



Top 10 Things to Stay Out of the News

David Williams and Matt Barnett

Formal intro

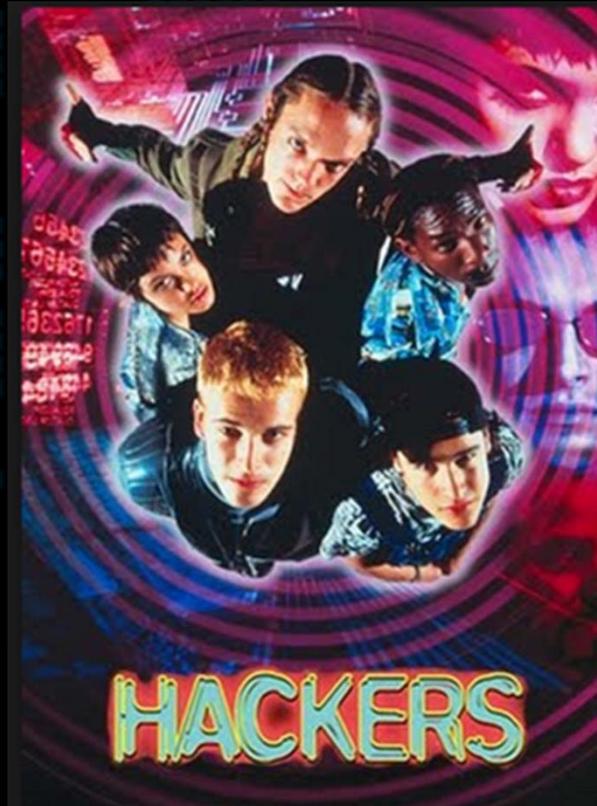


- **David Williams**, senior consultant
- **Matt Barnett**, consultant
- **BTB Security**
 - Security consulting services
 - Security monitoring solution & services

What we do

BTB SECURITY

We are hackers



...well...not exactly like that

These days

- A lot of breaches in the news
- We see that a lot of environments are vulnerable to simple issues



What we find

- Some attacks are complicated...
- But most take advantage of simple misconfiguration



Top Security Controls



This talk will focus on the **top security** controls that can be implemented **with low cost and low impact to your network**, ensuring maximum ROI of your Domain Admin's valuable time.

