LockoutGuard v1.2 Documentation

(The following graphics are screen shots from Microsoft® ISA Server and Threat Management Gateway which are 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

Preventing Denial of Service vector on Extranet

- Your organization uses ISA Server 2006 or Threat Management Gateway in a “reverse proxy” scenario for publishing an extranet.
- For security and identification, the extranet uses HTML Form authentication or HTTP Basic 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/TMG 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 and TMG 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 or Threat Management Gateway
- ISA/TMG authenticates to Active Directory (either ISA/TMG is a domain member, or uses LDAP)
- Extranet uses ISA/TMG HTML Form authentication, or Basic authentication.
- ISA/TMG needs LDAP (or LDAP-S) access to domain controller(s).
- Microsoft .NET Framework version 2 should be installed on each ISA/TMG 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/TMG 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/TMG 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.

How LockoutGuard works

Normal Active Directory Lockout behavior

When a lockout policy is configured on your domain, each AD domain controller maintains its own count of how many times a user has failed to log in recently, called the “bad password count”. These counters are not shared between DC’s.

Each time an incorrect logon password is supplied, whichever DC ISA/TMG is using will increment this count by one. Once the bad password count reaches the value configured in group policy, the user account becomes “locked out” on that domain controller, which means it cannot authenticate until the lockout duration expires.

How LockoutGuard imposes a “soft lockout”

LockoutGuard’s job is to watch the bad password counts (bpc) on each domain controller in the site (or whichever LDAP servers you have configured for authentication), and block login attempts from accounts whose bpc is over a certain threshold. Login attempts blocked by LockoutGuard will never reach the domain controller.

By making LockoutGuard’s threshold lower than the AD lockout threshold, we achieve a “soft lockout” where the user account can no longer authenticate to ISA/TMG, but the user account **can** authenticate on the LAN and to other services since it is not truly locked out of AD.

This maintains the same security benefits of AD lockout without causing as much inconvenience in the organization.

Configuring ISA/TMG authentication settings

Using AD authentication in a single domain

If your ISA/TMG is a domain member, your organization uses one flat domain, and you are using AD authentication (instead of LDAP), then you do not need to make any changes to your authentication settings.

LockoutGuard still uses LDAP to check the bad password count, since this is the only way the bad password count property is made available. But LockoutGuard will automatically find the domain controllers in your site, and poll them over LDAP.

Using AD authentication to multiple domains

If users from several domains will connect to ISA/TMG, you should set your listeners to use LDAP and **not** integrated AD, even if the firewall is a domain member. LockoutGuard must know what LDAP servers to connect to for various different domains in the forest. Global Catalog servers do not have lockout properties, so it is necessary to set up each domain explicitly in the LDAP settings.

If you continue to use AD authentication, LockoutGuard will not be able to find the records for users from other domains in your forest. This will cause errors and could compromise your lockout protection. So in summary, if you have multiple domains, don't use AD authentication with LockoutGuard, set it up as LDAP via the settings below.

