

Using HCL Domino Internet Lockout feature with SecurTrac

Find out how you can use SecurTrac to monitor the HCL Domino Internet Lockout feature.

Background

HCL Domino Internet lockout helps to prevent brute force and dictionary attacks on user Internet accounts by locking out any user who fails to authenticate successfully within a preset number of attempts. Information about authentication failures and lockouts are maintained in the Internet Lockout application, where the administrator can clear failures and unlock user accounts as needed.

Starting with HCL Domino® 12, it is possible to also enforce lockouts for users who are not in the Domino Directory. Lockouts can also be triggered by IP addresses.

How Internet Lockout works:

- A) Internet Password Lockout is enabled in the Domino Directory within the Server Configuration document - Security tab.

Internet Lockout HCL Domino Server Configuration

Internet Lockout	
Enforce Internet Password Lockout:	Yes
<input checked="" type="checkbox"/> Also enforce lockout based on IP address	
<input checked="" type="checkbox"/> Count user name failures also as IP address failures	
Log Settings:	<input checked="" type="checkbox"/> Lockouts <input checked="" type="checkbox"/> Failures
Default Maximum Tries Allowed:	5
Default Lockout Expiration:	1 Hours
Default Maximum Tries Interval:	1 Days

- B) Having the Internet Lockout feature enabled ensures that when a user fails to authenticate with the correct user credentials, the following message will appear on the HCL Domino server console to warn Domino Administrators.

Internet Lockout HCL Domino Server Console notification – Failed Authentication

```
nHTTP: administrator [127.0.0.1] authentication failure using internet password
Server Server1/ExtracommDEV reported the following problem causing authentication to fail: Wrong Password.
```

- C) In addition to displaying a notification on the HCL Domino server console as seen above, a new record is also created in the inetlockout.nsf application database.

- D) In the following example, within inetlockout.nsf, it is shown that for one particular user, two records were created. One record relates to the person's user name and the other record relates to their IP Address. This logging behavior is followed when the "Count user name failures also as IP address failures" was enabled in the configuration. With this configuration, both user credentials and IP based authentication failures will be recorded separately.

Internet lockout events recorded in inetlockout.nsf

Server Name	User Name/IP Address	Locked Out	Failed Attempts	First Failure Time	Last Failure Time
▼ Server1/ExtracommDEV					
	127.0.0.1	No	1	05/11/2022 03:40:29 PM	05/11/2022 03:40:29 PM
	Administrator/ExtracommDEV	No	1	05/11/2022 03:40:29 PM	05/11/2022 03:40:29 PM

- E) When the same user has another failed authentication attempt, the "Failed Attempts" count is incremented. In the example below, the "Failed Attempts" count has been increased from 1 to 2.

"Failed Attempts" count incremented after another failed authentication attempt by the same user.

Server Name	User Name/IP Address	Locked Out	Failed Attempts	First Failure Time	Last Failure Time
▼ Server1/ExtracommDEV					
	127.0.0.1	No	2	05/11/2022 04:02:24 PM	05/11/2022 04:02:26 PM
	Administrator/ExtracommDEV	No	2	05/11/2022 04:02:24 PM	05/11/2022 04:02:26 PM

- F) At a point when the "Failed Attempts" count reaches the maximum threshold of 5, as defined in the Internet lockout configuration of the HCL Domino server, the account is then locked out as seen below.

Internet Lockout HCL Domino Server Console notification – User is Locked out

```
nHTTP: administrator [127.0.0.1] authentication failure using internet password
nHTTP: CN=Administrator/O=ExtracommDEV [127.0.0.1] has just been locked out via internet password lockout: User is locked out
```

- G) The corresponding user records will be marked as "Locked Out" in inetlockout.nsf

User Record now updated to reflect that the user account and IP Address are now "Locked Out"

Server Name	User Name/IP Address	Locked Out	Failed Attempts	First Failure Time	Last Failure Time
▼ Server1/ExtracommDEV					
	127.0.0.1	Yes	5	05/11/2022 03:40:29 PM	05/11/2022 03:42:19 PM
	Administrator/ExtracommDEV	Yes	5	05/11/2022 03:40:29 PM	05/11/2022 03:42:19 PM

- H) After an account has been "Locked Out", the account will no longer be permitted to authenticate and errors will appear on the HCL Domino server console as seen below.