1-Separate DA from "everyday" Accounts

Domain Admin Account



2-Separate DA Password Policy



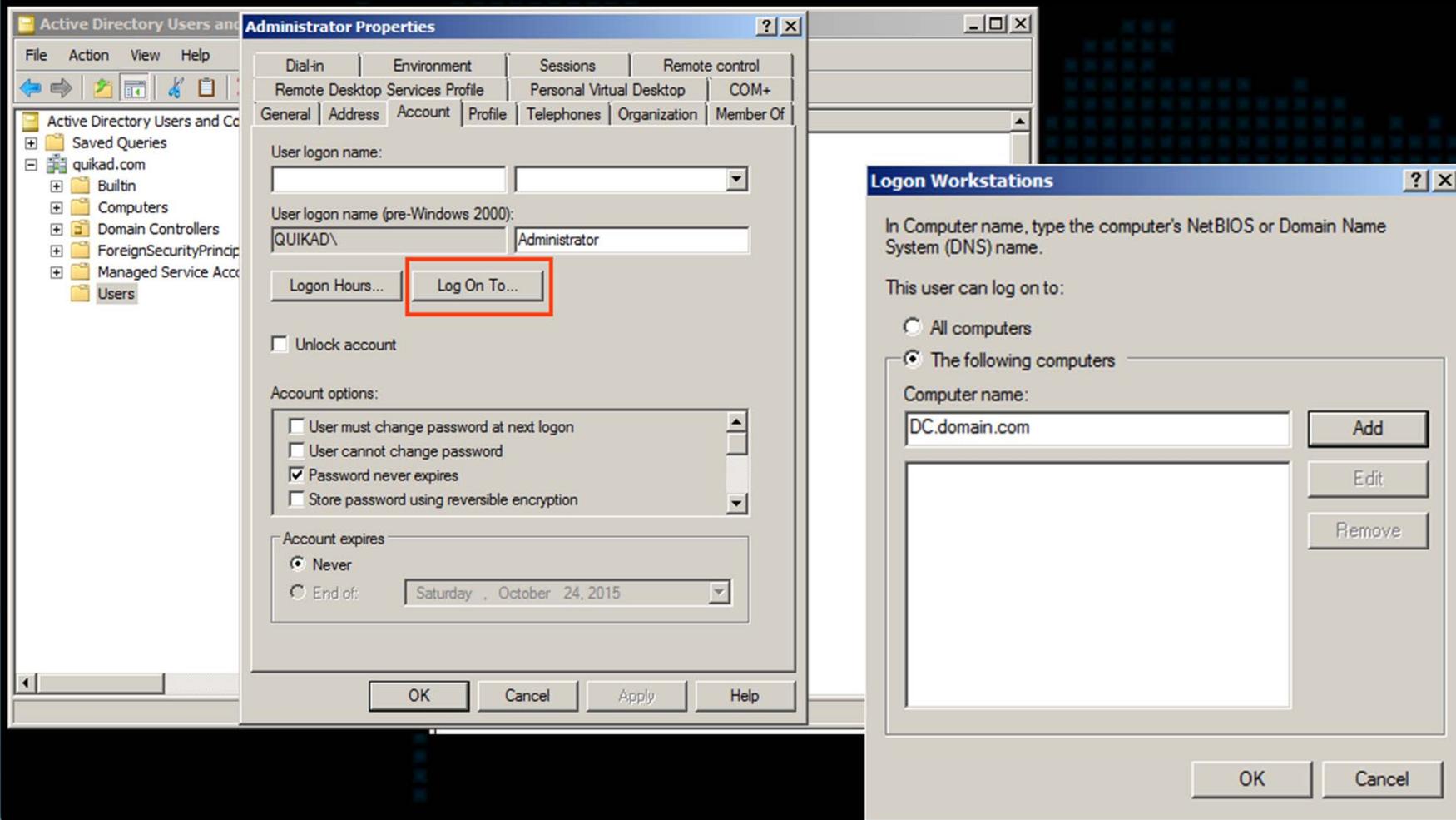
...t password

New

Confirm

 **The new password is too simple**
Please choose another password.

3-DA is Allowed to only Log in to Domain Controllers

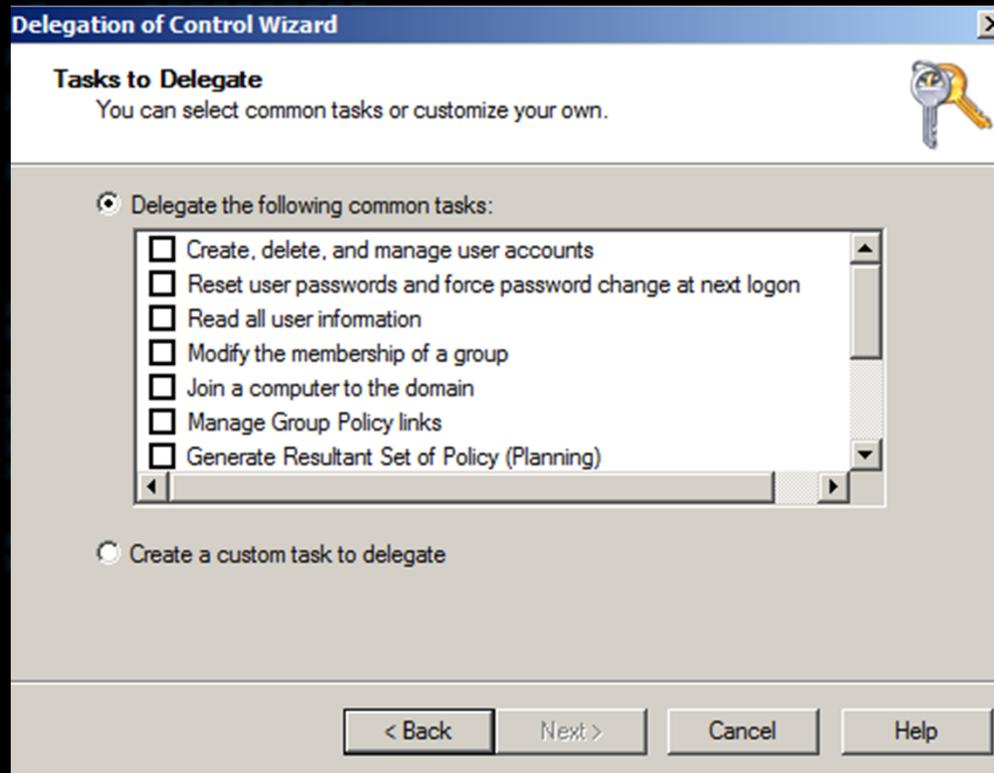


4-Delegate Rights to Users (Restrict User Access)

The screenshot shows the 'Active Directory Users and Computers' console tree with a context menu open over the 'Users' folder. The 'Delegation of Control...' option is selected. The 'Delegation of Control Wizard' dialog box is displayed in the foreground, showing the 'Welcome' screen. The wizard text reads: 'Welcome to the Delegation of Control Wizard. This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services. To continue, click Next.' The wizard has buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

| Name | Type |
|---------|--------------------|
| Builtin | builtinDomain |
| ... | Container |
| ont... | Organizational ... |
| ecur... | Container |
| Ser... | Container |
| ... | Container |

4-Delegate Rights to Users (Restrict User Access)



5-Disable Cached Credentials

BTB SECURITY



6-Microsoft Security Compliance Manager



Microsoft Security Compliance Manager

File View Help

Global setting search

DCNET - Win7-SSLF-Desktop 1.0 269 Setting(s)

Advanced View

| Name | Default | Microsoft | Customized | Severity | Path |
|--|--------------------|--------------------|--------------------|-------------|---------------------------------------|
| Audit Policies\Account Logon 4 Setting(s) | | | | | |
| Audit Policy: Account Logon: Creden | No auditing | Success and Failur | Success and Failur | None | Computer Configuration\Windows S |
| Audit Policy: Account Logon: Kerberc | No auditing | No Auditing | No Auditing | None | Computer Configuration\Windows S |
| Audit Policy: Account Logon: Kerberc | No Auditing | No Auditing | No Auditing | None | Computer Configuration\Windows S |
| Audit Policy: Account Logon: Other A | No auditing | No Auditing | No Auditing | None | Computer Configuration\Windows S |
| Audit Policies\Account Management 6 Setting(s) | | | | | |
| Audit Policy: Account Management: : | No auditing | No auditing | No auditing | None | Computer Configuration\Windows S |