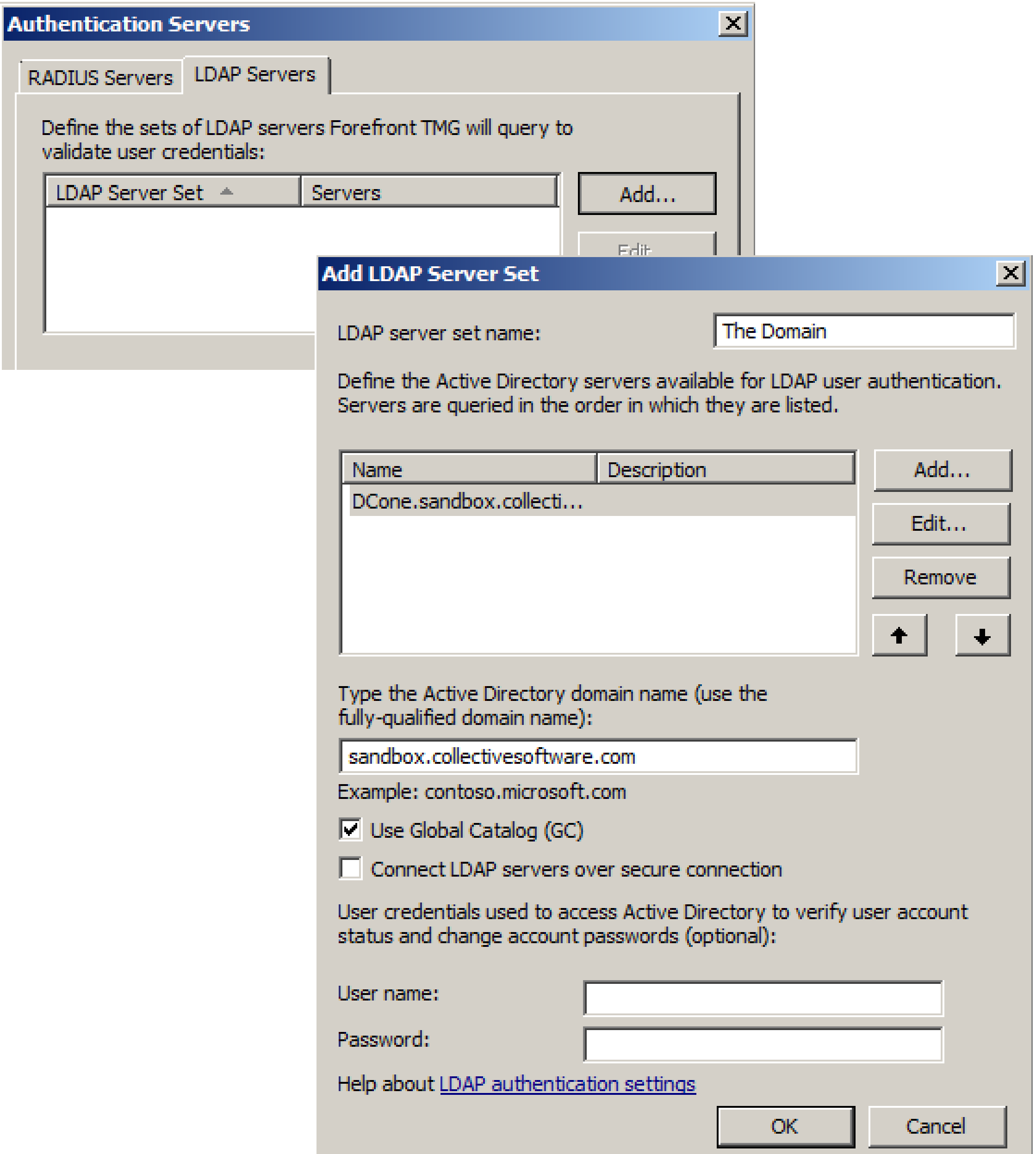
Using LDAP authentication

If your listeners are already set up to use LDAP authentication, then you do not need to make any changes.

If you are switching to LDAP instead of using AD integrated authentication, then you will need to tell the firewall how to contact your servers. Finding the LDAP settings:

- In ISA server, the LDAP server configuration is found under the "General" settings item.
- In TMG, go to the "Tasks" pane in the Firewall Policy section, and then select "Configure Authentication Server Settings"

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



Define the sets of LDAP servers Forefront TMG will query to validate user credentials:

LDAP server set name: The Domain

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

Name	Description
DCone.sandbox.collecti...	

Type the Active Directory domain name (use the fully-qualified domain name): sandbox.collectivesoftware.com

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):

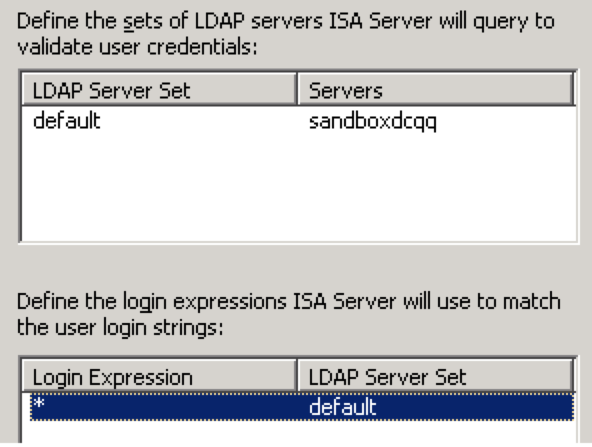
User name:

Password:

Help about LDAP authentication settings

- 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.
- Starting with LockoutGuard version 1.1, plain credentials are not sent over LDAP (only challenge/response is used) so it is not necessary to use the Secure connection setting.
- The user name and password can be left out if ISA/TMG is a domain member. The computer account will have sufficient permissions to perform LDAP lookups.
- The user name and password are **not optional** if ISA/TMG is a workgroup machine. Be sure to set them to a valid AD service account. This is because the filter must do the lockout check *before* allowing ISA/TMG 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/TMG 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.

