considerata la configurazione anche del Reverse Lookup tramite [Tools → DNS → SecureIT → Reverse Lookup Zones](#)

Va dunque premuto su **Add New Zone** e selezionata l'opzione **Primary Zone** assieme al flag in **Store the zone in Active Directory**.



Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

- ☒ **Primary zone**
Creates a copy of a zone that can be updated directly on this server.
- ☐ **Secondary zone**
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- ☐ **Stub zone**
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☒ **Store the zone in Active Directory** (available only if DNS server is a writeable domain controller)

< Back **Next >** Cancel

Nel passaggio successivo lasciamo **to all DNS server running on domain controllers in this domain: secureit.local**

☒ To all DNS servers running on domain controllers in this domain: secureit.local

E nella fattispecie scegliamo di configurare il Reverse di un IPV4:

Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.



Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

☒ IPv4 Reverse Lookup Zone

☐ IPv6 Reverse Lookup Zone

Avendo l'ip impostato in statico su **192.168.1.50**, l'ip di rete da inserire sarà dunque **192.168.1**

Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.



To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ Network ID:

192 .168 .1

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ Reverse lookup zone name:

1.168.192.in-addr.arpa

< Back

Next >

Cancel


Impostiamo poi l'opzione più sicura tra le disponibili ovvero **Allow only secure dynamic updates**:

Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.


Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

- ☒ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
- ☐ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.
- ☐ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back Next > Cancel

Next → Finish

File Action View Help				
				
DNS				
SECUREIT				
Forward Lookup Zones				
_msdcn.secureit.local				
secureit.local				
Reverse Lookup Zones				
1.168.192.in-addr.arpa				

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[1], secureit.secureit.local,...	static
(same as parent folder)	Name Server (NS)	secureit.secureit.local.	static

A quel punto possiamo creare un nuovo record contenente l'indirizzo IP del dominio locale - in questo caso 192.168.1.50 - e denominare l'hostname:

New Resource Record

Pointer (PTR)

Host IP Address: 192.168.1.50

Fully qualified domain name (FQDN): 50.1.168.192.in-addr.arpa

Host name: secureit.secureit.local

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel

Effettuato tutto questo non resta che testare tramite un tool come cmd o powershell l'effettivo lavoro svolto:

`nslookup 192.168.1.50`

```
C:\Users\Administrator\EPICODESERVER>nslookup 192.168.1.50
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:     secureit.secureit.local
Address:  192.168.1.50
```

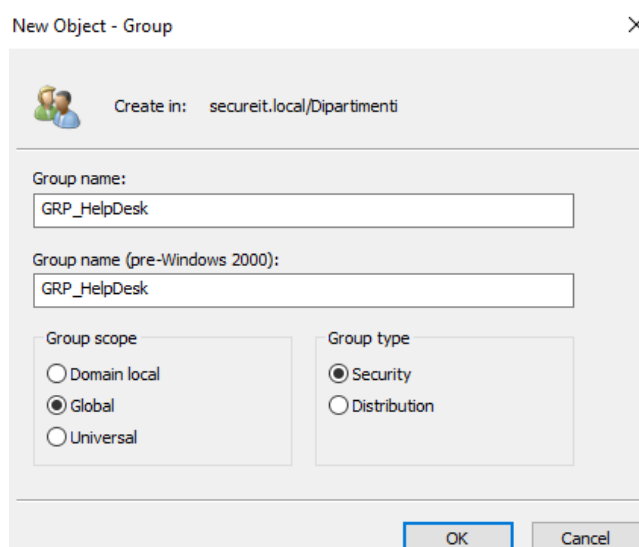
L'esito è chiaro, il DNS ha tradotto l'ip nel nome **secureit.secureit.local** confermando la validità del lavoro svolto in precedenza.

Creazione dei gruppi

Una volta settato il DNS si può procedere a strutturare i vari gruppi dell'azienda tramite [Tools → Active Directory Users and Computers](#)

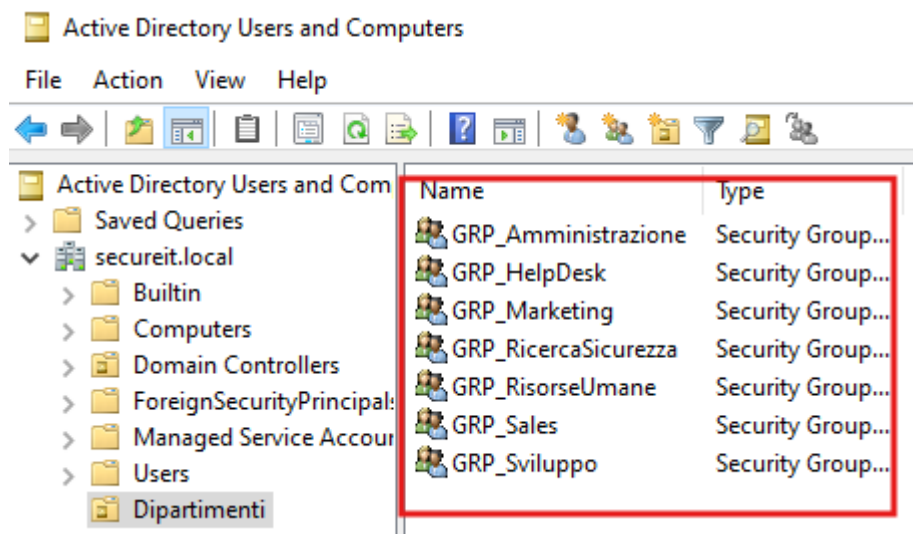
Al suo interno possiamo creare un'**Organizational Unit** attraverso [secureit.local → New → Organizational Unit](#) in modo da tenere tutto ordinato e compartimentato. In questo caso denominiamo la nuova OU **Dipartimenti**

Procedendo poi tramite [Dipartimenti → New → Group](#) possiamo effettivamente procedere alla creazione dei vari gruppi:



E' prassi comune utilizzare un prefisso come "GRP_" prima del nome del gruppo per distinguerli a colpo d'occhio da altri oggetti di tipo Users.

Una volta creato l'ultimo gruppo l'intera lista dovrebbe essere disponibile all'interno della sezione di destra:



Creazione Directories

Come base di partenza per l'azienda SecureIT ho pensato di realizzare la struttura qui di seguito:

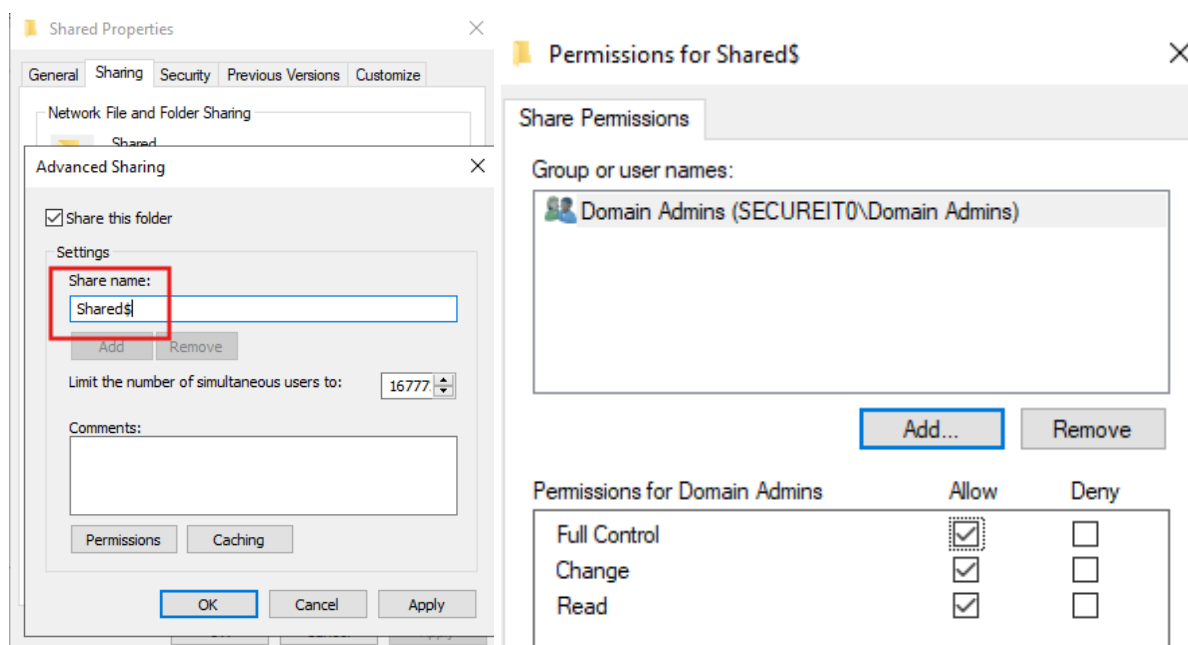
```
C:\Shared\  
├── HelpDesk  
│   ├── Procedure  
│   └── Ticket  
├── Risorse Umane  
│   ├── Personale  
│   └── DocumentiConfidenziali  
├── Marketing  
│   ├── Campagne  
│   └── Grafica  
├── Sales  
│   ├── Contratti  
│   └── Clienti  
├── Amministrazione  
│   ├── Bilanci  
│   └── Fatture  
├── Sviluppo  
│   ├── Codice  
│   └── Documentazione  
└── RicercaSicurezza  
    ├── Report  
    └── Tools
```


Condivisione della cartella root

La cartella **Shared** è stata condivisa in rete tramite **Advanced Sharing**, utilizzando il nome di condivisione **Shared\$**.

Il simbolo **\$** rende la cartella invisibile nella navigazione, ma accessibile conoscendo il percorso UNC (**\\secureit\\Shared\$**).

Nella scheda **Permissions** della condivisione sono stati rimossi i permessi predefiniti, mantenendo solo l'accesso amministrativo. Il controllo effettivo degli accessi viene demandato ai **permessi NTFS** delle sottocartelle.



Assegnazione dei permessi NTFS

Per ogni sottocartella è stato **rimosso** il gruppo **Everyone** e sono stati aggiunti solo i gruppi di sicurezza corrispondenti.

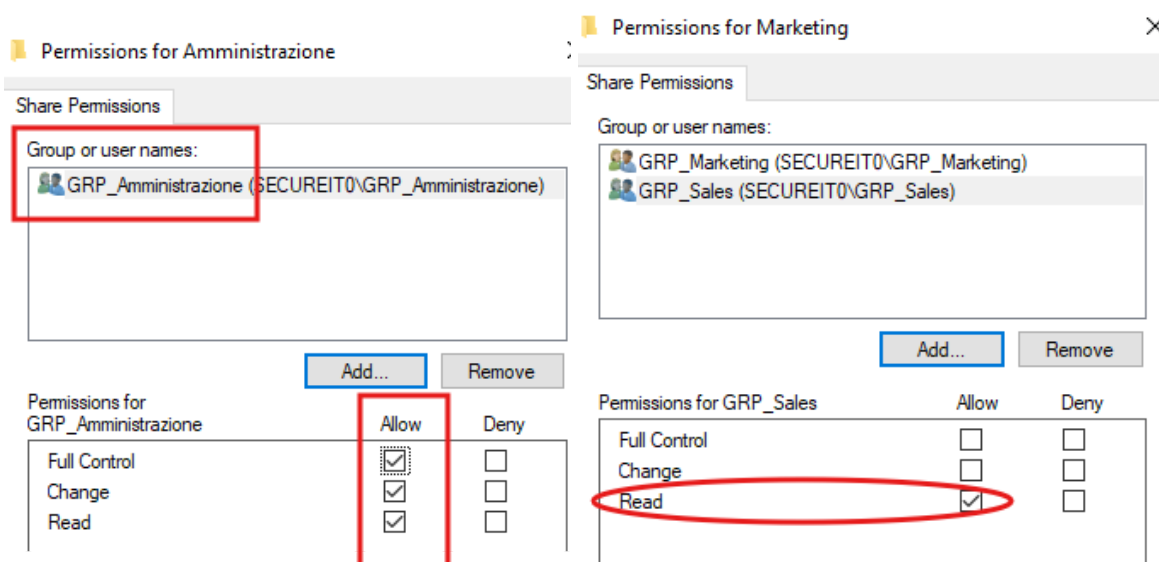
Inoltre, il gruppo **Domain Admins** mantiene sempre **Full Control** su tutta la root **C:\Shared** e relative sottocartelle, per garantire la gestione amministrativa.