| Audit Policy: Account Management: | No auditing | Success and Failur | Success and Failur | None | Computer Configuration\Windows S |
| Audit Policy: Account Management: | No auditing | No auditing | No auditing | None | Computer Configuration\Windows S |
| Audit Policy: Account Management: | No auditing | Success and Failur | Success and Failur | None | Computer Configuration\Windows S |
| Audit Policy: Account Management: | Success | Success and Failur | Success and Failur | None | Computer Configuration\Windows S |
| Audit Policy: Account Management: | Success | Success and Failur | Success and Failur | None | Computer Configuration\Windows S |
| Audit Policies\Detailed Tracking 4 Setting(s) | | | | | |
| Audit Policy: Detailed Tracking: DPAF | No auditing | No auditing | No auditing | None | Computer Configuration\Windows S |
| Audit Policy: Detailed Tracking: Proce | No auditing | Success | Success | None | Computer Configuration\Windows S |
| Audit Policy: Detailed Tracking: Pr | No auditing | No auditing | Success | None | Computer Configuration\Windows |
| Value must be equal to Success. Severity: None Collapse | | | | | |
| Customize setting value: Success Comments: <input type="text"/> | | | | | |
| Setting Details | | | | | |
| Audit Policy: Detailed Tracking: RPC I | No auditing | No Auditing | No Auditing | None | Computer Configuration\Windows S |
| Audit Policies\DS Access 4 Setting(s) | | | | | |
| Audit Policy: DS Access: Detailed Dirr | No auditing | No Auditing | No Auditing | None | Computer Configuration\Windows S |
| Audit Policy: DS Access: Directory Sei | No auditing | No auditing | No auditing | None | Computer Configuration\Windows S |
| Audit Policy: DS Access: Directory Sei | No auditing | No auditing | No auditing | None | Computer Configuration\Windows S |
| Audit Policy: DS Access: Directory Sei | No auditing | No auditing | No auditing | None | Computer Configuration\Windows S |
| Audit Policies\Logon Logoff 9 Setting(s) | | | | | |
| Audit Policy: Logon-Logoff: Account | Success | No auditing | No auditing | None | Computer Configuration\Windows S |
| Audit Policy: Logon-Logoff: IPsec Ext. | No auditing | No auditing | No auditing | None | Computer Configuration\Windows S |