Internet Lockout HCL Domino Server Console notification – Failed Authentication – User is locked out

```
nHTTP: CN=Administrator/O=ExtracommDEV [127.0.0.1] authentication failure using internet password: User is locked out
```

- l) When the user is locked out and tries to authenticate again, an error will appear in the user’s web browser as seen below:

Web Browser – User Locked Out notification



How to unlock an account that has been “Locked Out”:

- 1) To unlock an account, the corresponding user record(s) in the Internet Lockout database (inetlockout.nsf) must be deleted. The HCL Domino Administrator can manually delete the records in the database as seen below.

User Records for “Locked Out” Account flagged for Deletion/Unlock

A screenshot of the HCL Domino Administrator console. At the top, there are two buttons: 'Mark for Delete/Unlock' and 'Delete Marked Items', both of which are circled in red. Below the buttons is a table with the following columns: 'Server Name', 'User Name/IP Address', 'Locked Out', and 'Failed Attempts'. The table contains two rows of data under the 'Server1/ExtracommDEV' server. The first row has a checkmark in the left margin, '127.0.0.1' in the 'User Name/IP Address' column, 'Yes' in the 'Locked Out' column, and '5' in the 'Failed Attempts' column. The second row also has a checkmark in the left margin, 'Administrator/ExtracommDEV' in the 'User Name/IP Address' column, 'Yes' in the 'Locked Out' column, and '5' in the 'Failed Attempts' column.

	Server Name	User Name/IP Address	Locked Out	Failed Attempts
✓	Server1/ExtracommDEV	127.0.0.1	Yes	5
✓	Server1/ExtracommDEV	Administrator/ExtracommDEV	Yes	5

- 2) Alternatively, users can wait until the “Lockout Expiration” time period elapses. The “Lockout Expiration” can be set in the HCL Domino Server Configuration document.

Lockout Expiration Configuration

Internet Lockout	
Enforce Internet Password Lockout:	Yes
<input checked="" type="checkbox"/> Also enforce lockout based on IP address	
<input checked="" type="checkbox"/> Count user name failures also as IP address failures	
Log Settings:	<input checked="" type="checkbox"/> Lockouts <input checked="" type="checkbox"/> Failures
Default Maximum Tries Allowed:	5
Default Lockout Expiration:	1 Hours
Default Maximum Tries Interval:	1 Days

When the “**Lockout Expiration**” time period has elapsed, the Lockout record for a user will automatically be deleted by the http task, therefore allowing the user to attempt another authentication.

Remarks :

- Though the HCL Domino Internet Lockout feature provides a good mechanism to prevent brute force or dictionary attacks of Internet user accounts, it does have its limitations. The Internet lockout feature itself is also subject to Denial of Service (DoS) attacks. A DoS attack is one in which malicious users explicitly prevent legitimate users from using a service. In the case of Internet password lockout, legitimate Internet users could be prevented from authenticating with an HCL Domino server during a Denial of Service attack. This is where attackers intentionally cause repeated failed authentication attempts in order to overload the server and lockout users.
- Since “**Lockout Expiration**” provides the mechanism to automatically unlock accounts, this also provides a way for hackers to continue with brute force attacks on the user accounts.
- Both login failures and lockout logs are buried and scattered throughout in the Domino console log. As a result, it is difficult for Administrators to be alerted or perform investigations.
- When a manual or automatic unlock of a user account occurs, the action is not logged on the Domino server console, as the unlock event actually occurs within the inetlockout.nsf database. From a security standpoint, this makes it difficult to find out who performed the unlock action and when the action took place.
- When taking into the limitation noted above, an effective way to monitor login failures, lockout and unlock events is needed.

How can using SecurTrac help you?

SecurTrac's advanced monitoring features allows Domino Administrators to detect and collect information related to the following security event cases:

1. Log IP/user authentication failures.
2. Log IP/user lockout events.
3. Detect signs of brute force attacks (many authentication failures in a short period of time)
4. Detect signs of DoS attacks (many lockouts in a short period of time)
5. Log the specific critical details related to when an unlock account event is triggered.