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



Define the sets of LDAP servers ISA Server will query to validate user credentials:

LDAP Server Set	Servers
default	sandboxdcqq

Define the login expressions ISA Server will use to match the user login strings:

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

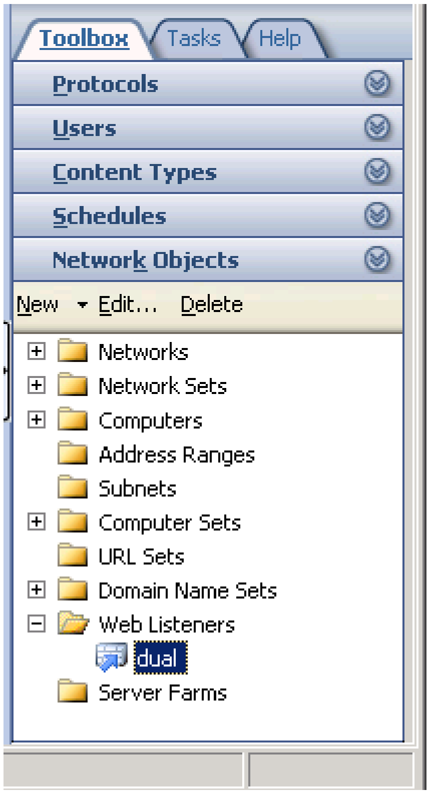
LockoutGuard will report errors in LDAP configuration by setting Alerts in the Monitoring section's Alerts tab. The alerts tab is always the first place to check for any problems.

- If this is a workgroup ISA/TMG, then check the service account 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/TMG 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 ISA/TMG is a domain member and you are using the ISA machine account for credentials, the previous test does not apply. To verify it's not a permissions problem, try connecting with ldp.exe from the ISA console, and binding with an AD user account.
- 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.

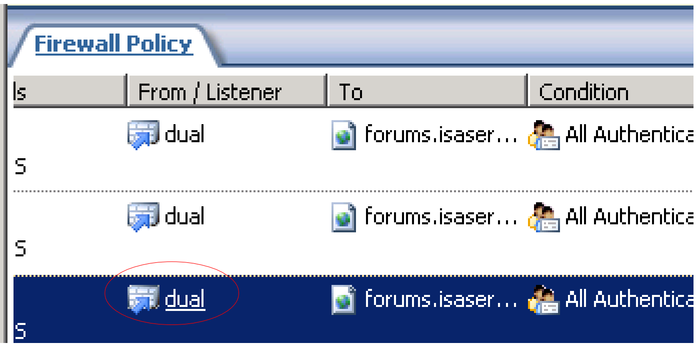
Configuring a listener to use LockoutGuard

Invoking the properties tab

Due to a design flaw in the ISA/TMG console, custom tabs cannot be shown when the Listener dialog is opened from within the firewall rule. Instead, you **must** access the listener from the Toolbox area on the right:

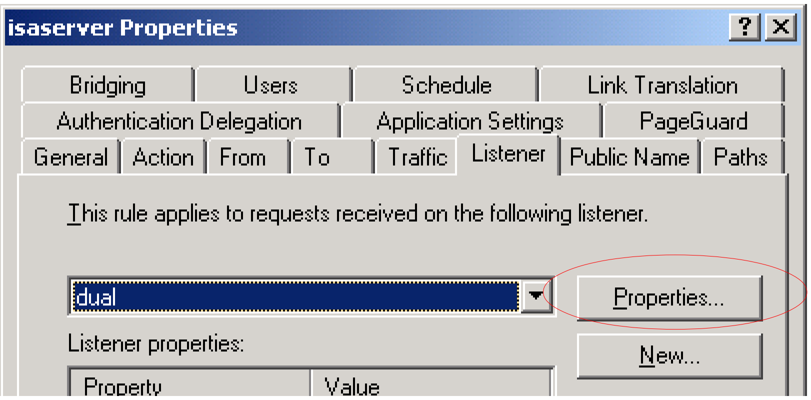


Note: If you do not see the “LockoutGuard” tab, it may be because you opened the Listener dialog by clicking here, in the web rule line:



ls	From / Listener	To	Condition
s	dual	forums.isaser…	All Authentica
s	dual	forums.isaser…	All Authentica
s	dual	forums.isaser…	All Authentica