Sulla root **C:\Shared** è stato mantenuto per tutti i gruppi un livello minimo di accesso, in modo da permettere la navigazione fino alla cartella di competenza senza esporre il contenuto delle altre directory.

Eccezioni applicate

L'unica eccezione alle regole qui sopra è data dalla directory **Marketing** che è stata resa leggibile anche al gruppo **GRP_Sales**, per permettere al reparto commerciale di accedere ai materiali promozionali.

Nessun altro gruppo può accedere a risorse non destinate al proprio reparto.



Creazione Utenti

Dopo aver creato un ulteriore **Group Organisation**, all'interno del nostro dominio, denominata **UtentiSecureIT** è possibile generare al suo interno altri sotto-container al cui interno inserire gli utenti da associare ai relativi gruppi.

La scelta della **naming convention** dipende dalla dimensione dell'azienda: nei contesti enterprise si usano spesso codici numerici per reparti, mentre nelle PMI è più comune utilizzare convenzioni leggibili come nome.cognome o iniziale+cognome. In ogni caso, è fondamentale mantenere coerenza e documentazione.

Per garantire ordine e scalabilità nella gestione, è stata adottata una convenzione di denominazione basata su codici numerici legati al reparto di appartenenza. Nello specifico, ogni utente assume un identificativo nella forma **UT + codice reparto + numero progressivo** (ad esempio UT100, UT101, UT200). Questa scelta, tipica di realtà aziendali medio-grandi, consente di riconoscere immediatamente l'area di competenza di ciascun account e riduce il rischio di ambiguità rispetto a convenzioni basate esclusivamente su nome e cognome.

Una volta creato i vari sotto-containers ho provveduto ad inserire al loro interno uno user di prova che seguisse la regola sopra riportata:

<i>Amministrazione</i>	→	<i>UT100</i>	<i>Mario Rossi</i>
<i>HelpDesk</i>	→	<i>UT200</i>	<i>Elena Gialli</i>
<i>Sales</i>	→	<i>UT300</i>	<i>Anna Verdi</i>
<i>RicercaSicurezza</i>	→	<i>UT400</i>	<i>Massimo Neri</i>
<i>Sviluppo</i>	→	<i>UT500</i>	<i>Andrea Grigio</i>
<i>Marketing</i>	→	<i>UT600</i>	<i>Maria Rosa</i>
<i>RisorseUmane</i>	→	<i>UT700</i>	<i>Giorgio Bianchi</i>

Nei campi FirstName e LastName verranno comunque inseriti i dati identificativi dell'utente a cui è stato assegnato l'account:

New Object - User ×

Create in: secureit.local/UtentiSecureIT/Amministrazione

First name: Initials:

Last name:

Full name:

User logon name:

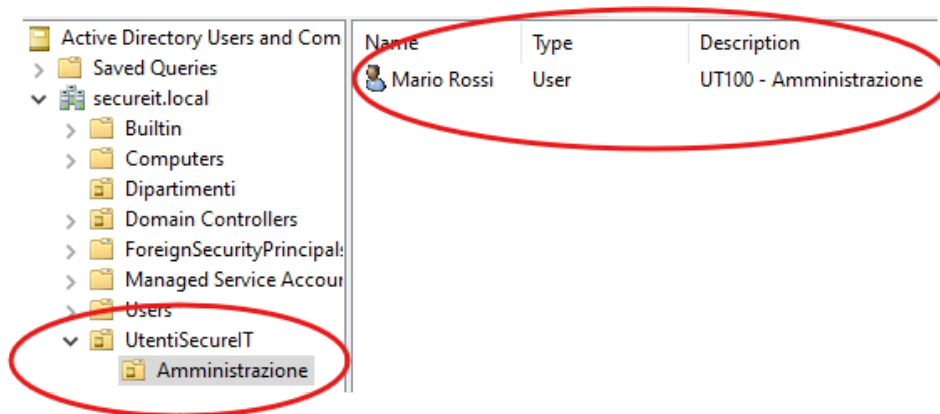
User logon name (pre-Windows 2000):

< Back **Next >** Cancel

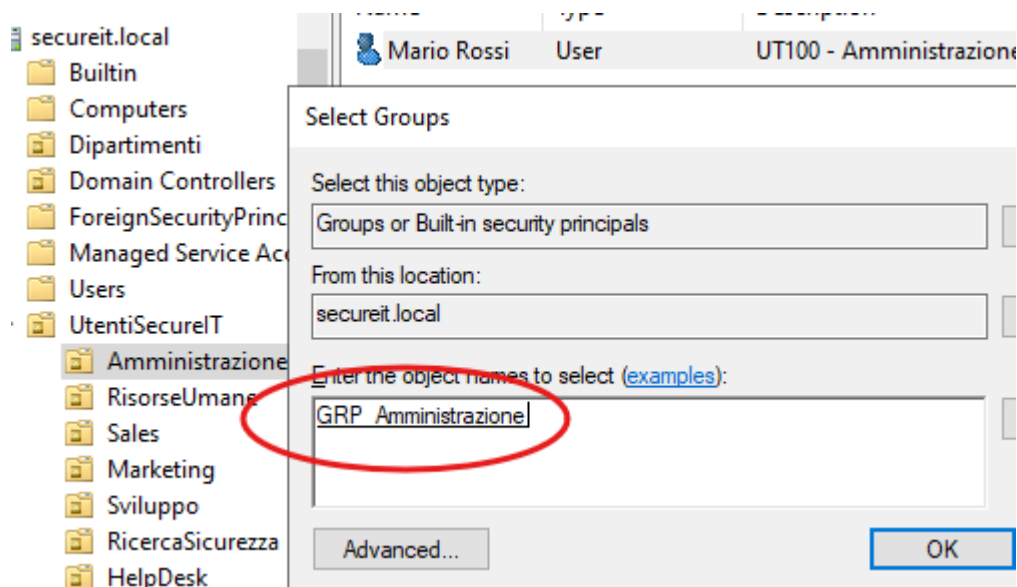
E' buona norma che la password non sia conosciuta da nessun'altro all'infuori dell'assegnatario dell'account, ho così flaggato l'opzione per il cambio di password in concomitanza con il primo login.

☒ User must change password at next login

Infine ho aggiunto una descrizione esplicativa contenente il numero di account ed il relativo reparto in modo da avere tutto disponibile a colpo d'occhio:



Una volta creati gli users, per collegarli al relativo, gruppo è sufficiente effettuarvi un click destro sopra → add to group e digitare il nome del gruppo a cui aggiungerlo.



Configurazione Client

Per poter ora accedere con uno degli account creati è necessario configurare un'altra macchina affinché si ritrovi sulla stessa rete del server ed abbia i giusti parametri DNS.

A quel punto è possibile, all'interno del menù per la modifica del nome del dispositivo, andare a specificare di che dominio è membro il computer che stiamo configurando; nel nostro caso dovremmo attribuirlo come parte del dominio secureit.local.

Modifica impostazioni IP

Manuale

IPv4

Attivato

Indirizzo IP

192.168.1.100

Lunghezza prefisso subnet

24

Gateway

192.168.1.1

DNS preferito

192.168.1.50

Cambiamenti dominio/nome computer

È possibile modificare il nome e l'appartenenza del computer. Le modifiche potrebbero compromettere l'accesso alle risorse di rete.

Nome computer:

PC1

Nome completo computer:

PC1

Altro...

Membro di

☒ Dominio:

secureit.local

☐ Gruppo di lavoro:

WORKGROUP

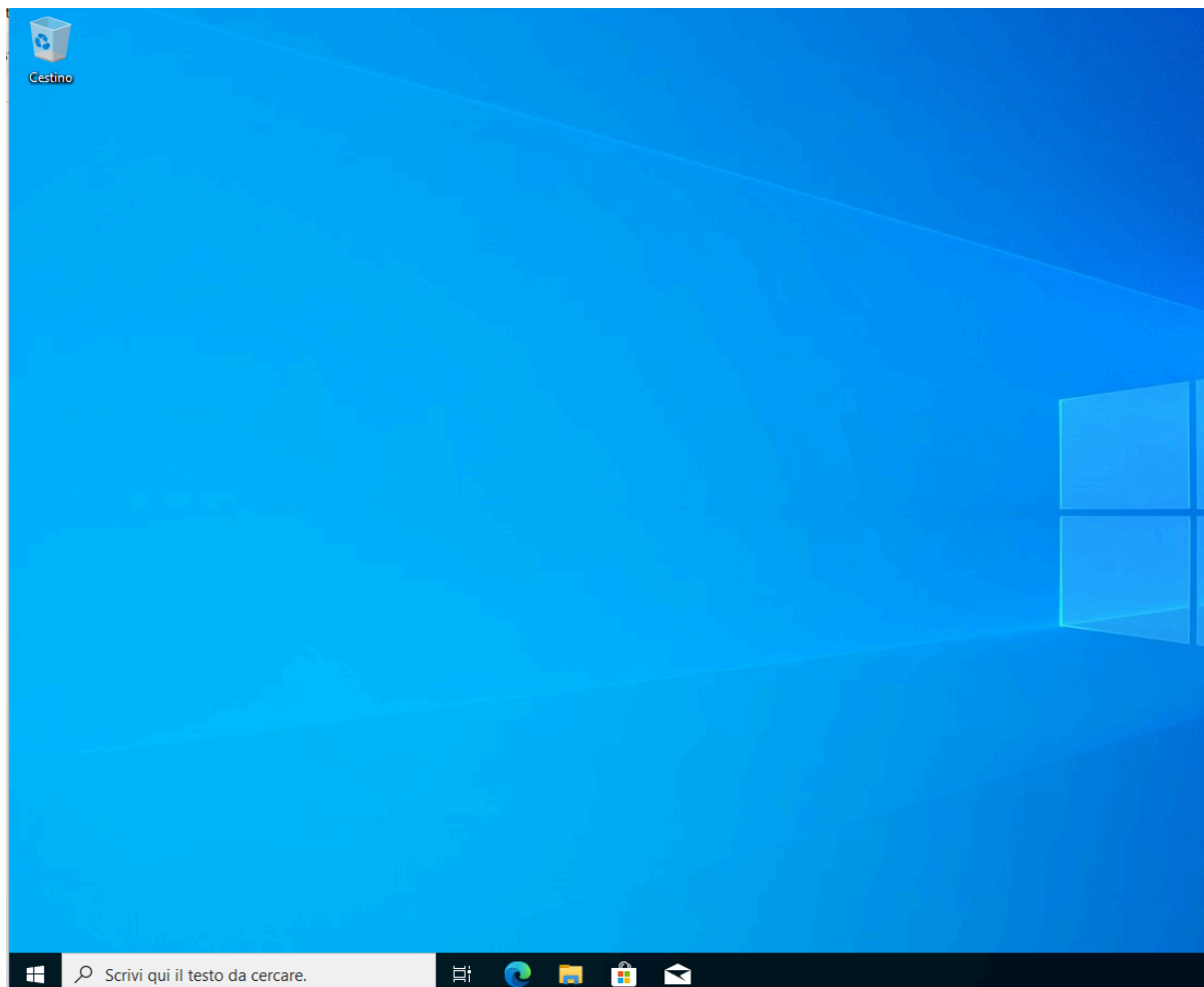
OK

Annulla

Una volta fatto ciò il pc verrà riavviato consentendoci di utilizzare le credenziali create in precedenza per accedere con uno degli utenti generati.

