

Date: 23/07/2012 Procedure: Active Directory - Find All Locked Out Accounts Source: LINK Permalink: LINK Created by: HeelpBook Staff Document Version: 1.0

Active Directory - Find All Locked Out Accounts

Use Saved Queries to quickly locate all locked out user accounts.

You can use the **Saved Queries** feature of **Windows Server 2003** to query **Active Directory** for any locked-out accounts. Just open the **Active Directory Users and Computers** console, right-click on **Saved Queries** in the console tree and select **New** –> **Query**.

• Type a name and description for the query, specify a query root (where in your namespace your query begins searching), and click the **Define Query** button.

Since there's no default option for finding locked-out accounts in the Common Queries box, select Custom
 Search instead to open the Find Custom Search box.

• Then select the **Advanced** tab and enter the following **LDAP** string in the **Enter LDAP Query** textbox:

(&(&(objectCategory=person)(objectClass=user)(lockoutTime:1.2.840.113556.1.4.804:=42949 67295))))

Click **OK** twice to create and run the saved query. The string works on **Windows Server 2003 SP1**.

Update: Here's another LDAP query that finds all locked out accounts:

(&(objectCategory=Person)(objectClass=User)(lockoutTime>=1))

SOLUTION (ALTERNATIVE) BY HEELPBBOOK STAFF

If none of these works you could try the following one, tested even on R2 releases:

```
(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=2)
)
```

Hope this helps!

Date: 23/07/2012 Total Chars: 1151