Import: [GPO Backup \(folder\)](#), [SCM \(.cab\)](#)

Export: [Excel \(.xlsm\)](#), [GPO Backup \(folder\)](#), [SCAP v1.0 \(.cab\)](#), [SCCM DCM 2007 \(.cab\)](#), [SCM \(.cab\)](#)

Baseline: [Compare / Merge](#), [Delete](#), [Duplicate](#), [Lock](#), [Properties](#)

Setting: [Add](#), [Delete](#), [Move](#)

Setting Group: [Add](#), [Delete](#), [Properties](#)

Help: [About](#), [Help Topics](#), [Release Notes](#), [Send Feedback](#), [Privacy Statement](#)

7-Disable NULL Sessions

```
net use \\IP_ADDRESS\ipc$ "" /user:""
```

8-Disable LLMNR/NBNS Protocols

LL What? NB Who?

Link-Local Multicast Name Resolution and NetBIOS Naming Service

- 1) Hosts File
- 2) DNS Server
- 3) LLMNR Multicast or NBNS Broadcast

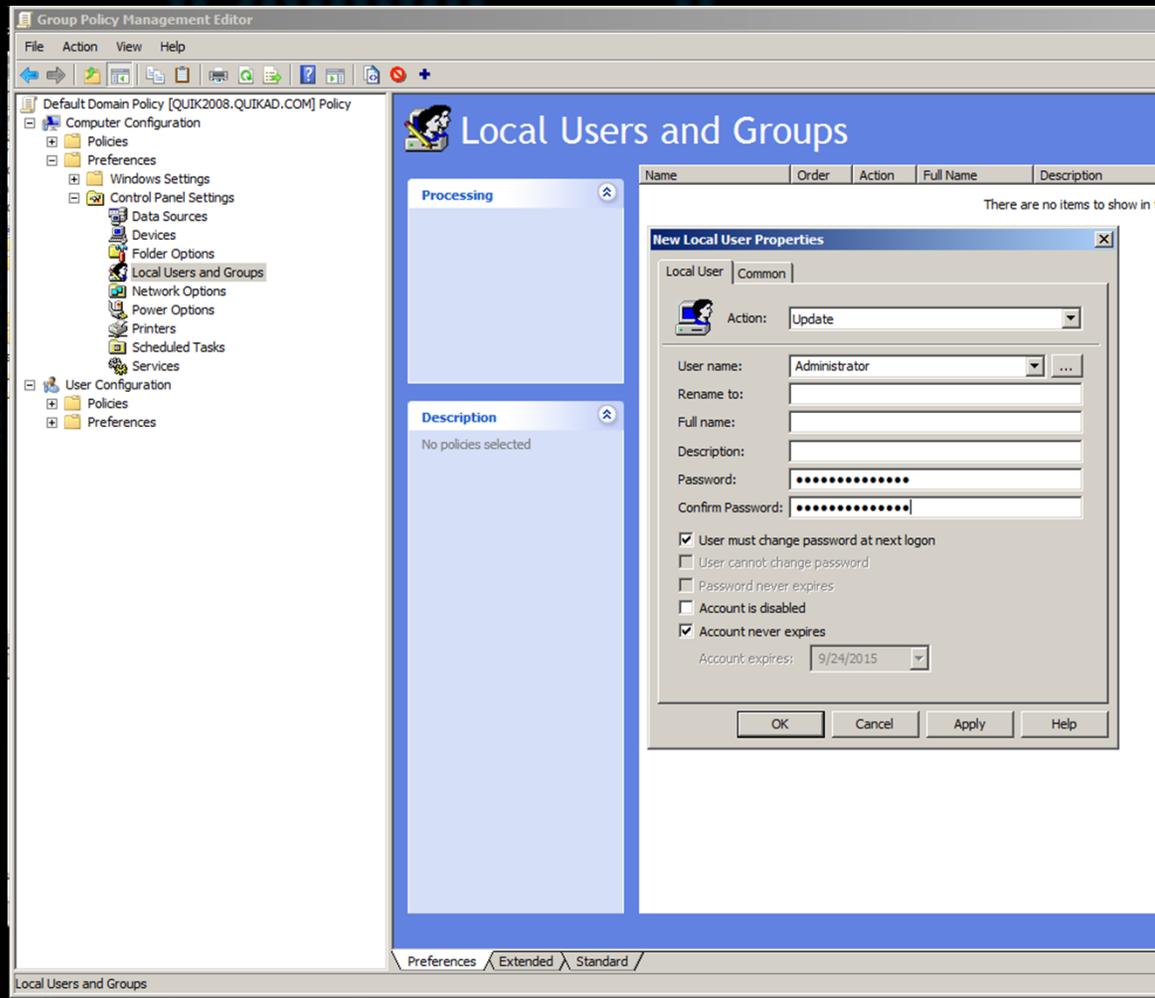
9-Set SMB Signing to Enabled and Required



