



LockoutGuard Documentation

(The following graphics are screen shots from Microsoft® ISA Server 2006 which is the property of Microsoft Corp. and are included here for instructive use. Some images illustrate LockoutGuard, which is the property of Collective Software.)

Table of Contents

LockoutGuard Documentation.....	1
Preventing Denial of Service vector on Extranet.....	2
Problems.....	2
Solution.....	2
Features.....	2
Requirements.....	2
Caveats.....	3
Help is Available!.....	3
Installation of LockoutGuard.....	4
Install Procedure.....	4
Troubleshooting.....	4
Install rolls back (with red error message at the end).....	4
Frozen or hung install.....	4
Configuring ISA's LDAP settings.....	6
Troubleshooting LDAP configuration.....	7
Configuring a listener to use LockoutGuard.....	8
Invoking the properties tab.....	8
The lockout settings.....	10
Soft Lockout.....	10
Reset time.....	11
Testing the soft lockout.....	12
How to check and reset the bad password count.....	14
Filter licensing.....	16
Demo/Lab mode.....	17
Troubleshooting.....	17
Support for LockoutGuard.....	17

Preventing Denial of Service vector on Extranet

- Your organization uses ISA Server 2006 in a “reverse proxy” scenario for publishing an extranet.
- For security and identification, the extranet uses ISA Form authentication.
- To prevent brute force password guessing attacks, your Active Directory is configured to lock out accounts after several failed login attempts.

Problems

- Each failed authentication attempt at ISA counts in AD as a failed login.
- Therefore, it is trivial for a remote attacker to lock out any of your AD accounts if they know (or can guess) the login name. No further credentials or privilege is required for this attack.
- In severe cases this attack may represent a substantial remotely triggerable denial of service vulnerability in your network.

Solution

LockoutGuard from Collective Software augments the capabilities of ISA 2006 to allow a “soft lockout”.

Features

- LockoutGuard can be configured to start denying authentication attempts before the AD lockout limit is reached.
- This acts as an additional tier of “lockout security”, safely locking the account out of the extranet.
- During soft lockout of a user's account, password guessing on the extranet will fail since LockoutGuard is blocking authentication attempts for that account.
- Even during this soft lockout, the user account can still be logged in from inside your LAN, or over a VPN. Thus, the DoS potential is substantially controlled, with a minimum inconvenience.

Requirements

- ISA Server 2006
- ISA authenticates to Active Directory (either ISA is a domain member, or uses LDAP)
- Extranet uses ISA Form authentication, or Basic.
- ISA needs LDAP (or LDAP-S) access to domain controller(s).
- Microsoft .NET Framework version 2 should be installed on each ISA server.

Caveats

- If your group policy is not configured to reset the failed password count, then the soft lockout condition will remain in effect until:
 - The user authenticates locally or over a VPN, or
 - An administrator resets the user's failed password count

Help is Available!

We are always happy to help you get our software set up and working. If you have questions or need assistance understanding/configuring/testing a Collective product, you can get in touch with our support staff quickly and easily. For the most up-to-date information, please see our Support page at <http://www.collectivesoftware.com/Support/>

Installation of LockoutGuard

Install Procedure

1. Close the ISA management console if it's open.
2. Execute the LockoutGuard.msi file. This will stop your firewall service, install the filter and interface software, register the filter, and then re-start the firewall service.
3. If you are installing over a remote desktop session, keep in mind that when the firewall service stops and restarts your RDP connection may be frozen, dropped or timed out. If an error occurs during the installation and the firewall service cannot be restarted, you will need to access the console to troubleshoot further (see below).
4. You must run the installer on each ISA server in an array separately, so they will all have the filter files installed and registered.
5. If the installation completes with no errors, then you can proceed to the configuration section.

Troubleshooting

The installation normally completes without errors. However there are a few possible failure modes that can occur for this complex install process.

Install rolls back (with red error message at the end)

If you are presented with an error message on the final screen, then check out the application event log, which often will contain details on why the installation failed. The problem may be immediately solvable from this information, or you may need to work with Collective support for additional troubleshooting assistance.