Una volta loggati una nuova istanza verrà generata e l'utente avrà a disposizione una postazione di lavoro operativa secondo le regole impostate sul server:

È in corso la preparazione del computer



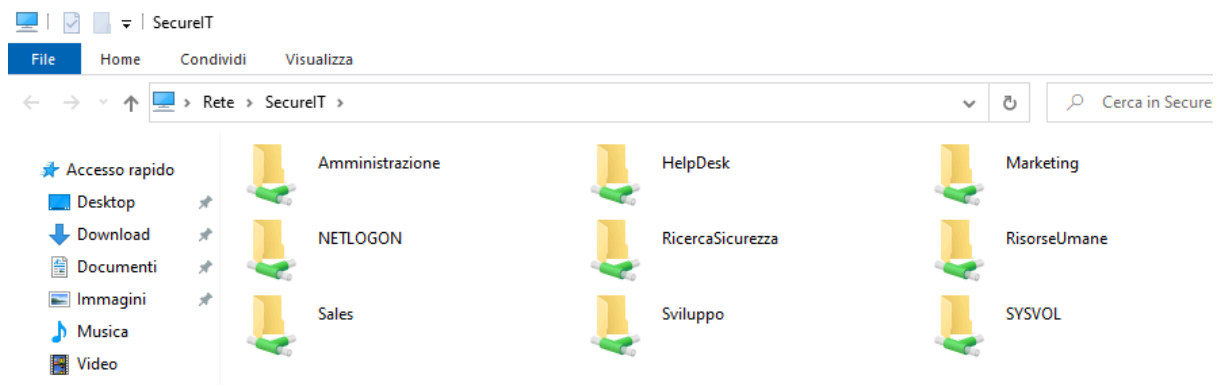
Un'ultima cosa utile da fare prima di accedere con un utente Server è quella di attivare i due servizi responsabili dell'individuazione delle risorse di rete cambiandone l'avvio da Manuale a Automatico (Ritardato)::

- Function Discovery Provider Host
- Function Discovery Resource Publication

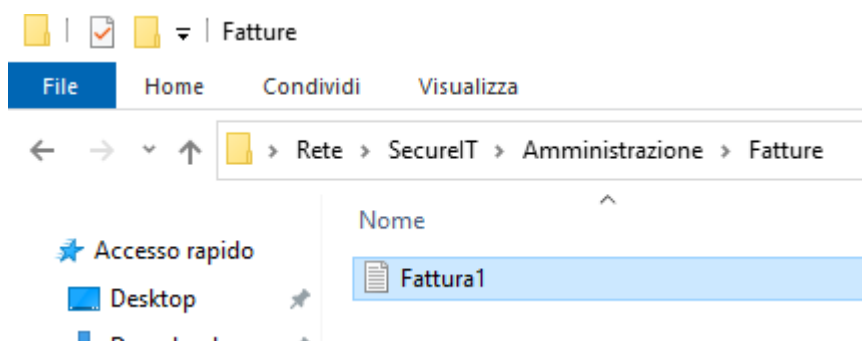
 Host provider di individuazione funzioni	Il servizio F...	Manuale	Servizio locale
 Pubblicazione risorse per individuazione	Pubblica qu...	Manuale (avv...	Servizio locale

Verifica NTFS

Come primo account ho effettuato l'accesso con Mario Rossi (Amministrazione) e mi sono diretto all'interno della cartella del server dove ho potuto visualizzare tutte le cartelle condivise in rete:



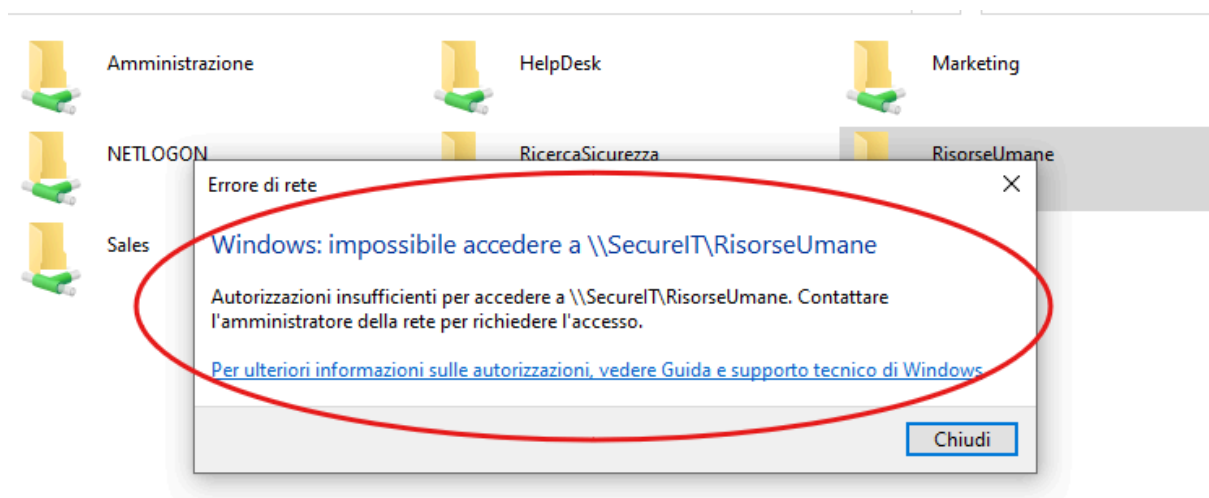
Ho dunque provato ad accedere alla cartella Amministrazione dove ho potuto navigare liberamente ed altresì creare un file all'interno della directory Fatture:



Ciò dimostra che i permessi della cartella in relazione al nostro gruppo erano stati correttamente attribuiti.

Il prossimo step è stato quello di verificare che l'utente non avesse però accesso a nessun'altra delle cartelle destinate agli altri gruppi.

Tentando infatti la procedura con qualunque delle altre cartelle riceviamo un messaggio di errore che ci comunica la mancanza di permessi sufficienti ad accedere a quel determinato percorso.



Possiamo confermare anche in questo caso che i permessi relativi al gruppo Amministrazione e alle varie cartelle sono stati correttamente attribuiti.

La stessa procedura è stata ripetuta anche sull'account **UT300 - Anna Verdi** - parte del gruppo **Sales** che è riuscita solamente ad accedere alla sua directory oltre che alla cartella Marketing dove però è stata impossibilitata a creare alcun tipo di file o apportare qualsivoglia modifica.

Ancora una volta è stato possibile confermare la corretta attribuzione dei privilegi tra i vari gruppi e risorse.

Creazione GPO

Per completare la configurazione dell'infrastruttura di dominio, è stata prevista l'applicazione di alcune **Group Policy Objects (GPO)** con lo scopo di centralizzare la gestione delle impostazioni di sicurezza e di utilizzo dei client. Le GPO rappresentano uno strumento essenziale in ambiente Active Directory, in quanto consentono di applicare configurazioni uniformi e controllate a utenti e computer, riducendo al minimo la necessità di interventi manuali.

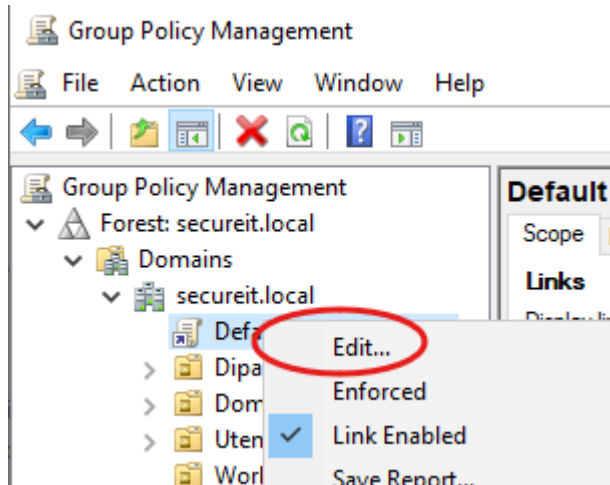
Nel caso di **SecureIT** sono state individuate quattro policy principali, selezionate in base a criteri di sicurezza e praticità operativa:

- **Policy di sicurezza delle password:** per garantire complessità minima, scadenza periodica e blocco degli account dopo tentativi falliti.
- **Policy di accesso remoto (RDP):** per permettere il collegamento ai soli amministratori di dominio, riducendo i rischi di accessi non autorizzati.
- **Policy di mappatura automatica delle cartelle di rete:** per rendere immediatamente disponibili agli utenti le risorse del proprio reparto senza necessità di configurazioni manuali.
- **Policy di restrizione sui client:** per impedire modifiche non autorizzate, limitando l'accesso a strumenti come il Pannello di Controllo, CMD o PowerShell agli utenti standard.

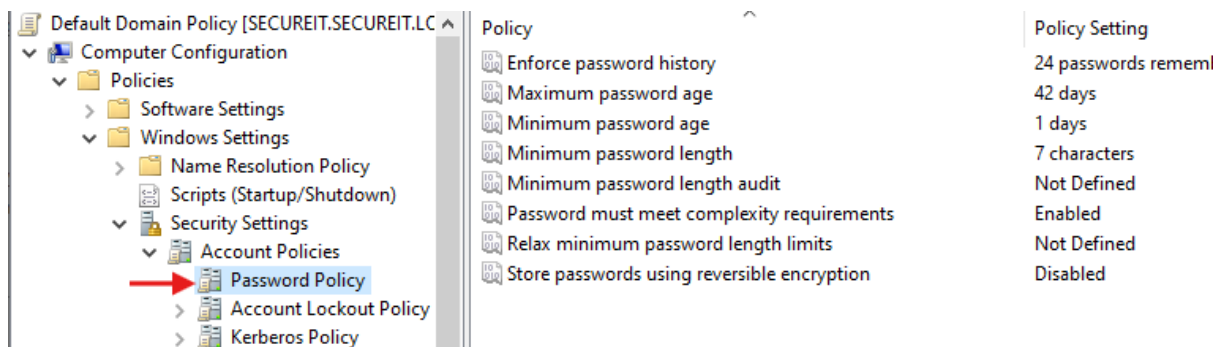
Queste policy sono state scelte per simulare esigenze reali di un'azienda di consulenza IT: maggiore sicurezza degli account, controllo centralizzato degli accessi, disponibilità semplificata delle risorse e protezione dell'integrità dei sistemi client.

Password Policy

Per procedere con il settaggio delle GPO è necessario spostarsi all'interno della sezione [Tools → Group Policy Management](#) e cliccare Edit, tramite tasto destro, sopra alla voce [Default Domain Policy](#) all'interno del dominio:



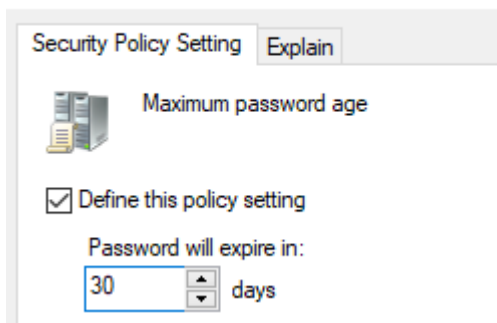
A questo punto avremo a disposizione un menù ricco di opzioni per la modifica di una moltitudine di Policies diverse; ciò che è di nostro interesse al momento è la sezione localizzata nel seguente percorso [Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy](#)



Alla voce [Enforce password history](#) possiamo lasciare il valore di default:24 in modo che l'utente sia obbligato a cambiare password 24 volte prima di poter riutilizzare una password di cui ha già usufruito in passato.

Come [Maximum password age](#) ho optato per inserire un valore di 30 giorni in modo che l'utente sia obbligato a cambiare credenziali ogni mese:

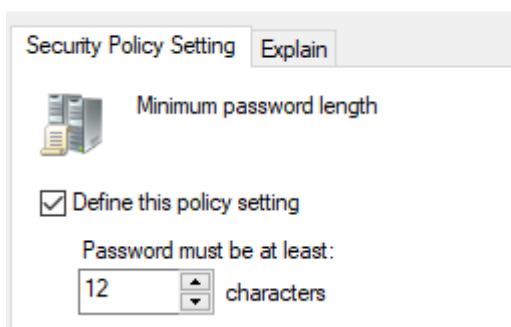
Maximum password age Properties



Su **Minimum password age** ho lasciato il valore di default 1 day (per evitare che un utente cambi più volte di fila fino a tornare alla vecchia password).

Il valore relativo a **Minimum password length** è stato incrementato fino a 12 per migliorare la difficoltà di rilevamento tramite attacchi bruteforce:

Minimum password length Properties



Password must meet complexity requirements è stato settato su Enabled in modo da forzare l'utilizzo di maiuscole, minuscole, numeri e caratteri speciali.