Case #1 & 3: Log IP/user login failures and detect sign of brute force attacks:

- SecurTrac, through use of its powerful **Intrusion Detection Monitor – “Event to Match” and “Wording(s) to be matched”** configuration, SecurTrac can help identify brute force attacks when they happen.
- Since it is known that user and IP authentication failures generate a Domino console message with the text “<user> <IP> **AUTHENTICATION FAILURE USING INTERNET PASSWORD**”, SecurTrac can be easily configured to detect and look for that string of text in the Domino Console log and if the event occurs repeatedly within a specific time frame, SecurTrac will trigger an alert that is sent to notify the Administrator.

SecurTrac Intrusion Detection Monitor Configuration – Detect Authentication Failure

Intrusion Detection Monitor
Created: 07/06/2021 06:14:20 PM ZES

Basics | **Monitor** | Report | Administration

Intrusion Detection

This monitor will generate a detailed log when the system detects the selected event

Event to Match

Pre-defined Event

Event Description : HTTP - Authentication failure

Wording(s) to be matched: * AUTHENTICATION FAILURE USING INTERNET PASSWORD

Email Notification

Mailing Address:

Importance: Normal
Delivery Priority: Normal

Customize E-mail Notification Message

Domino Event

Generate Domino Event

Bulk Action Detection

Enable Bulk Action Detection

Generate Bulk Action log if the above defined events occurred 10 times in 60 seconds

Send e-mail notification to:
Administrator/ExtracommDEV

- With SecurTrac’s bulk action detection feature, Administrators get notified immediately when there is sudden increase of authentication failures. This may be a sign that a brute force attack is taking place.
- With the SecurTrac Intrusion Detection Monitor configured, it will detect and capture all authentication failures on any Domino servers running SecurTrac. SecurTrac logs can also be stored in a centralized SecurTrac log database. This makes tracking, analyzing and sorting the SecurTrac logs a much more efficient process.

SecurTrac Logs showing authentication events captured by the SecurTrac – Intrusion Detection Monitor

	Time ^	Event ^	Details ^
Server1/ExtracommDEV	31		
07/08/2021	31		
	07/08/2021 03:38:22 PM	HTTP - Authentication failure	07/08/2021 03:38:22 PM nHTTP: administrator [127.0.0.1] authentication failure using internet password
	07/08/2021 03:38:28 PM	HTTP - Authentication failure	07/08/2021 03:38:28 PM nHTTP: admin [127.0.0.1] authentication failure using internet password
	07/08/2021 03:38:34 PM	HTTP - Authentication failure	07/08/2021 03:38:34 PM nHTTP: admin [127.0.0.1] authentication failure using internet password
	07/08/2021 03:38:39 PM	HTTP - Authentication failure	07/08/2021 03:38:39 PM nHTTP: admin [127.0.0.1] authentication failure using internet password
	07/08/2021 03:38:44 PM	HTTP - Authentication failure	07/08/2021 03:38:44 PM nHTTP: admin [127.0.0.1] authentication failure using internet password
	07/08/2021 03:38:44 PM	HTTP - User/IP address has just been locked out	07/08/2021 03:38:44 PM nHTTP: IP Address [127.0.0.1] has just been locked out via internet password lockout: User is locked out
	07/08/2021 03:43:16 PM	HTTP - Authentication failure	07/08/2021 03:43:16 PM nHTTP: IP Address [127.0.0.1] authentication failure using internet password: User is locked out
	07/08/2021 04:14:30 PM	HTTP - Authentication failure	07/08/2021 04:14:30 PM nHTTP: administrator [127.0.0.1] authentication failure using internet password
	07/08/2021 04:14:38 PM	HTTP - Authentication failure	07/08/2021 04:14:38 PM nHTTP: administrator [127.0.0.1] authentication failure using internet password
	07/08/2021 04:14:44 PM	HTTP - Authentication failure	07/08/2021 04:14:44 PM nHTTP: administrator [127.0.0.1] authentication failure using internet password
	07/08/2021 04:14:49 PM	HTTP - Authentication failure	07/08/2021 04:14:49 PM nHTTP: administrator [127.0.0.1] authentication failure using internet password
	07/08/2021 04:14:55 PM	HTTP - Authentication failure	07/08/2021 04:14:55 PM nHTTP: administrator [127.0.0.1] authentication failure using internet password
	07/08/2021 04:14:55 PM	HTTP - User/IP address has just been locked out	07/08/2021 04:14:55 PM nHTTP: CN=Administrator/O=ExtracommDEV [127.0.0.1] has just been locked out via internet password lockout: User is locked out
	07/08/2021 04:14:55 PM	HTTP - User/IP address has just been locked out	07/08/2021 04:14:55 PM nHTTP: IP Address [127.0.0.1] has just been locked out via internet password lockout: User is locked out
	07/08/2021 04:15:01 PM	HTTP - Authentication failure	07/08/2021 04:15:01 PM nHTTP: CN=Administrator/O=ExtracommDEV [127.0.0.1] authentication failure using internet password: User is locked out
	07/08/2021 04:26:59 PM	HTTP - Authentication failure	07/08/2021 04:26:59 PM nHTTP: administrator [127.0.0.1] authentication failure using internet password
	07/08/2021 04:27:04 PM	HTTP - Authentication failure	07/08/2021 04:27:04 PM nHTTP: administrator [127.0.0.1] authentication failure using internet password
	07/08/2021 04:27:09 PM	HTTP - Authentication failure	07/08/2021 04:27:09 PM nHTTP: administrator [127.0.0.1] authentication failure using internet password