Frozen or hung install

The installer tries to start the firewall service after it is done registering the filter components. In rare cases, everything may register properly but there could still be a problem preventing the firewall service from starting. In this situation, the installation may appear to hang on the "Starting services..." item. This is because it is trying repeatedly to start the service, and failing. In fact if you look at the application event log, you will see several errors from the firewall service as it tries to start. These messages may help identify the cause of the problem.

The install should eventually give up on starting the service, but it may take a long time. If necessary, you can expedite the rollback by going into the services control panel and setting the Microsoft Firewall service to Disabled temporarily (and applying that change). This will cause the installer to quickly give up, and it should then correctly roll back the installation while leaving the firewall service down. After this happens you can then re-enable and restart the firewall service.

This kind of problem should not normally occur, and will probably require additional

troubleshooting by Collective support. However if you are able to fix the problem you can re-run the install safely after completing this procedure.

Configuring ISA's LDAP settings

Note: Even if your ISA is a domain member, you still need to configure LDAP settings correctly to use LockoutGuard. This is because the filter must use an LDAP lookup to learn the current failed password count for the user who is trying to authenticate. (You *do not* need to change your authentication settings from LDAP to integrated, however.)

The settings can be found in:

Configuration -> General -> Specify RADIUS and LDAP servers -> LDAP tab

A thorough discussion on configuration of ISA's LDAP settings is beyond the scope of this guide. Please consult the ISA help and Microsoft support for more information.

The simplest configuration is when all authentication is done to one AD domain. Add an LDAP Server Set:

Add LDAP Server Set

LDAP server set name:

Define the Active Directory servers available for LDAP user authentication. Servers are queried in the order in which they are listed.

Name	Description
sandboxdc	sandboxdc

Type the Active Directory domain name (use the fully-qualified domain name):

Example: contoso.microsoft.com

Use Global Catalog (GC)
 Connect LDAP servers over secure connection

User credentials used to access Active Directory to verify user account status and change account passwords (optional):

User name:
Password:

- To prevent a single point of failure, add more than one server here. An LDAP server must always be reachable for LockoutGuard to function.
- Note that regardless of your “Global Catalog” setting here, LockoutGuard will always connect to the normal LDAP port, not the GC. This is because the Bad-Pwd-Count attribute is not available in the GC, so it is not useful to use that setting.
- If possible you should use “connect LDAP servers over secure connection” to prevent potential transmission of confidential login information.
- The user name and password is **not optional** when you are using

LockoutGuard; be sure to set them to a valid AD account. This is because the filter must do the lockout check *before* allowing ISA to authenticate the extranet user. Otherwise if we used the user's credentials for LDAP then it would count as an authentication attempt in Active Directory. That would defeat the function of LockoutGuard, which is to soft lockout before overrunning the domain's lockout count!

- Don't use a username here that has access to your extranet. In particular, don't be tempted to use *your own* account, and then test the filter with that same account; it won't work. Since ISA has the LDAP user's correct password, each time it tries to connect, its own bad password count will be reset to zero. Thus, the LDAP user you specify here can effectively *never* be locked out, since it is constantly authenticating successfully and getting reset to zero.

LockoutGuard will report errors in LDAP configuration by setting ISA alerts. The alerts tab is always the first place to check for any problems.

In this example, there is only one domain, so all authentication requests "*" are matched and sent to our only LDAP set "default".

The screenshot shows two configuration sections. The first section is titled "Define the sets of LDAP servers ISA Server will query to validate user credentials:". It contains a table with two columns: "LDAP Server Set" and "Servers". The table has one row with "default" in the first column and "sandboxdcq" in the second column.

LDAP Server Set	Servers
default	sandboxdcq

The second section is titled "Define the login expressions ISA Server will use to match the user login strings:". It contains a table with two columns: "Login Expression" and "LDAP Server Set". The table has one row with "*" in the first column and "default" in the second column.

Login Expression	LDAP Server Set
*	default

If you have more than one domain in your environment, you need to add more sets, and match them to various login expressions such as "domain2*", "[*@domain2fqdn.com](#)", etc...