Store passwords using reversible encryption rimane Disabled in quanto risulta insicuro tenere in memoria i dati delle password decriptati.

Effetto

Con l'implementazione di tale policy tutti gli utenti del dominio **secureit.local** dovranno creare password complesse, non potranno riutilizzare facilmente quelle vecchie e saranno obbligati a cambiarle ogni 30 giorni.

Questa configurazione è stata applicata direttamente alla **Default Domain Policy**, in quanto in Active Directory le impostazioni relative a password e blocco account sono gestite esclusivamente a livello di dominio. Non è quindi possibile differenziare tali regole per singole OU tramite GPO standard.




Account Lockout Policy

Questa policy ha lo scopo di impedire tentativi di accesso non autorizzati tramite attacchi a forza bruta o tentativi ripetuti di indovinare la password. Dopo un numero definito di errori consecutivi, l'account viene bloccato per un periodo stabilito, aumentando la sicurezza del dominio.

Il percorso per accedervi è il seguente (proprio sotto al precedente):
[Computer Configuration](#) → [Policies](#) → [Windows Settings](#) → [Security Settings](#) → [Account Policies](#) → [Account Lockout Policy](#)

I valori impostati sono stati i seguenti:

- **Account lockout threshold** → 3 invalid logon attempts
(dopo 3 password errate consecutive, l'account viene bloccato).
- **Account lockout duration** → 30 minutes
(durata del blocco prima che l'account venga sbloccato automaticamente).
- **Reset account lockout counter after** → 30 minutes
(dopo 15 minuti senza nuovi errori, il conteggio dei tentativi falliti si azzerà).

Policy	Policy Setting
 Account lockout duration	30 minutes
 Account lockout threshold	3 invalid logon attempt:
 Reset account lockout counter after	30 minutes

Effetto

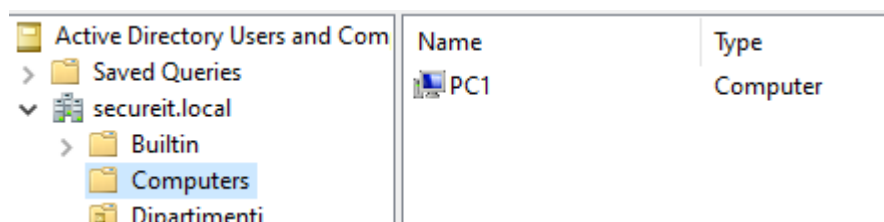
Grazie a questa configurazione, gli utenti del dominio **secureit.local** hanno una protezione aggiuntiva contro tentativi di accesso forzato. Dopo 3 tentativi di login falliti, l'account viene temporaneamente bloccato, rendendo inefficaci eventuali attacchi brute-force e costringendo a tempi di attesa.

Questa impostazione, come la Password Policy, viene gestita a livello di dominio e non può essere differenziata per singole OU.

GPO Accesso Remoto (RDP)

Un'altra policy importante consiste nella corretta configurazione e abilitazione del servizio **Remote Desktop** sui client garantendo che solo gli amministratori di dominio possano collegarsi. Questo previene che utenti standard accedano via RDP ad altri PC, riducendo i rischi di compromissione e mantenendo l'uso del protocollo confinato alla gestione IT.

Prima di procedere con la creazione di questa Policy ho ritenuto opportuno spostarmi all'interno dell'OU di default chiamata **Computers** dove ho potuto notare la presenza dell'oggetto **PC1**, il client che abbiamo utilizzato in precedenza per gli accessi agli utenti:

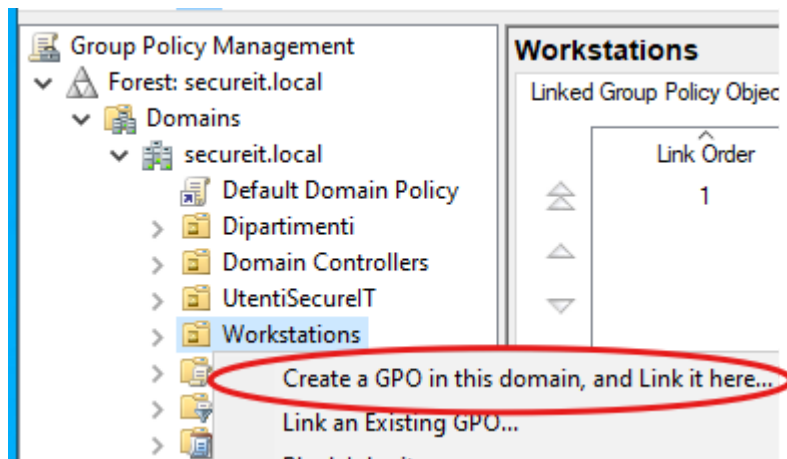


A questo punto, per avere una migliore compartimentazione e gestione ho deciso di spostarlo all'interno di una nuova Organizational Unit chiamata **Workstations**:

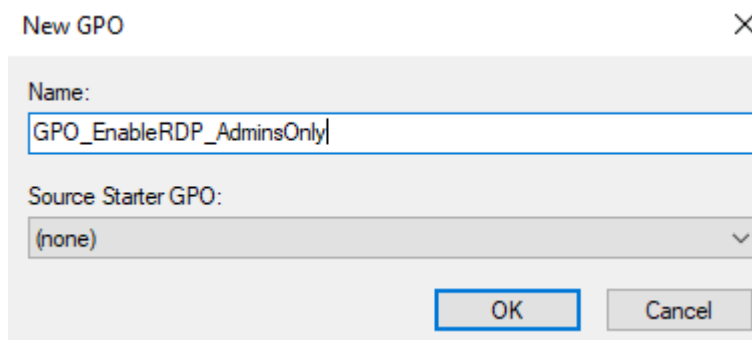
New Object - Organizational Unit

The screenshot shows the 'New Object - Organizational Unit' dialog box. It has a 'Create in:' field set to 'secureit.local/'. Below this is a 'Name:' field with the text 'Workstations' entered. At the bottom, there is a checkbox labeled 'Protect container from accidental deletion' which is checked.

Una volta creata la nuova OU mi sono spostato nuovamente all'interno del **Group Policy Management** ed ho creato una nuova policy relativa alla organisation Unit appena creata:



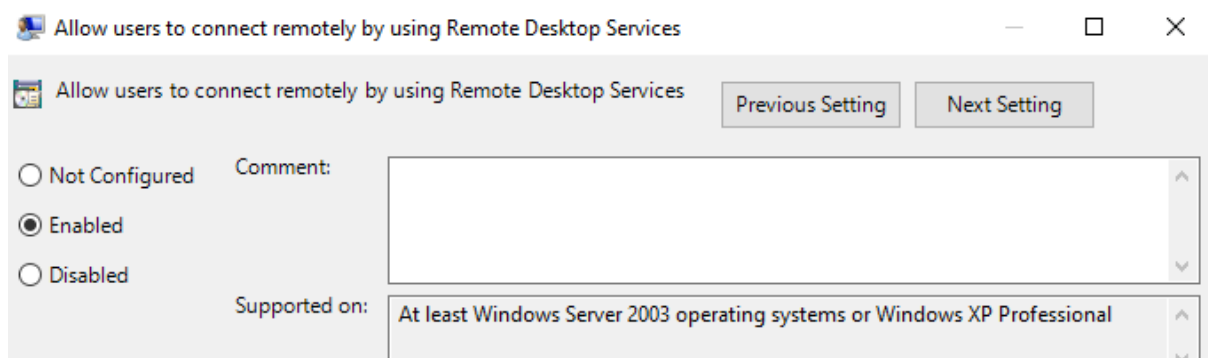
E le assegnato un nome descrittivo relativo al suo scopo:



Il prossimo passo è stato abilitare RDP tramite il seguente percorso:

Computer Configuration → Policies → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Connections

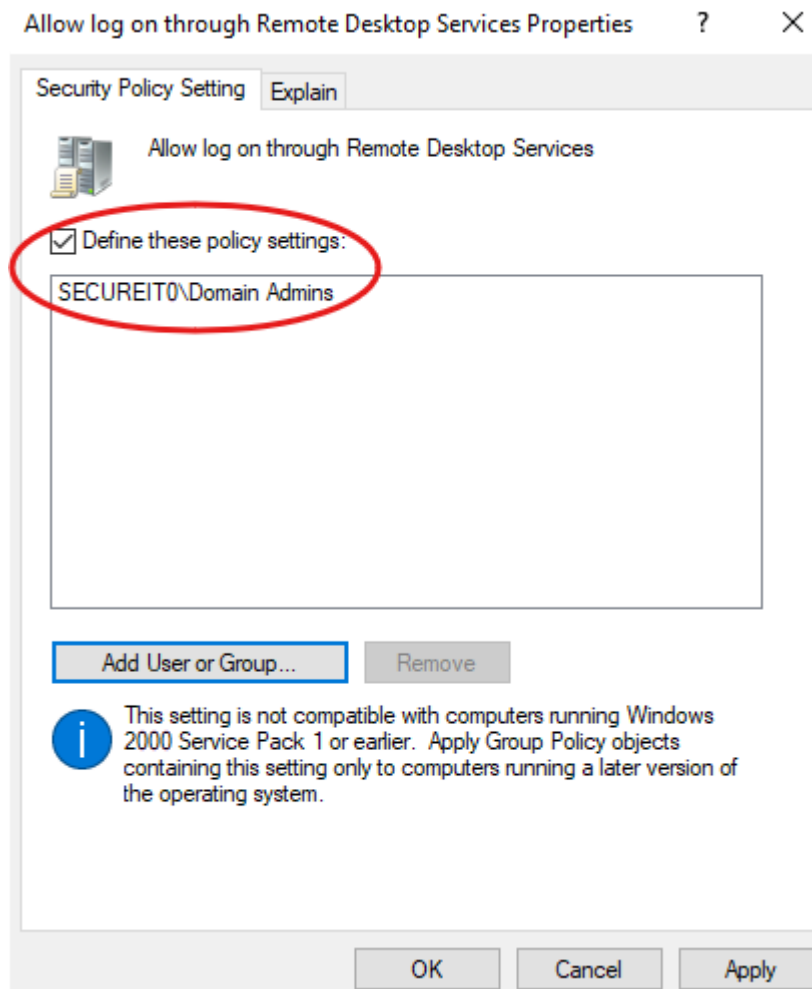
Ed abilitare **Allow users to connect remotely using Remote Desktop Services**.



Il secondo passaggio è stato limitare agli Admins la possibilità di accesso in RDP spostandosi all'interno di questo percorso:

Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment

Ed assegnando al gruppo **Domain Admins** la policy **Allow log on through Remote Desktop Services**.



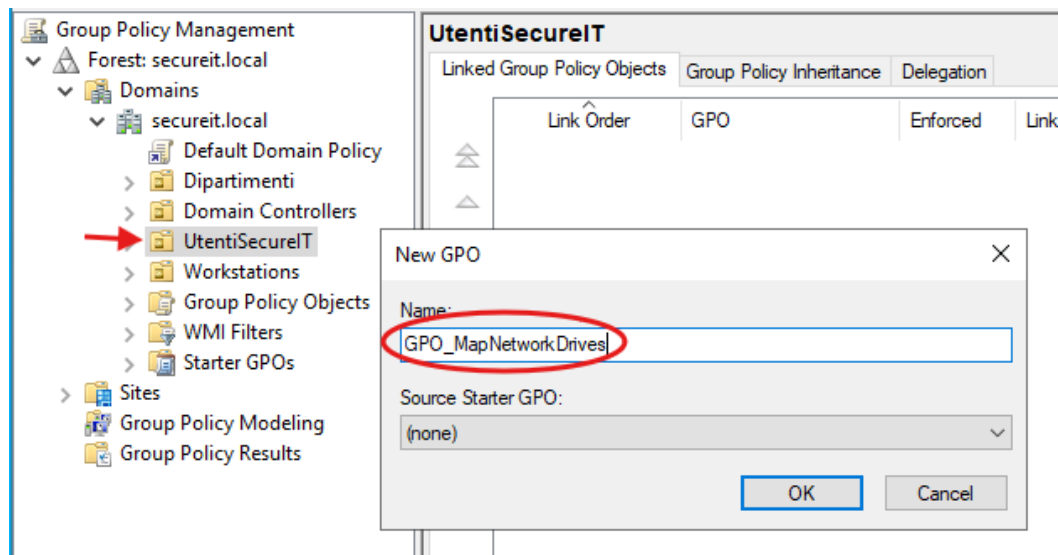
Effetto

Tutti i computer presenti nell'OU **Workstations** avranno il servizio RDP attivo, ma soltanto i membri del gruppo **Domain Admins** potranno accedere tramite Remote Desktop. Gli utenti standard di dominio (es. Mario Rossi – UT100) non potranno stabilire sessioni RDP.