Case #2 & 4: Log IP/user lockouts and detect sign of DoS attacks:

- SecurTrac can also monitor this type of activity through use of its powerful **Intrusion Detection Monitor** – “**Event to Match**” and “**Wording(s) to be matched**” configuration.
- Since it is known that when a user account is locked out, the action generates a Domino console message with `<user> <IP> HAS JUST BEEN LOCKED OUT VIA INTERNET PASSWORD LOCKOUT: USER IS LOCKED OUT`”, SecurTrac can be easily configured to detect and look for that string of text in the Domino Console log and if the event occurs repeatedly within a specific time frame, SecurTrac will trigger an alert that is sent to notify the Administrator.
- With SecurTrac’s bulk action detection feature, get notified immediately when there is a sudden increase in the number of account lockouts. This may evidence that DoS attacks are taking place.

SecurTrac Intrusion Detection Monitor Configuration – Detect Account Lockouts

Intrusion Detection Monitor
Created: 07/08/2021 03:36:14 PM ZE8

Basics | Monitor | Report | Administration

Intrusion Detection

This monitor will generate a detailed log when the system detects the selected event

Event to Match

Pre-defined Event

Event Description : HTTP - User/IP address has just been locked out

Wording(s) to be matched: * HAS JUST BEEN LOCKED OUT VIA INTERNET PASSWORD LOCKOUT: USER IS LOCKED OUT

Email Notification

Mailing Address:

Importance: Normal
Delivery Priority: Normal

Customize E-mail Notification Message

Domino Event

Generate Domino Event

Bulk Action Detection

Enable Bulk Action Detection

Generate Bulk Action log if the above defined events occurred times in seconds

Send e-mail notification to:
Administrator/ExtracommDEV

Case #5: Details of account unlock events:

- With audit trails a standard requirement by most I.T. Security departments, SecurTrac can provide exactly just what they are looking for. In this example, we reveal how SecurTrac can be used to capture full details as it relates to user account unlock events.
- This is accomplished by leveraging the extensive feature set provided through the SecurTrac - Database Monitor. First start by specifying that SecurTrac should monitor the **inetlockout.nsf** application database, as seen below.

SecurTrac – Database Monitor for inetlockout.nsf

The screenshot shows the 'Database Monitor' configuration page in SecurTrac. The page title is 'Database Monitor' with a creation timestamp of '07/08/2021 04:08:08 PM ZE8'. There are four tabs: 'Basics', 'Monitor', 'Report', and 'Administration', with 'Basics' selected. The main configuration area is divided into three sections:

- Database to Monitor:** Contains a 'File/Folder name' field with the value 'inetlockout.nsf' and an empty 'Exclude File(s)/Folder name(s):' field.
- People to Monitor:** Includes a text area for 'Monitor the following people's action only: (e.g. User1/Extracomm, */Extracomm, GroupA)'. The 'People:' field contains an asterisk '*'. There is an unchecked checkbox for 'AND the people are using Full Access Administration privilege'.
- Server(s):** Features two radio buttons: 'All in the domain' (which is selected) and 'Only the following:'.
- Description:** Contains a 'Description (Optional):' field with the text 'User has been unlocked'.