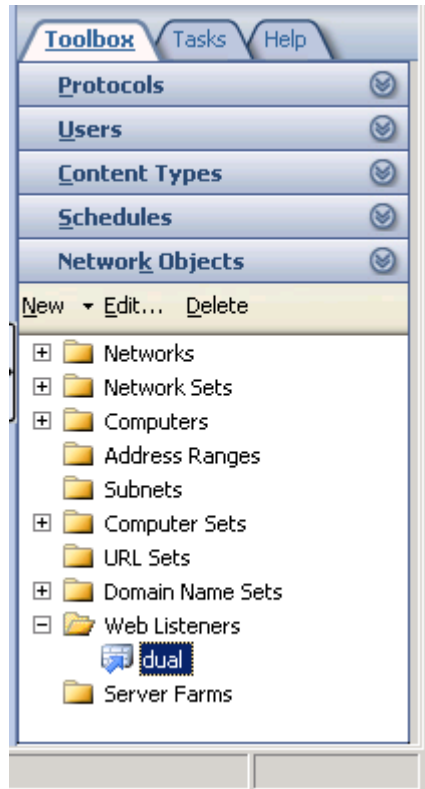
Troubleshooting LDAP configuration

- Check the credentials used. Use the support tool ldp.exe (or another LDAP browser) to bind to your DC over LDAP with that account, and try to look into the Users container or the OU where users exist. Make sure you can see their properties.
- Make sure ISA is allowed to send LDAP traffic to your DC. Do this by repeating the above test, but with the ldp.exe tool running from the ISA console
- If you have a 0x20 LDAP error, you may have set the FQDN of your directory incorrectly. This field is for the domain name, **not** the name of a single server.

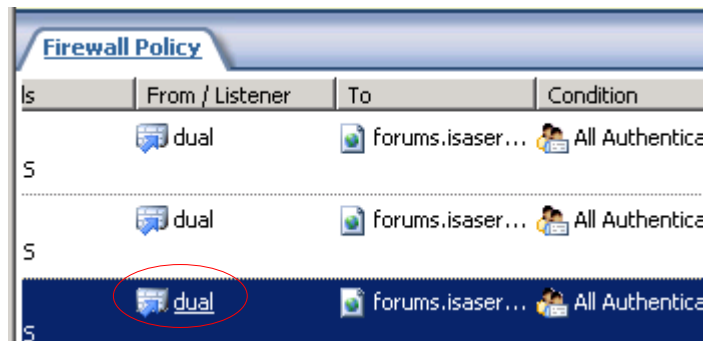
Configuring a listener to use LockoutGuard

Invoking the properties tab

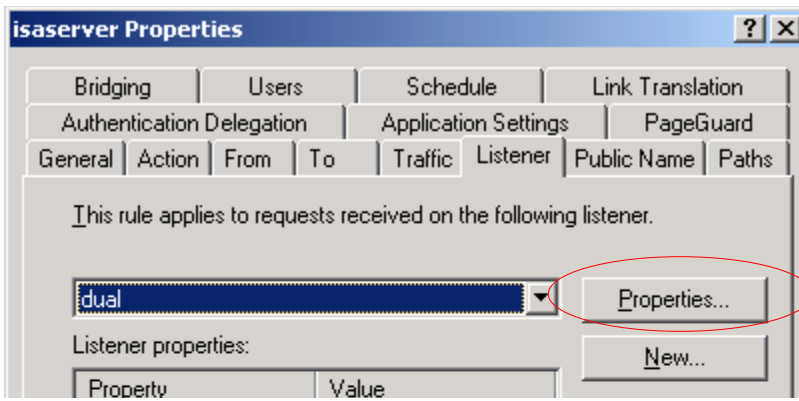
Due to a bug in the ISA console, custom tabs cannot be shown when the Listener dialog is opened this way. Instead, you **must** access the listener from the Toolbox area on the right:



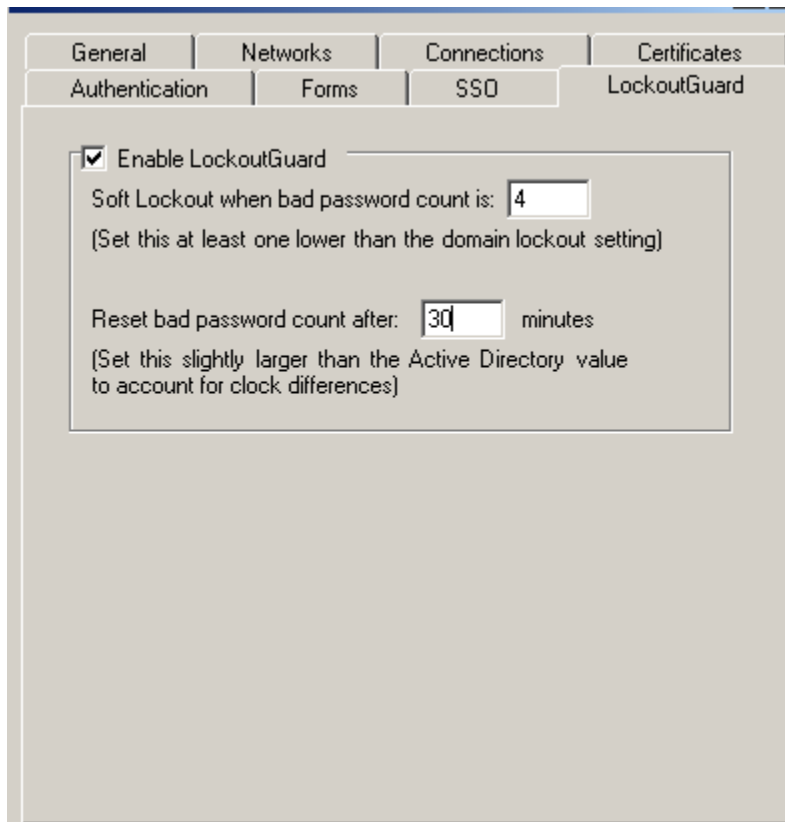
Note: If you do not see the “LockoutGuard” tab, it may be because you opened the Listener dialog by clicking here, in the web rule line:



Or here, in the rule dialog:



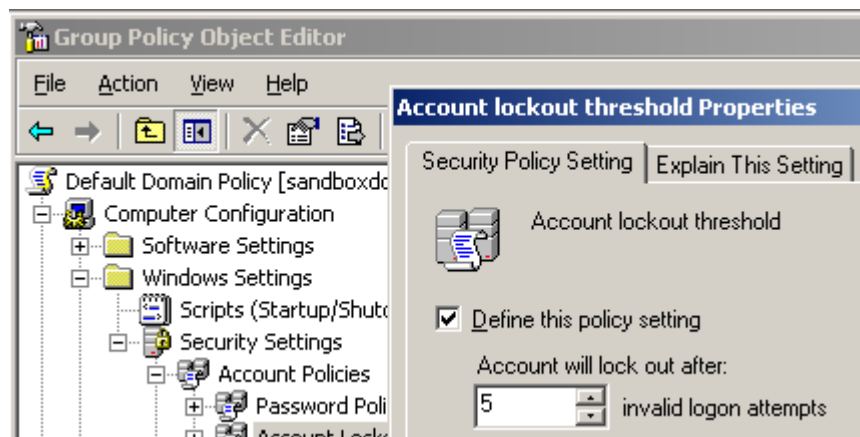
The lockout settings



LockoutGuard is configured separately for each Listener. Enable it for any listener that performs AD authentication and faces an insecure network.

Soft Lockout

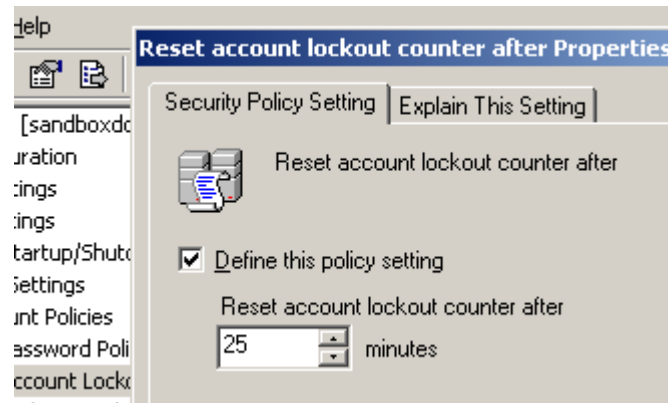
The “Soft Lockout” number is extremely important. Set this value to a smaller number than the AD lockout setting:



The difference between the two values is the number of attempts the account will “have left” during a soft lockout.