GPO Mappatura automatica cartelle di rete

La seguente policy è stata pensata per garantire che ogni utente, una volta autenticato nel dominio, abbia già disponibile come unità di rete la cartella condivisa del proprio reparto, senza doverla mappare manualmente. Questo semplifica l'operatività e riduce gli errori.

Per la configurazione di tale GPO è stato necessario creare una nuova GPO all'interno dell'OU UtentiSecureIT che è stata denominata **GPO_MapNetworkDrives**:

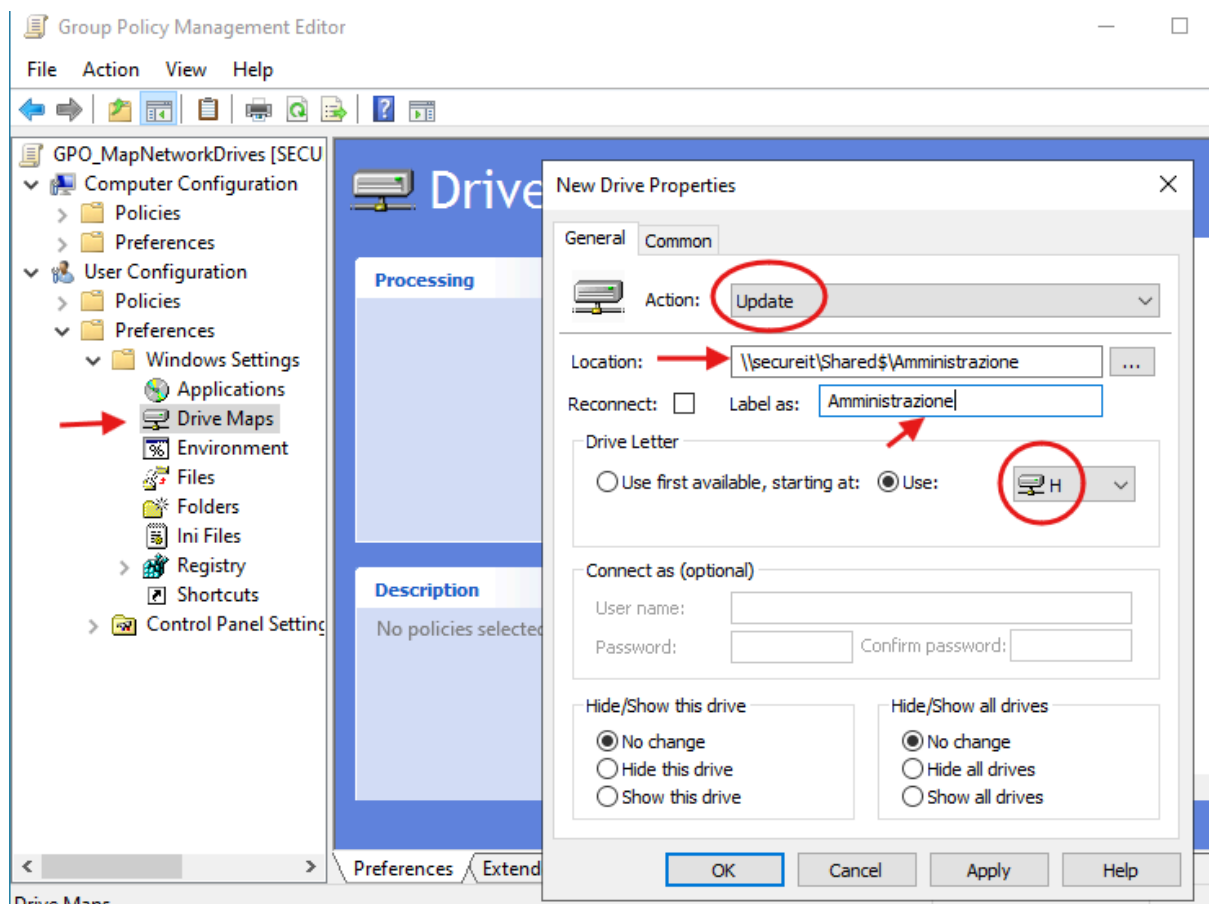


Fatto ciò è stato ovviamente necessario andare a modificarla cliccando su edit e raggiungendo il seguente percorso:

[User Configuration](#) → [Preferences](#) → [Windows Settings](#) → [Drive Maps](#).

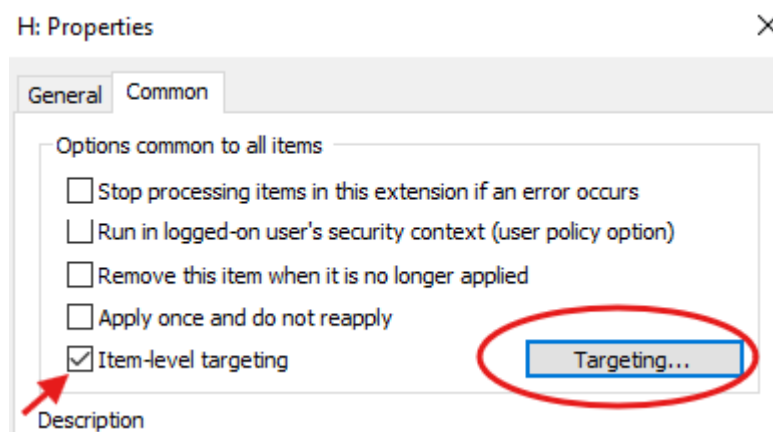
Tramite clic destro → New → Mapped Drive impostare il drive come segue:

- Location: [\\secureit\\Shared\\$\\Amministrazione](#)
- Drive letter: **H:** (o un'altra libera)
- Label: [Amministrazione](#)
- Action: Update

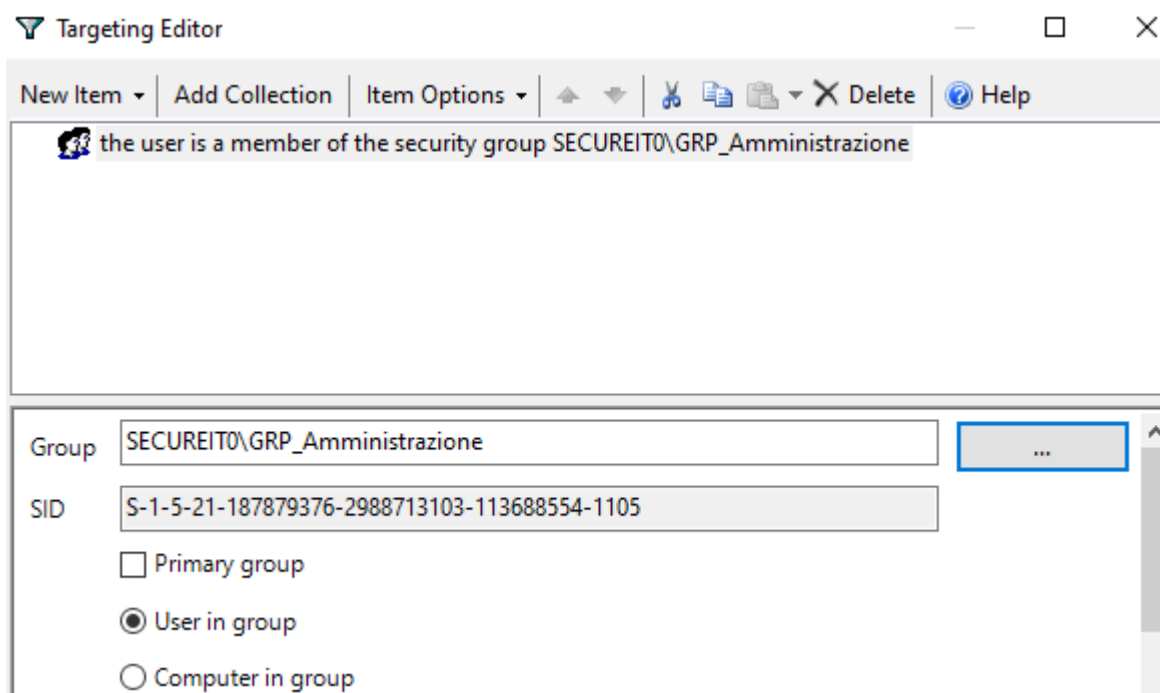


L'ultimo passaggio da compiere consiste nel filtraggio per gruppo.

Spostandosi nella scheda **Common**, spuntando **Item-level targeting** e cliccando successivamente su **Targeting...**



E' possibile aggiungere una regola di *Security Group is* → *GRP_Ammministrazione* In modo che la mappatura sia applicata solo agli utenti del gruppo Amministrazione.



La stessa procedura va ovviamente ripetuta creando una mappatura per ogni reparto (*Sales*, *Marketing*, ecc.) con targeting sul gruppo corrispondente.

Effetto

Quando un utente di dominio accede (es. Mario Rossi – GRP_Ammministrazione), vedrà automaticamente in Esplora file l'unità di rete **H:** puntata alla cartella del proprio reparto. Non sarà necessario mappare manualmente le cartelle, e ciascun utente avrà accesso solo alle risorse per cui ha permessi NTFS.

GPO Restrizioni Client (Workstations)

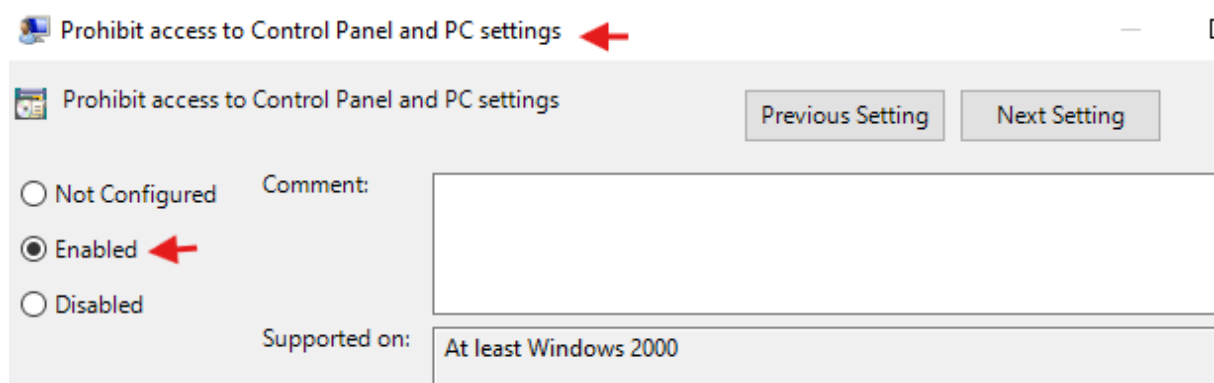
Con quest'ultima policy si mira a limitare ciò che gli utenti standard possono fare sui PC aziendali. È pensata per aumentare la sicurezza e ridurre i rischi di configurazioni sbagliate o esecuzione di comandi dannosi.