Or here, in the rule dialog:



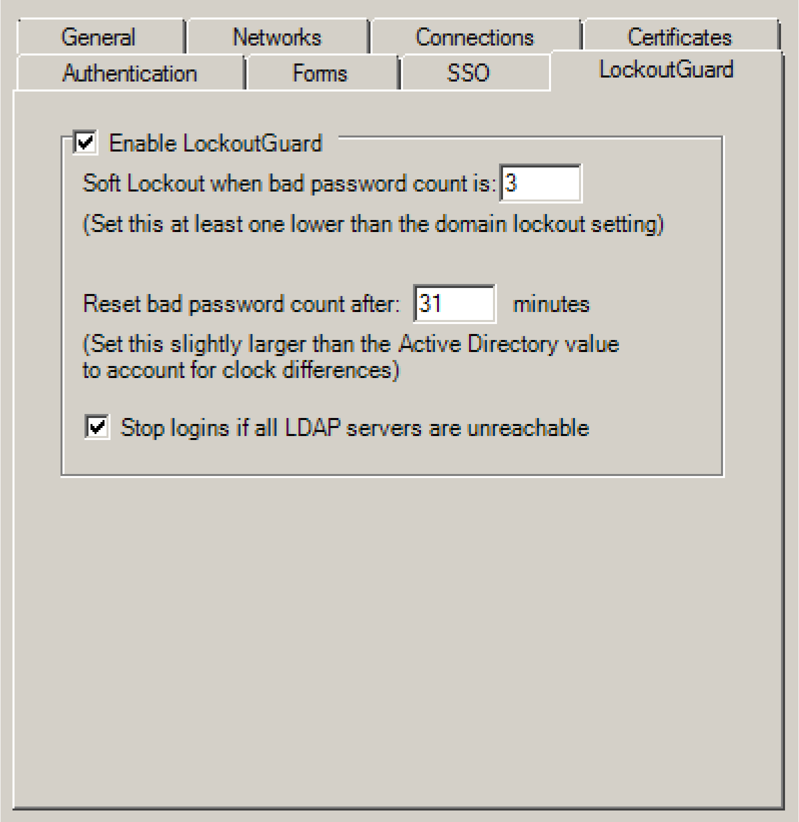
This rule applies to requests received on the following listener.

dual

Listener properties:

Property	Value

The lockout settings



☑ Enable LockoutGuard

Soft Lockout when bad password count is: 3

(Set this at least one lower than the domain lockout setting)

Reset bad password count after: 31 minutes

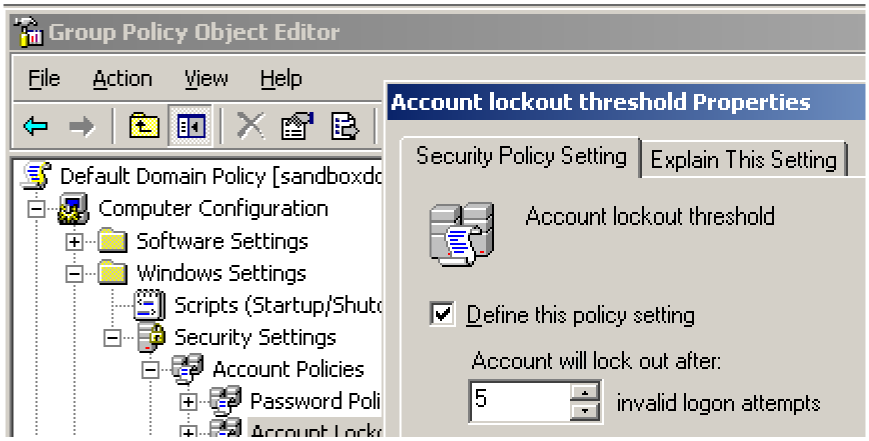
(Set this slightly larger than the Active Directory value to account for clock differences)

☑ Stop logins if all LDAP servers are unreachable

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:



☑ Define this policy setting

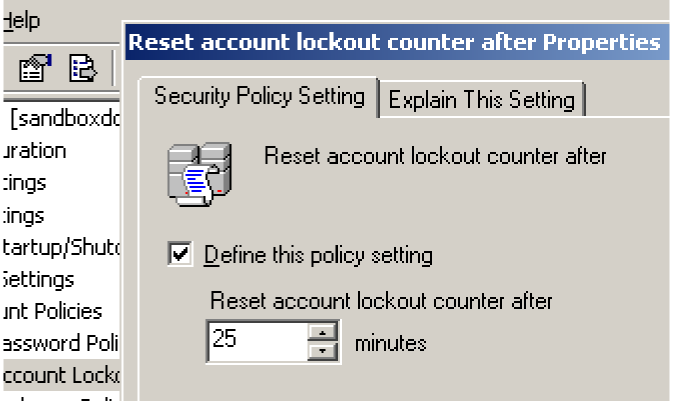
Account will lock out after:

5 invalid logon attempts

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:



☑ Define this policy setting

Reset account lockout counter after

25 minutes

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/TMG 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/TMG and the domain controllers are not allowed to vary by more than this amount.

Stop logins if all LDAP servers are unreachable

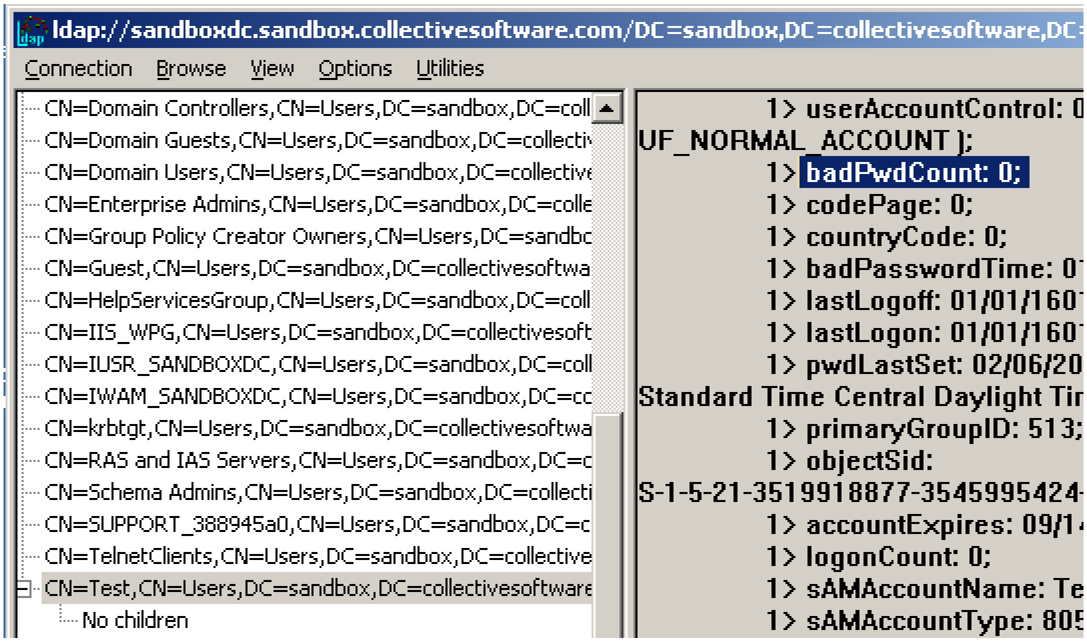
This setting determines what behavior the filter will have in the event that a configuration error or network problem prevents it from being able to check bad password counts. If you select this item, then LockoutGuard will block ALL logins when it is unable to contact any LDAP server.

Unless there are configuration errors or connection problems, then this setting generally won’t make any difference, because if the authentication servers are unreachable, then logins will fail whether LockoutGuard blocks them or not.

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

Testing the soft lockout

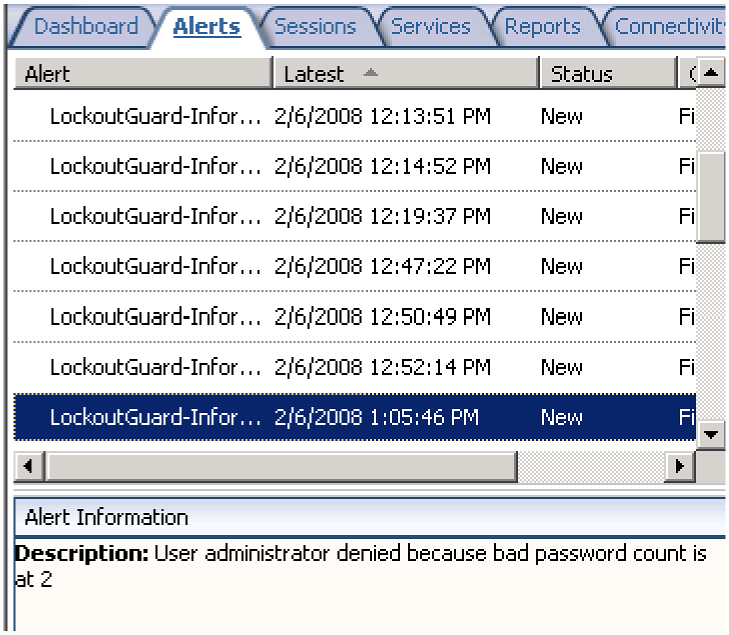
Each time you use a correct username but the wrong password, Active Directory will add 1 to the "badPwdCount" property of the user on whichever domain controller is used for the authentication. You can see this in ldp.exe:


ldap://sandboxdc.sandbox.collectivesoftware.com/DC=sandbox,DC=collectivesoftware,DC=
Connection
Browse
View
Options
Utilities

```
CN=Domain Controllers,CN=Users,DC=sandbox,DC=coll
CN=Domain Guests,CN=Users,DC=sandbox,DC=collecti
CN=Domain Users,CN=Users,DC=sandbox,DC=collective
CN=Enterprise Admins,CN=Users,DC=sandbox,DC=colle
CN=Group Policy Creator Owners,CN=Users,DC=sandbc
CN=Guest,CN=Users,DC=sandbox,DC=collectivesoftwa
CN=HelpServicesGroup,CN=Users,DC=sandbox,DC=coll
CN=IIS_WPG,CN=Users,DC=sandbox,DC=collectivesoft
CN=IUSR_SANDBOXDC,CN=Users,DC=sandbox,DC=coll
CN=IWAM_SANDBOXDC,CN=Users,DC=sandbox,DC=cc
CN=krbtgt,CN=Users,DC=sandbox,DC=collectivesoftwa
CN=RAS and IAS Servers,CN=Users,DC=sandbox,DC=c
CN=Schema Admins,CN=Users,DC=sandbox,DC=collecti
CN=SUPPORT_388945a0,CN=Users,DC=sandbox,DC=c
CN=TelnetClients,CN=Users,DC=sandbox,DC=collective
CN=Test,CN=Users,DC=sandbox,DC=collectivesoftware
    No children
```

```
        1> userAccountControl: 0
UF_NORMAL_ACCOUNT );
        1> badPwdCount: 0;
        1> codePage: 0;
        1> countryCode: 0;
        1> badPasswordTime: 0
        1> lastLogoff: 01/01/160
        1> lastLogon: 01/01/160
        1> pwdLastSet: 02/06/20
Standard Time Central Daylight Tir
        1> primaryGroupID: 513;
        1> objectSid:
S-1-5-21-3519918877-3545995424
        1> accountExpires: 09/1
        1> logonCount: 0;
        1> sAMAccountName: Te
        1> sAMAccountType: 805
```

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:



Alert	Latest	Status	C
LockoutGuard-Infor...	2/6/2008 12:13:51 PM	New	Fi
LockoutGuard-Infor...	2/6/2008 12:14:52 PM	New	Fi
LockoutGuard-Infor...	2/6/2008 12:19:37 PM	New	Fi
LockoutGuard-Infor...	2/6/2008 12:47:22 PM	New	Fi
LockoutGuard-Infor...	2/6/2008 12:50:49 PM	New	Fi
LockoutGuard-Infor...	2/6/2008 12:52:14 PM	New	Fi
LockoutGuard-Infor...	2/6/2008 1:05:46 PM	New	Fi