Reset time

LockoutGuard does not write changes to Active Directory's lockout counter, that value is managed internally by the domain controller. AD also maintains a reset value, in the following policy item:



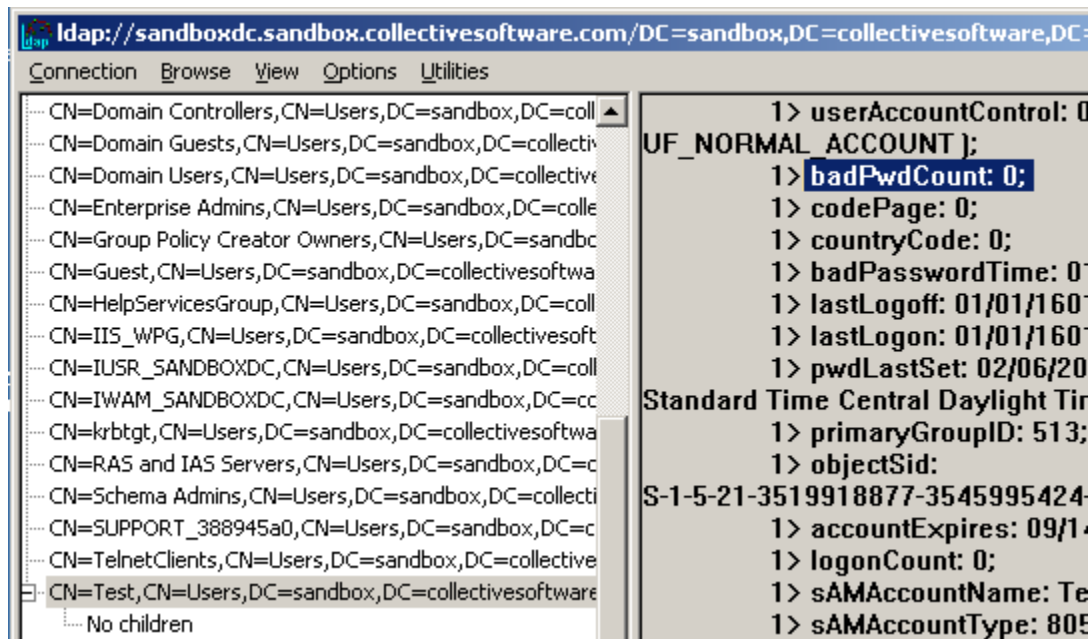
The domain controller does not *actively* reset the bad password count after this time passes, but instead waits for the next bad logon attempt to check the count. LockoutGuard must know how long the reset interval is, so it can make the proper decision about whether to send the authentication attempt to the DC or block it.

Since the clocks on ISA and the domain controllers may not be synchronized exactly, you **should specify a higher value** in the LockoutGuard settings than in AD, by 2-5 minutes. This mitigates the risk that LG will send the logon attempts through when the DC believes the old bad password count is still in effect. You should also ensure that the clocks on ISA and the domain controllers are not allowed to vary by more than this amount.