La policy va configurata sull'OU workstation in quanto andrà a contenere tutti gli endpoint utilizzati dagli utenti non admin:

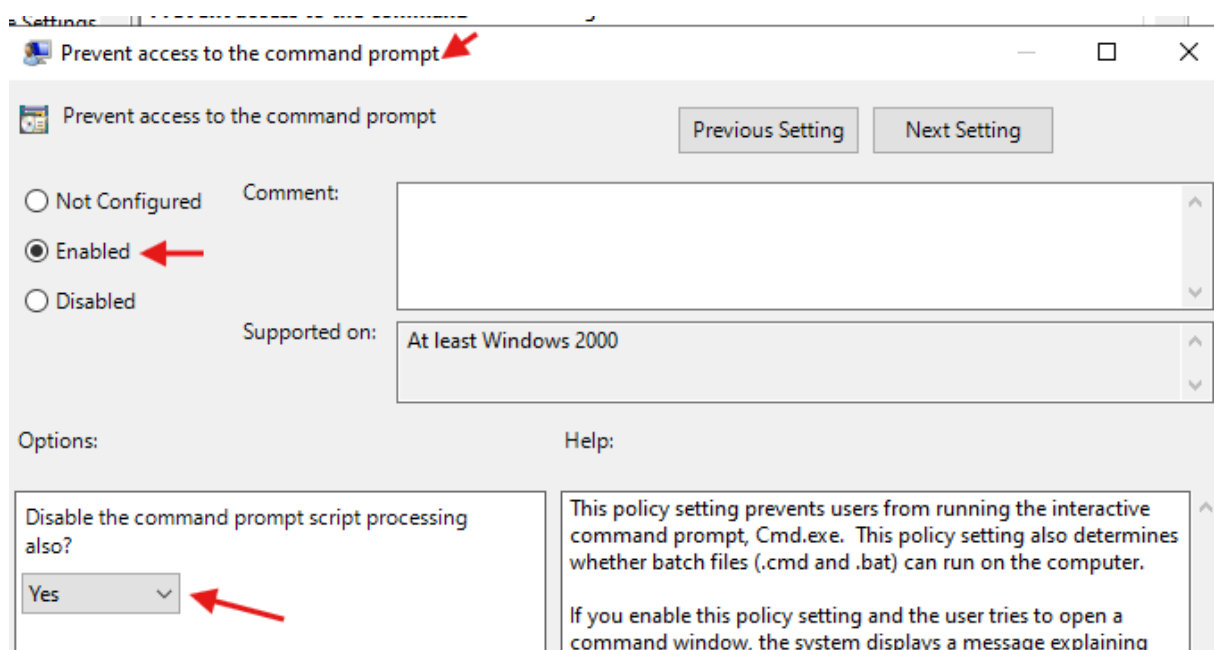
GPO_ClientRestrictions

La policy va poi modificata per:

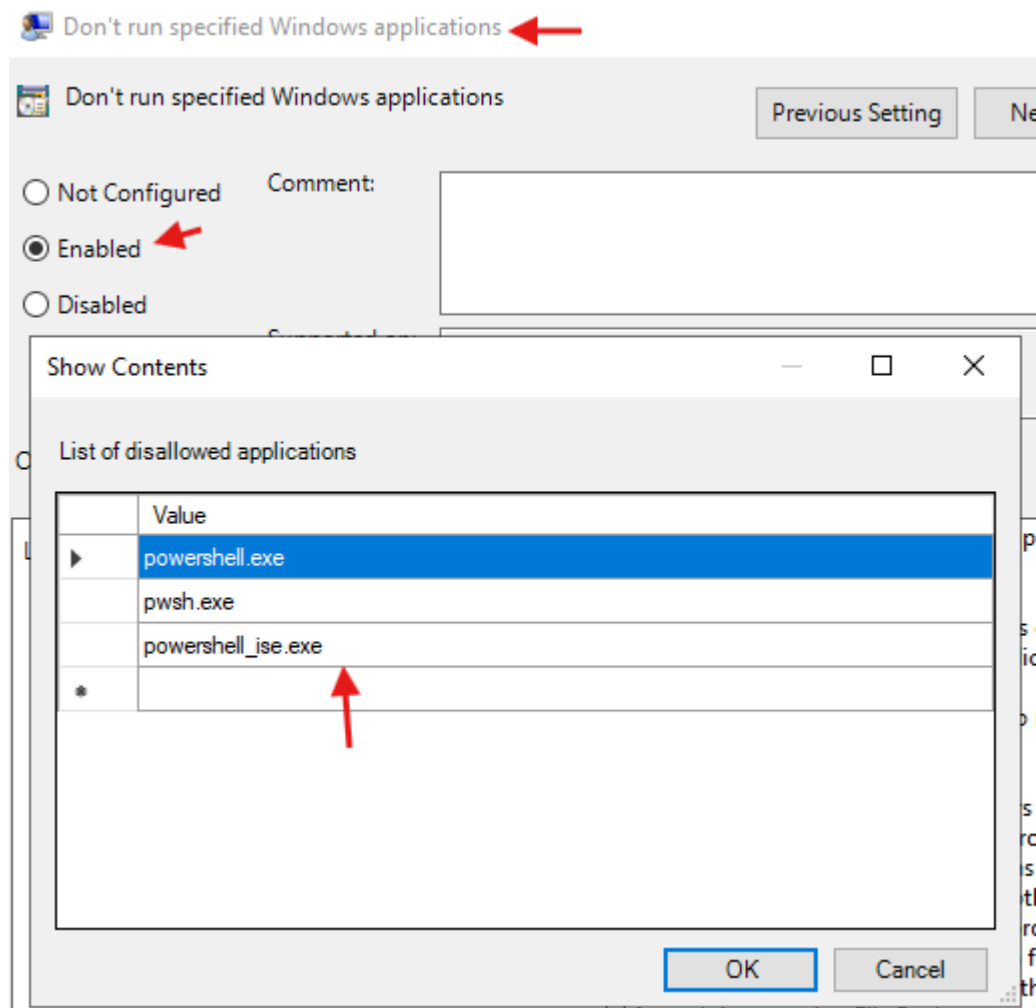
Bloccare Pannello di Controllo e Impostazioni tramite [User Configuration](#) → [Policies](#) → [Administrative Templates](#) → [Control Panel](#) e abilitando **Prohibit access to Control Panel and PC settings**.



Bloccare Prompt dei comandi (CMD) tramite [User Configuration](#) → [Policies](#) → [Administrative Templates](#) → [System](#) e abilitando **Prevent access to the command prompt** ed impostando anche che non si possano eseguire file batch.



Limitare PowerShell tramite [User Configuration](#) → [Policies](#) → [Administrative Templates](#) → [System](#) e abilitando **Don't run specified Windows applications** inserendo [powershell.exe](#) e [powershell_ise.exe](#) come programmi da bloccare.



NOTA BENE: Per impedire bypass semplici come il rinominare [powershell.exe](#), è necessario utilizzare **AppLocker**: un meccanismo di Application Control più robusto di una semplice lista di eseguibili. AppLocker permette di creare regole basate su **publisher**, **path** o **file hash** e viene gestito tramite GPO. Per bloccare PowerShell in modo resistente ai semplici rinominamenti, la soluzione consigliata è creare regole **deny** basate sull'**hash** del file.

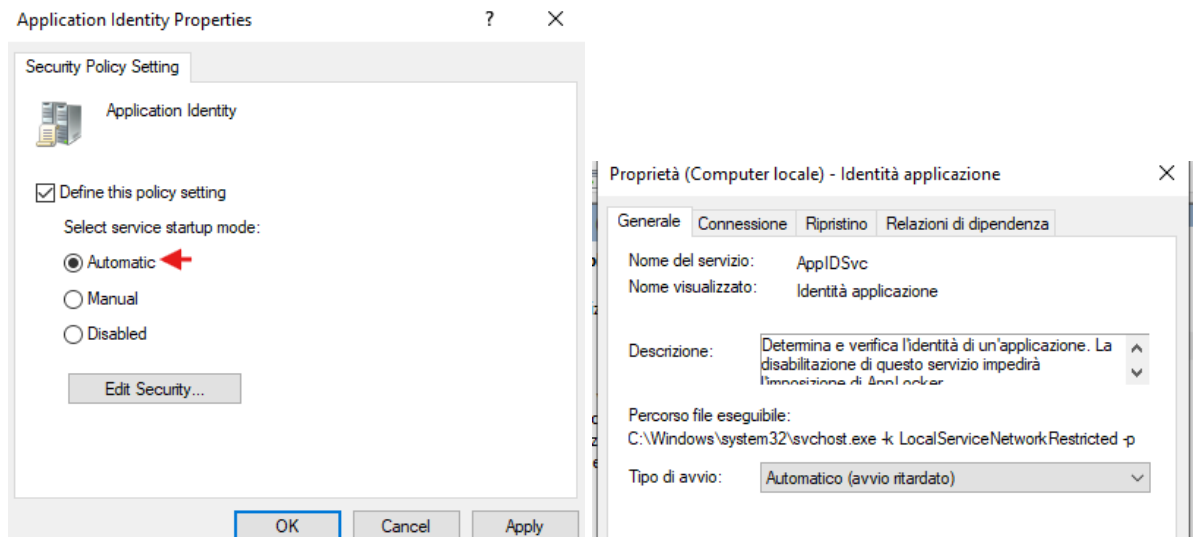
Per configurarlo è necessario creare una GPO dedicata ad AppLocker e collegarla all'OU [Workstations](#) (non al dominio intero). Questo permette di testare il comportamento sui client senza impattare server o altri oggetti.

In Group Policy Management click destro su [Workstations](#) → Create a GPO in this domain, and Link it here... → nome: [GPO_AppLocker_Workstations](#)

Modificare successivamente la GPO e andare in [Computer Configuration → Policies → Windows Settings → Security Settings → System Services](#).

Trovare il servizio **Application Identity** ed impostare lo startup su Automatic.

Il servizio Application Identity (AppIDSvc) è essenziale: senza di lui AppLocker non applica nessuna regola. Impostandolo su Automatic, si assicura che parta sempre all'avvio delle workstation.



Infine nell'editor della GPO andando in [Computer Configuration → Policies → Windows Settings → Security Settings → Application Control Policies → AppLocker](#)

Troviamo quattro categorie: Executable Rules, Windows Installer Rules, Script Rules, Packaged app Rules.

Su **Executable Rules** selezioniamo Create New Rule:




Nella schermata iniziale selezioniamo Deny e settiamo la condizione:

Scegliamo **File hash** (così il blocco non dipende dal nome o percorso, ma dall'impronta crittografica del file).

Select the type of primary condition that you would like to create.

☐ Publisher
Select this option if the application you want to create the rule for is signed by the software publisher.

☐ Path
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

☒ **File hash** 
Select this option if you want to create a rule for an application that is not signed.

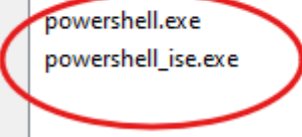
Procedendo su Browse si seleziona **powershell.exe** da **C:\Windows\System32\WindowsPowerShell\v1.0**.

Aggiungiamo anche **powershell_ise.exe** (editor) e, se disponibile, **pwsh.exe** (PowerShell Core).

Select the file from which the file hash will be created. Click Browse Files to select a specific file or click Browse Folders to select all files within a folder.

Files:

File Name	Size
powershell.exe	440 KB
powershell_ise.exe	208 KB



Browse Files...
Browse Folders...
Remove

Ed infine assegnamo la regola al gruppo **Everyone** (così vale per tutti gli utenti).

Effetto

- Gli utenti normali (es. UT100 Mario Rossi – Amministrazione) non potranno aprire **Pannello di Controllo** o modificare impostazioni di sistema.
- Non avranno accesso al **Prompt dei comandi**, né potranno eseguire script **.bat**.
- L'uso di **PowerShell** sarà bloccato, riducendo drasticamente i rischi di esecuzione di comandi dannosi o script non autorizzati.
- I membri del gruppo **Domain Admins** non saranno limitati, poiché possono sempre bypassare queste restrizioni grazie ai privilegi elevati.

Testing GPOs

A questo punto si può procedere a testare le Policy appena implementate.

Possiamo iniziare loggando con un utente a cui viene richiesto il cambio di password per testare se effettivamente le policy inerenti alla lunghezza e complessità delle credenziali sono ora operative.