Alert Information

Description: User administrator denied because bad password count is at 2

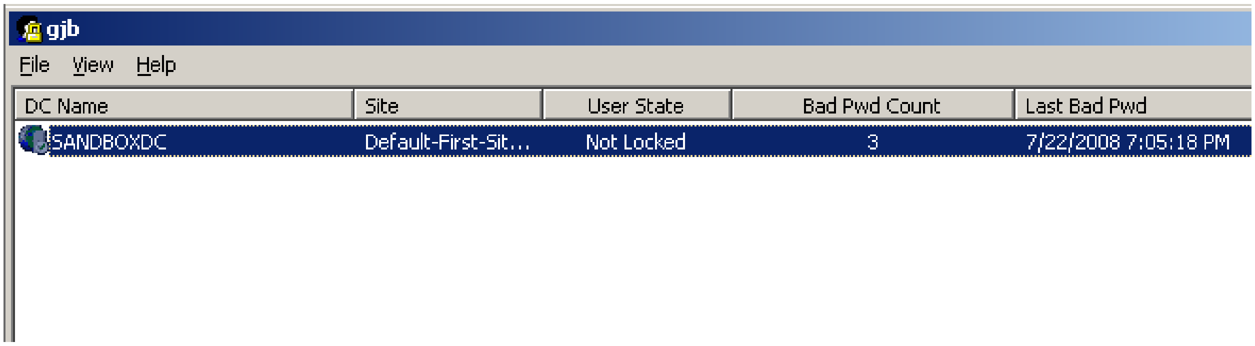
Just as with a normal lockout, even if the user enters their correct credentials to the extranet after this, they cannot log in. They must do one of the following:

- 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

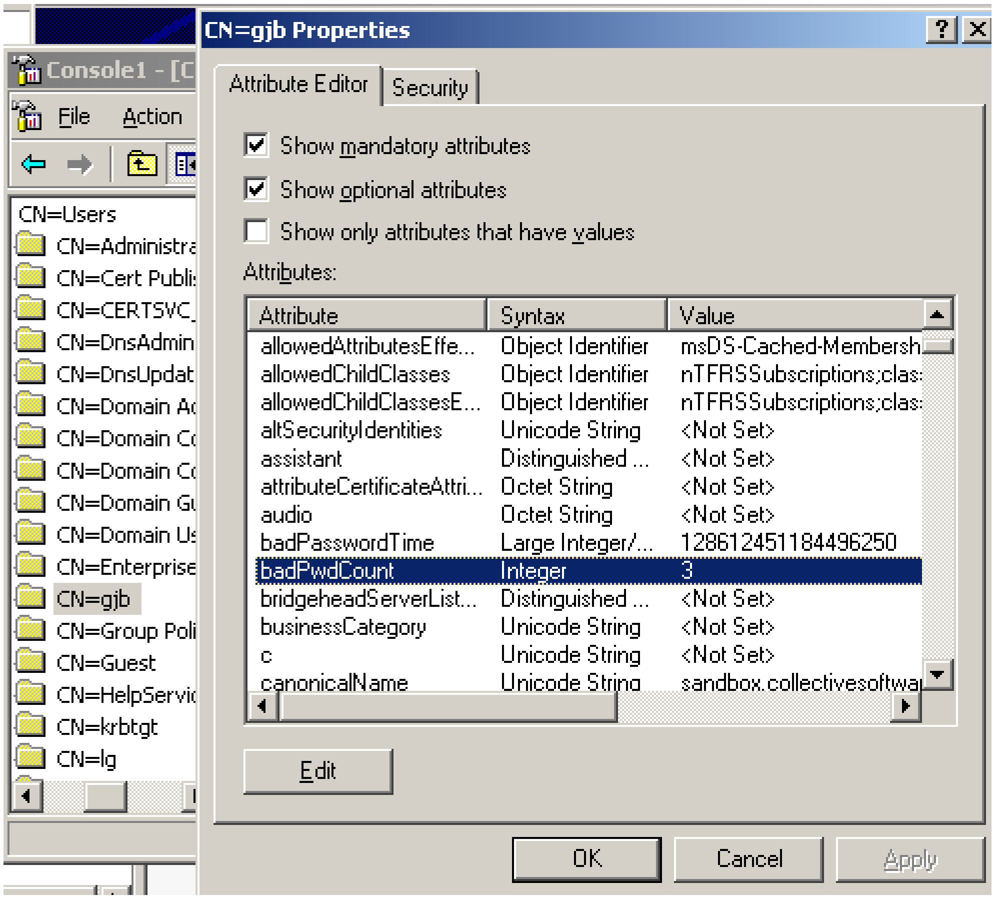
In addition to querying the LDAP value manually, as above, you can use a number of tools that add interfaces to display lockout information, including the free tool "LockoutStatus" provided by Microsoft.