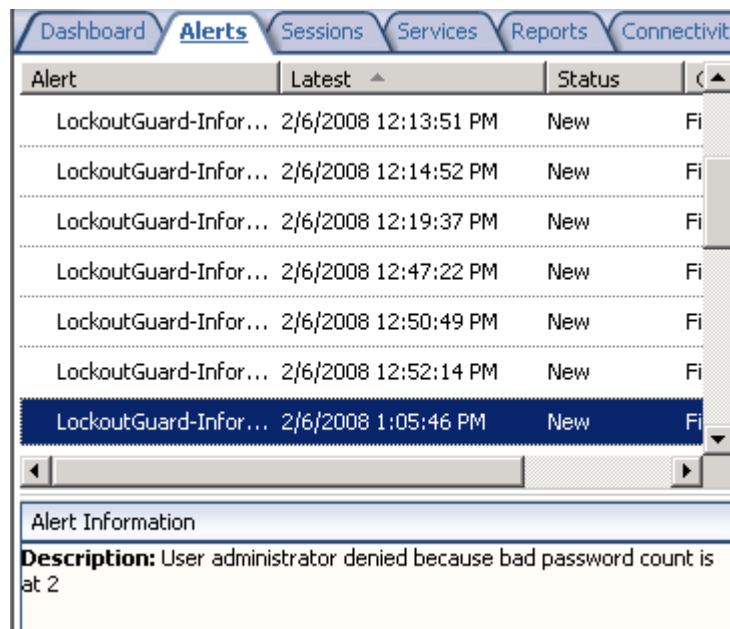
Note: Remember that during soft lockout, the user cannot authenticate to the extranet over this listener!

Testing the soft lockout

Each time you use a correct username but the wrong password, Active Directory will add 1 to the “badPwdCount” property of the user. You can see this in ldp.exe:



Once the account has accrued a bad password count equal to the soft lockout limit, it is considered to be in “soft lockout” mode. If another authentication attempt is made to that account, ISA will log an information-level alert:



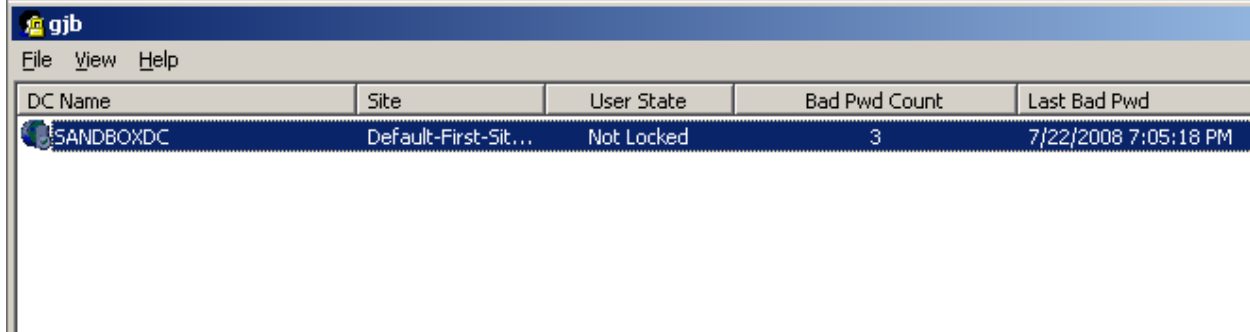
Just as with a normal lockout, even if the user enters their correct credentials to the extranet after this, they cannot log in. They must do one of the following:

- log in locally,
- log in on VPN,

- wait for AD to reset the lockout counter (if this policy is configured)
- Have the bad password count reset by an administrator user. (This can be done for example with an ADSI script, or by forcing the account to lockout, and then resetting the lockout via AD Users and Groups)