<http://btbsecurity.com/resources/videos/204-smbrelay-and-llmnr-zero-to-breach-in-ten-minutes>

10-Do Not Store Passwords within Group Policy Preferences (GPP)

BTB SECURITY



10-Do Not Store Passwords within Group Policy Preferences (GPP)



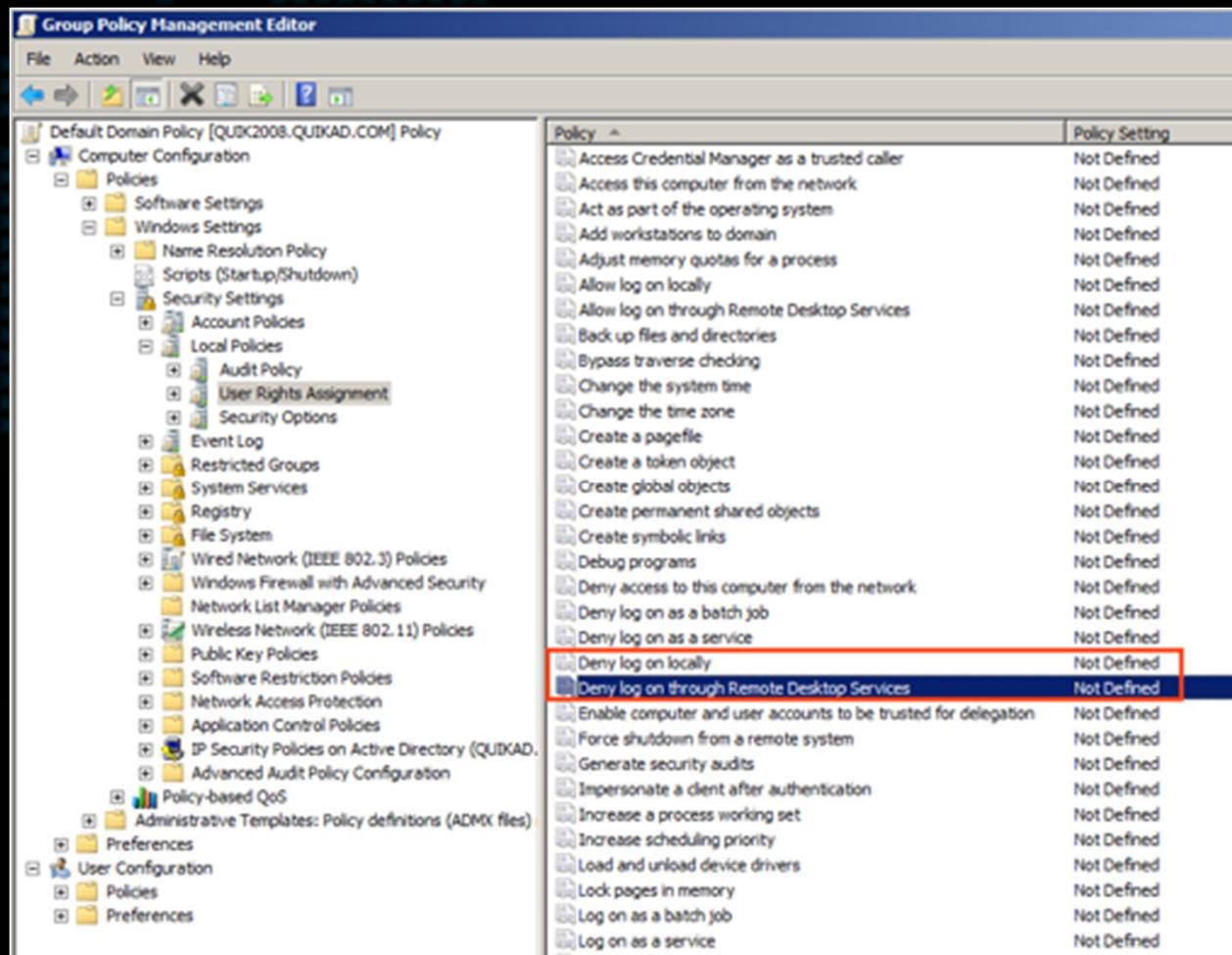
```
C:\>findstr /S cpassword \\dc1.securus.corp.com\sysvol\*.xml
\\192.168.122.55\sysvol\securus.corp.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Pref
erences\Groups\Groups.xml: =" description=" cpassword="1MJPOM4MqvDWWJq5IY9nJqeUHMMt6N2CUtb7B/jRFPs"
 changeLogon="0" noChange="0" neverExpires="0" acctDisabled="1" subAuthority="RID_ADMIN" userName="Ad
ministrator (built-in)"/>
```

```
gpp-decrypt 1MJPOM4MqvDWWJq5IY9nJqeUHMMt6N2CUtb7B/jRFPs
1q2w3e4r5t
```