DC Name	Site	User State	Bad Pwd Count	Last Bad Pwd
SANDBOXDC	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. To see how many bad login attempts have been recorded, see the "badPwdCount" property:



☑ Show mandatory attributes

☑ Show optional attributes

☐ Show only attributes that have values

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 String	sandbox.collectivesoftwa

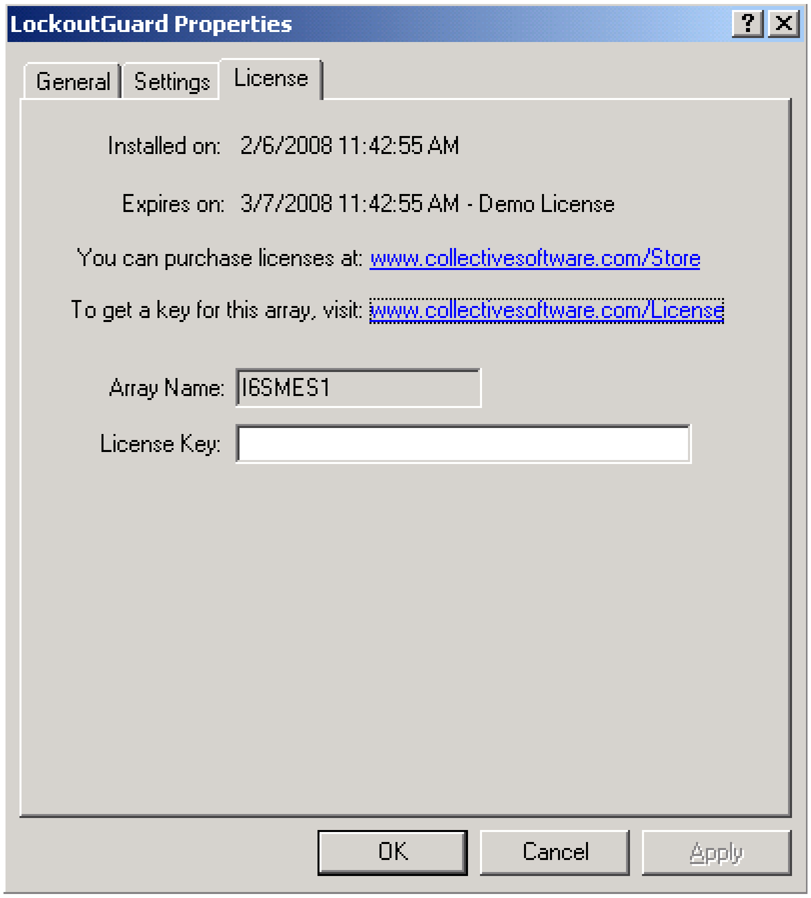
You cannot directly edit the badPwdCount value, however you can still *indirectly* clear it to zero. To do this, you set the value of a different attribute: "lockoutTime". Set that to "0" (even if it is already showing as zero) and you will see that badPwdCount is also reset. This is counter-intuitive, but it's the only way to reset the bad password count apart from waiting for the reset time interval.

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:



Installed on: 2/6/2008 11:42:55 AM

Expires on: 3/7/2008 11:42:55 AM - Demo License

You can purchase licenses at: www.collectivesoftware.com/Store

To get a key for this array, visit: www.collectivesoftware.com/License

Array Name: I6SMES1

License Key:

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/TMG 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 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.

Appendix A: Changes in LockoutGuard version 1.2

If you used LockoutGuard prior to version 1.2, there are several changes you should be apprised of that can affect your configuration and performance.

Configuration changes you should make

- If you are using integrated AD authentication, previous versions of LockoutGuard instructed you to create a set of ISA/TMG LDAP settings anyway. This is **no longer the case**. Unless you are using LDAP for authentication, you should **clear** any LDAP settings you may have added in the past for LockoutGuard.
- If there are no LDAP settings, the new filter version will automatically poll all the active DC's in the site.

Changes in filter operation

- The filter used to create an LDAP connection for each login request. It now maintains a persistent connection pool in order to decrease latency and load on the DC's.
- The old filter attempted to determine which DC the firewall service was using, and check the same one. This was necessary since the bad password count is not replicated. However it was not always possible to correctly match the server being used, which led to problems.
- The new version of the filter simultaneously checks all active DC's in the site (for integrated auth), or all LDAP servers you have configured (for LDAP auth). If any one of the servers' bad password count/times indicates the user should be soft locked out, the filter will do so. This means it should always get the correct answer instead of potentially polling the wrong server.
- Requests to each DC are sent in parallel, to decrease latency.
- The filter now maintains knowledge of which LDAP servers are not responding (i.e. "down"). It used to try each server in list order for every request, which caused more server load and caused logins to fail when servers became unresponsive.