How to check and reset the bad password count

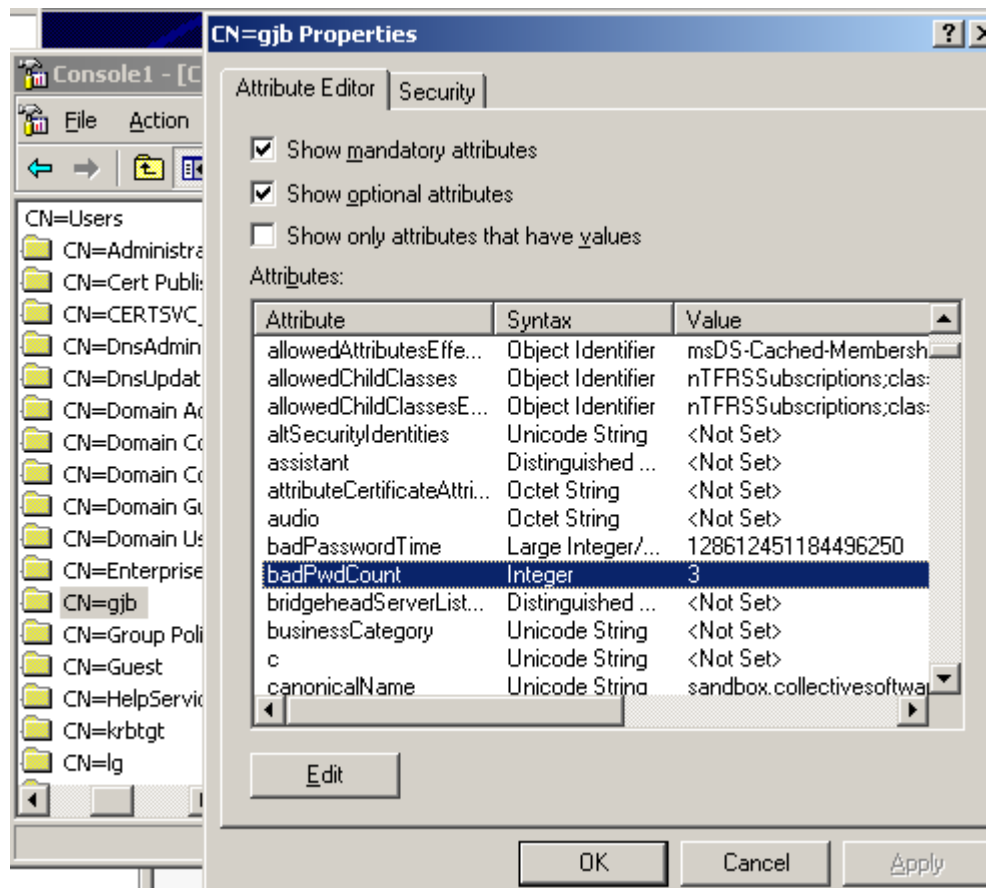
In addition to querying the LDAP value manually, as above, you can use a number of tools that add interfaces to display lockout information, including the free tool "LockoutStatus" provided by Microsoft.



DC Name	Site	User State	Bad Pwd Count	Last Bad Pwd
ESANDBOXDC	Default-First-Sit...	Not Locked	3	7/22/2008 7:05:18 PM

Note: AD does not actively reset the "Bad Pwd Count" value until the next bad logon attempt. Therefore, to determine the *effective* count, check the "Last Bad Pwd" column too. If it is a date/time that is older than the reset interval set in AD and LockoutGuard, then the effective count should be considered "0".

Clearing the bad password counter manually is not supported in the normal management interfaces, but if you have the Microsoft Support tools installed, you can use the "ADSI Edit" console to do this. The value to change is named "badPwdCount":



Console1 - [C:\...]

File Action

Attributes:

Attribute	Syntax	Value
allowedAttributesEffe...	Object Identifier	msDS-Cached-Membersh...
allowedChildClasses	Object Identifier	nTFRSSubscriptions;clas...
allowedChildClassesE...	Object Identifier	nTFRSSubscriptions;clas...
altSecurityIdentities	Unicode String	<Not Set>
assistant	Distinguished ...	<Not Set>
attributeCertificateAttri...	Octet String	<Not Set>
audio	Octet String	<Not Set>
badPasswordTime	Large Integer/...	128612451184496250
badPwdCount	Integer	3
bridgeheadServerList...	Distinguished ...	<Not Set>
businessCategory	Unicode String	<Not Set>
c	Unicode String	<Not Set>
canonicalName	Unicode Strin...	sandbox.collectivesoftwa...