- As we've established that the Internet Lockout feature and the process of unlocking a user account involves deleting the user record document from the **inetlockout.nsf** application database, SecurTrac should be configured to monitor for when the "**Delete**" action of the user record document is detected.

SecurTrac – Database Monitor Delete Action

Database Monitor
Created: 07/08/2021 04:08:08 PM ZE8

Basics | **Monitor** | Report | Administration

Document | Design | ACL | Agent

Document

This monitor will generate a detailed log when a user performs a selected action and the document matches the criteria.

Action

Select the action to log:

Open Create Update Delete

Criteria to Match

Specify criteria by using: Formula Editor Formula Wizard

Log if formula is true

ILLockedOut = 1

Any the following fields are changed. (This option applies to the Update action only.)

- Once configured, SecurTrac will now create a log whenever a user account is unlocked. SecurTrac can log both automatic unlocks performed by the server and manual unlocks performed by an individual.
- When a user account is manually unlocked by an Administrator, the SecurTrac log will show the Initiator’s user name and that the related service used was nserver.

SecurTrac Log - Manual unlock of a user account

Action Details	
Initiator :	Administrator/ExtracommDEV
Database Title:	Internet Password Lockout (12)
Form :	UserLogin
Document ID :	OFB8F5976E.8CCF8A87-ON4825870C.002D45E8
Triggered by Monitor :	Log user unlock
Time :	07/08/2021 04:23:27 PM ZE8
Database Path:	inetlockout.nsf
Action :	Delete (Hard)
Is From Replication:	No
Used Full Access Admin privilege:	No

Connection Details	
Service :	nserver
Port Name :	ICPIP
Address :	127.0.0.1:51216

Document Details

Monitor Fields | RichText | Attachment

Field Name	Value
Form	UserLogin
ILAttempts	5
ILFirst Failure Time	07/08/2021 04:14:30 PM
ILLast Failure Time	07/08/2021 04:14:55 PM
ILLockedOut	1
ILServerName	CN=Server1/O=ExtracommDEV
ILUserName	127.0.0.1

- In instances where the account was automatically unlocked by the server, the SecurTrac log will show that the Initiator of the action was the server and identify that the related service is nhttp.

SecurTrac Log - Automatic unlock of user account

Action Details

Initiator :	Server1/ExtracommDEV	Time :	07/08/2021 04:33:59 PM ZE8
Database Title:	Internet Password Lockout (1Z)	Database Path:	inetlockout.nsf
Form :	UserLogin	Action :	Delete (Hard)
Document ID :	OF6EAC4C98:31F8A9A9-ON4825870C:002E6AC3	Is From Replication:	No
Triggered by Monitor :	User has been unlocked	Used Full Access Admin privilege:	No

Connection Details

Service :	nhttp	Address :	127.0.0.1
Port Name :			

Document Details

Monitor Fields | RichText | Attachment

Field Name	Value
Form	UserLogin
ILAttempts	5
ILFirst Failure Time	07/08/2021 04:26:59 PM
ILLast Failure Time	07/08/2021 04:27:20 PM
ILLockedOut	1
ILServerName	CN=Server1/O=ExtracommDEV
ILUserName	CN=Administrator/O=ExtracommDEV

Conclusion:

- The HCL Domino Internet Lockout feature provides both Administrators and I.T. Security teams an improved ability to enhance and maintain user account security in Domino environments. Its use can be further extended when paired with the powerful features provided by SecurTrac, like detecting and being notified immediately about user accounts being locked or unlocked or when potential brute force or DoS attacks might be happening in a Domino environment.
- To learn more about SecurTrac and other Extracomm products, please visit our web site: <http://www.etracomm.com>



Extracomm Inc.

1730 McPherson Court Unit 6

Pickering, Ontario

Canada, L1W 3E6

Tel: 905-709-8602

Fax: 905-709-8604

<http://www.extracomm.com>

Product names, logos, brands, and other trademarks featured or referred to within this document are the property of their respective trademark holders.