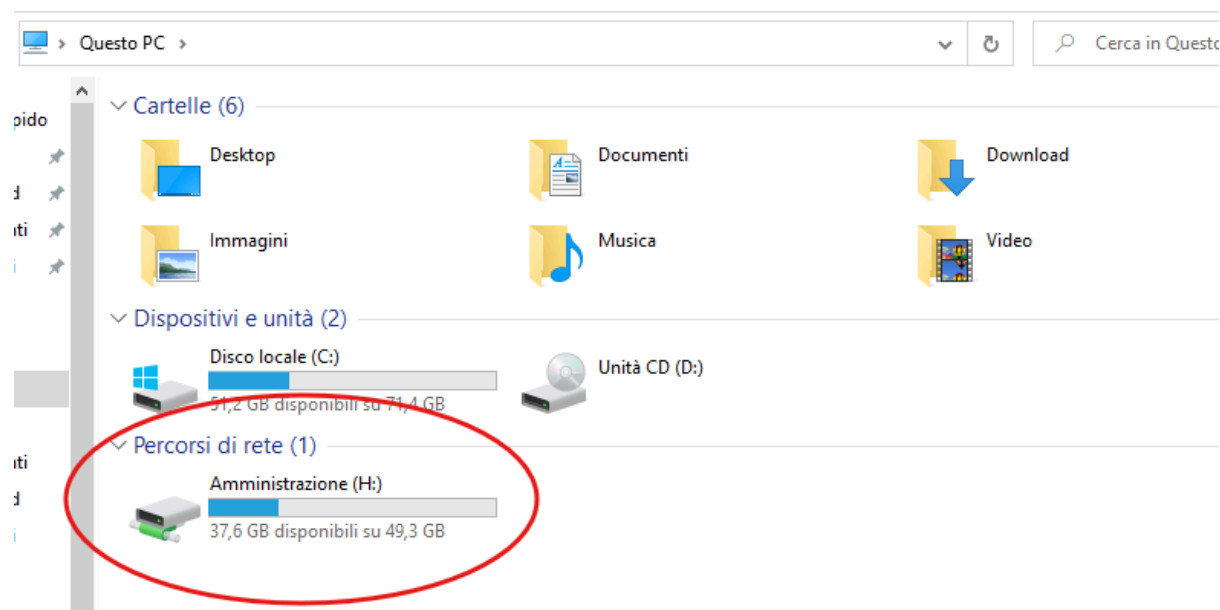
Dopo aver tentato il login con l'UT200 notiamo infatti che, provando ad inserire una password con lunghezza minore di 12 caratteri e/o con la mancanza di Maiuscole, minuscole, numeri e simboli ci verrà restituito un errore:



La Password Policy è dunque stata configurata correttamente!

Una volta impostata una password adeguata possiamo procedere nel confermare la presenza della Mappatura automatica delle cartelle di rete.

Procedendo all'interno della sezione **Computer** è possibile notare la presenza del volume di appartenenza del gruppo dell'utente:

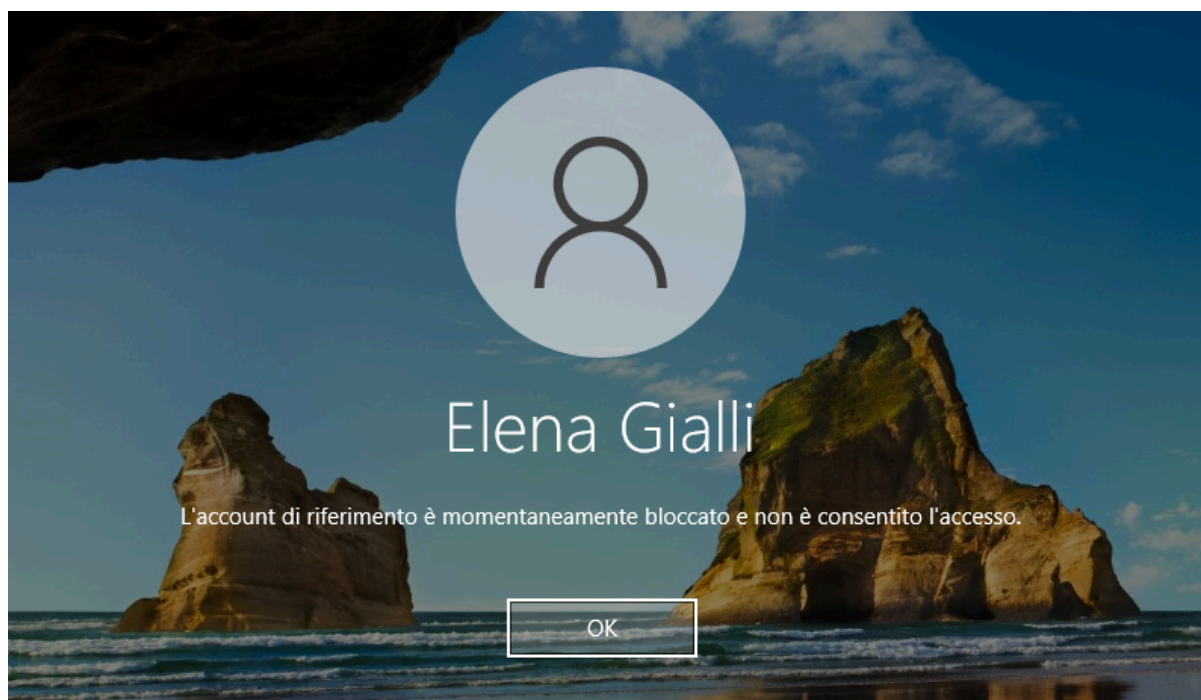


Il tentativo è stato svolto con l'utente Mario Rossi(Ammministrazione) in quanto è stata prima testata la policy di lockout impedendoci così di accedere all'account all'UT200 per 30 minuti.

Anche in questo caso, **la Policy della mappatura della cartella di rete è stata configurata con successo!**

Per testare la Lockout Policy possiamo semplicemente disconnetterci dalla sessione e tentare di riloggarci sbagliando di proposito la password immessa.

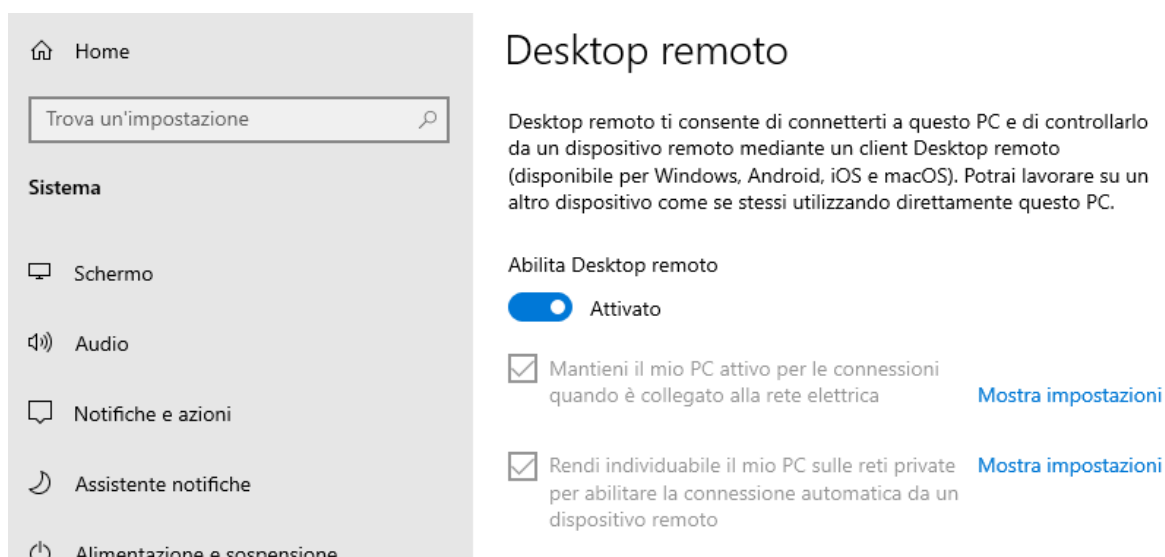
Dopo il terzo tentativo constatiamo che il nostro account è stato **momentaneamente bloccato**:



La GPO per l'Account Lockout è stata implementata correttamente!

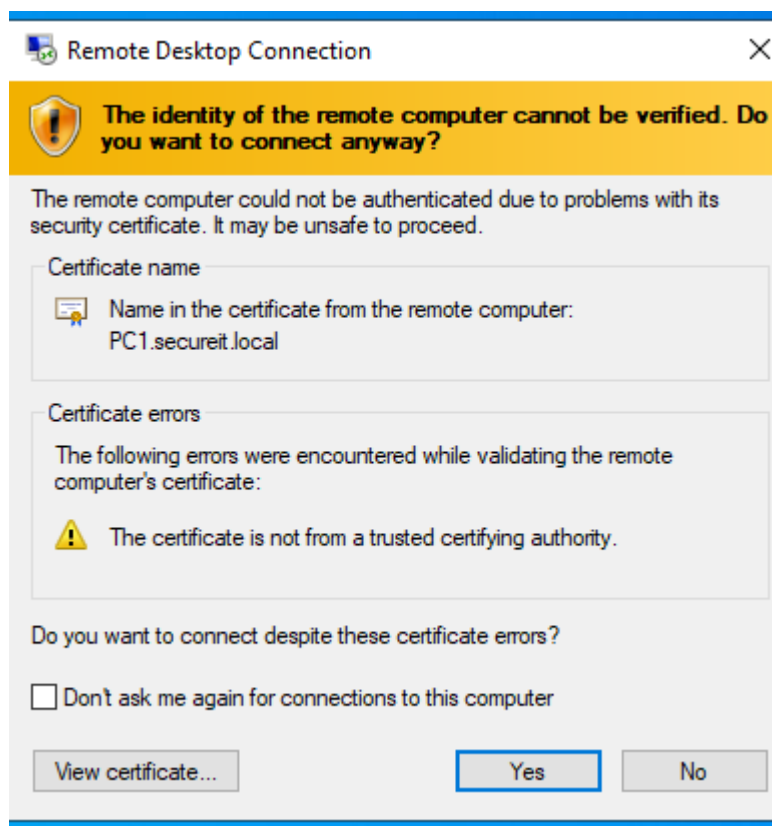
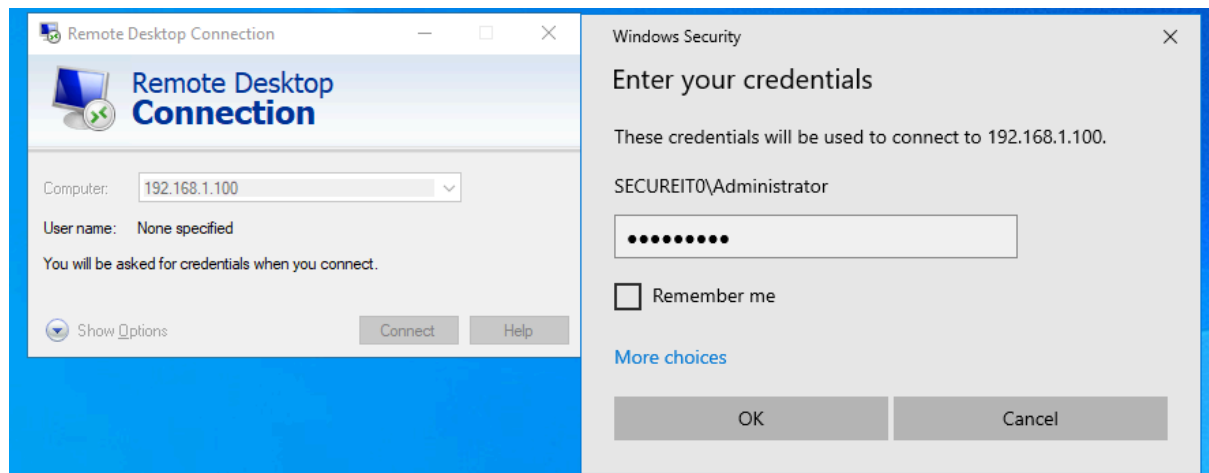
Non resta ora che testare le GPO relative alla connessione tramite Remote Desktop.