Edit

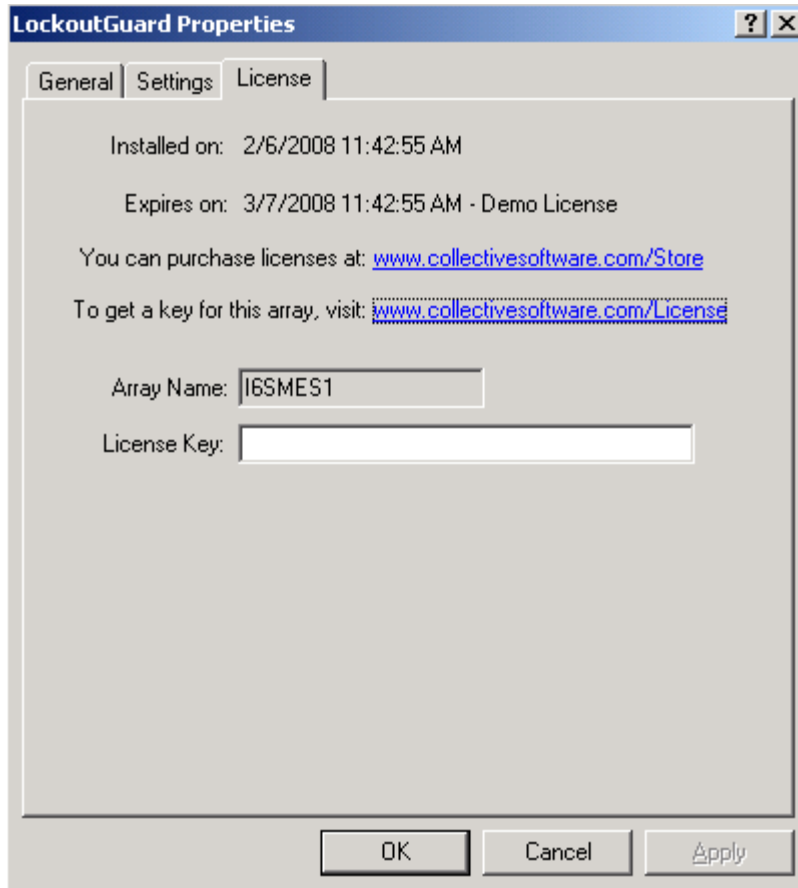
OK Cancel Apply

Information on installation of ADSI edit can be found [at Microsoft's site](#).

Filter licensing

To view your evaluation period or enter a key, go to Add-ins, Web Filters, and select LockoutGuard properties:

and select the License tab:



The License tab is used to check how long remains in the evaluation period, and to activate a permanent license.

To be eligible for a license key, you need to purchase license(s). You can do this on our [web store](#) or by [contacting us](#).

Once you have available license(s) you can request a key for your array (or single server) at our [licensing page](#). When requesting a license key, you will need to tell us the name of the ISA array, which is indicated on this dialog. The exact name is important, because it will be used to validate the key.

The license key is sensitive to the number of servers in the array. For example if you begin with only 2 servers in the array but plan to have 4, you can purchase 4 licenses and request a license key for a 4-server array. Then as you bring future servers online, they will be licensed automatically (you still need to [install the certificates](#) though.)

Warning: if you install more servers than you have licensed then the license key will be seen as invalid, and the servers will begin to operate in [demo/lab mode](#). So if you need to add more servers to a live array then you should acquire and apply your new license key in advance, so this behavior does not take place.

Demo/Lab mode

When the evaluation period expires (after 30 days) or when an invalid license key is used, the filter runs in demo/lab mode. In this mode the filter will work normally for a period of 2 hours from the starting of the Firewall Service, and then stop working after that time. This mode is meant to be useful for test labs where you don't wish to purchase licenses but still want to be able to run meaningful test setups. After 2 hours, you can restart the firewall service and the lab timer will reset again.

Troubleshooting

The first place to look if something seems to be working incorrectly is the ISA alerts tab in the Monitoring section. Often this will directly indicate the cause of the problem. This information will also be required in almost all cases if you need support.

Support for LockoutGuard

Collective is proud to offer support for LockoutGuard, whether you need help getting a configuration working, find a bug, or just have a feature question.

Support is available from our web site at <http://www.collectivesoftware.com/Support/>

- *Knowledge Base*: When our staff answers questions that will apply to the whole community, they will often create a permanent KB item to disseminate this knowledge. There is a Search feature here; you can also easily browse by topic. To get fast answers to FAQs (frequently asked questions) the knowledge base is the best place to start.
- *Support ticket*: We are always happy to help you get set up and working. If you have questions or need assistance understanding/configuring/testing a Collective product, you can get in touch with our support staff quickly and easily. For the most up-to-date information, please see our Support page.