The End

#Bonus 1 - Disable Interactive Logon for Service Accounts



#Bonus 2 - Use Managed Service Accounts

- Active Directory Users and Computers [Quik2008.quikad.com]
 - + Saved Queries
 - quikad.com
 - + Builtin
 - + Computers
 - + Domain Controllers
 - + ForeignSecurityPrincipals
 - + LostAndFound
 - Managed Service Accounts**
 - + Program Data
 - + System
 - + Users
 - + NTDS Quotas

#Bonus 4 - Who can Add Workstations to your Domain?

The screenshot displays the Group Policy Management Editor interface. On the left, the tree view shows the hierarchy: Default Domain Policy (QUKAD.COM) > Computer Configuration > Policies > Security Settings > Local Policies > User Rights Assignment. The 'Add workstations to domain' policy is selected in the main pane. The right pane shows the policy settings, with 'authenticated users' listed under 'Policy Setting'. A dialog box titled 'Add workstations to domain Properties' is open, showing the 'Security Policy Setting' tab. The dialog contains the following text:

Add workstations to domain

This security setting determines which groups or users can add workstations to a domain.

This security setting is valid only on domain controllers. By default, any authenticated user has this right and can create up to 10 computer accounts in the domain.

Adding a computer account to the domain allows the computer to participate in Active Directory-based networking. For example, adding a workstation to a domain enables that workstation to recognize accounts and groups that exist in Active Directory.

Default: Authenticated Users on domain controllers.

Note: Users who have the Create Computer Objects permission on the Active Directory computers container can also create computer accounts in the domain. The distinction is that users with permissions on the container are not restricted to the creation of only 10 computer accounts. In addition, computer accounts that are created by means of Add workstations to domain have Domain Administrators as the owner of the computer account, while computer accounts that are created by

For more information about security policy and related Windows features, [see the Microsoft website](#).

Buttons: OK, Cancel, Apply

#Bonus 5 - Disable Powershell and CMD

BTB SECURITY



Questions?

BTB SECURITY

David Williams

David.Williams@btbsecurity.com

Matt Barnett

matt.barnett@btbsecurity.com

W W W . B T B S E C U R I T Y . C O M