Prima di iniziare è fondamentale assicurarsi che la macchina verso la quale si vuole effettuare la connessione abbia il servizio attivo; per fare ciò è necessario andare in [Impostazioni](#) → [Sicurezza](#) → [Remote Desktop](#) e attivarlo:

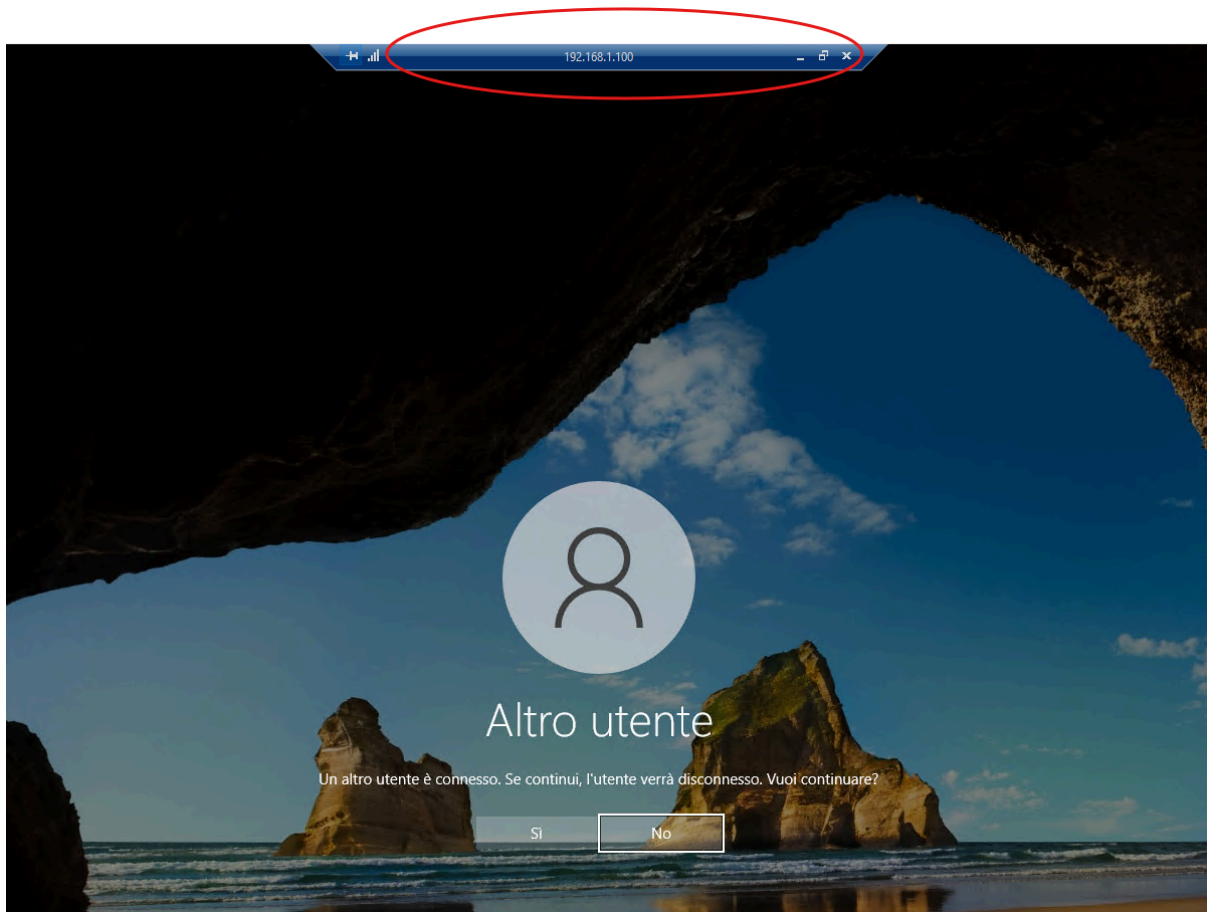


Fatto ciò possiamo tentare di connetterci all'IP della macchina PC1 utilizzando l'account Administrator - parte del gruppo Domain Admin - ed una volta

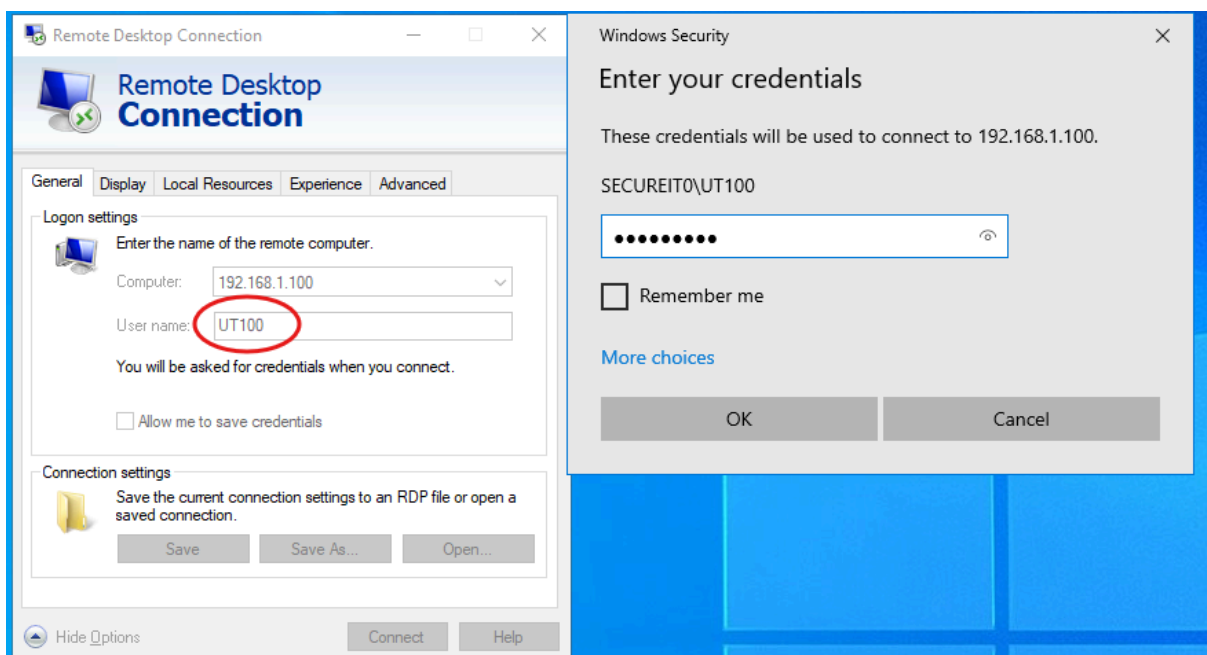
inserita la password ci verrà chiesto di confermare la volontà di connetterci al dispositivo sebbene non ufficialmente riconosciuto:



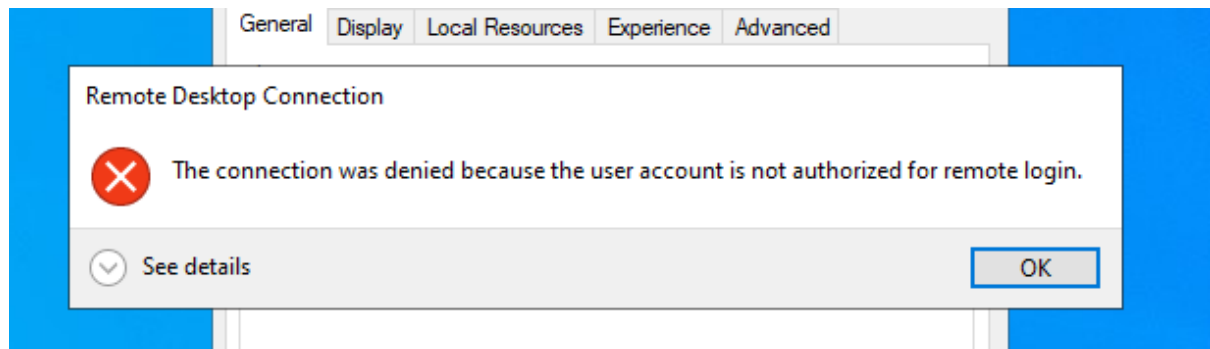
Confermate le nostre intenzioni nel proseguire, possiamo chiaramente notare che siamo riusciti ad effettuare la connessione tramite l'account Administrator:



Per confermare però l'intera configurazione della GPO dobbiamo anche tentare il collegamento tramite un account non facente parte del gruppo Admin:

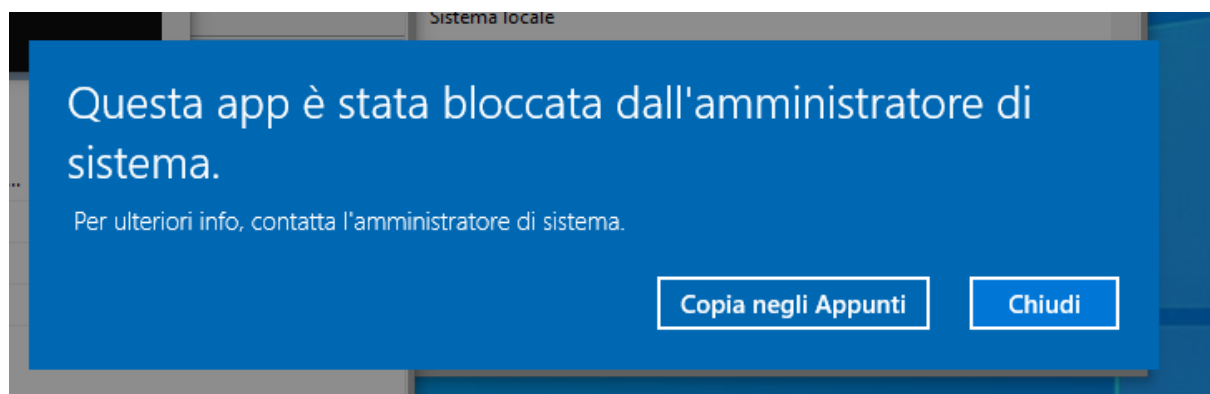


Questa volta a seguito della conferma di voler proseguire con la connessione il sistema ci restituirà un pop-up che ci segnalerà l'impossibilità nel proseguire in quanto **l'account utilizzato non risulta autorizzato a compiere l'operazione**:



Le GPO relative ad RDP sono state correttamente configurate!

L'ultimo test rimasto è quello relativo all'AppLocker; per confermare il funzionamento delle restrizioni imposte ho semplicemente avviato Powershell tramite tasto destro sul menù start ed ho subito ricevuto il messaggio di Windows che mi informa del fatto che **l'app è stata bloccata dall'amministratore di sistema**:



Anche l'ultima GPO si conferma correttamente configurata!

Conclusioni

L'esercizio ha permesso di sperimentare concretamente la gestione di un dominio Active Directory in ambiente Windows Server 2022, con un focus specifico su utenti, gruppi e politiche di sicurezza centralizzate.

La creazione dei gruppi per i diversi reparti di SecureIT e la definizione dei permessi NTFS hanno mostrato l'efficacia del modello RBAC (Role Based Access Control), garantendo separazione delle risorse e riduzione dei rischi di accesso non autorizzato.

Le GPO applicate hanno coperto diversi aspetti fondamentali:

- Sicurezza degli account tramite password complesse e policy di logout.
- Centralizzazione dell'accesso alle risorse aziendali grazie alla mappatura automatica delle cartelle di rete.
- Protezione dell'infrastruttura client con restrizioni a CMD, PowerShell e Pannello di Controllo, completate dall'uso di AppLocker.
- Gestione sicura dell'accesso remoto, limitato agli amministratori di dominio.

I test eseguiti con utenti reali (es. Mario Rossi – UT100) hanno confermato il corretto funzionamento delle configurazioni, dimostrando la capacità del dominio di applicare regole coerenti e sicure su tutti i client.

Nel complesso, l'attività ha permesso di acquisire familiarità sia con gli strumenti di base (OU, utenti, gruppi, NTFS) sia con funzionalità avanzate (GPO, AppLocker), evidenziando come una corretta pianificazione e segmentazione delle policy sia essenziale per garantire sicurezza e scalabilità in un contesto aziendale.