







Article

[John Murray](#) · Apr 24, 2017 1m read

Diagnosing the cause of <PROTECT> errors

If your application is raising <PROTECT> errors and you're finding it hard to work out why, here's a way to get additional information.

First, if auditing is not already enabled, turn it on:

 Home	Configuration »	Users	Enable Auditing
 DeepSee	Security »	Roles	Disable Auditing
 Ensemble	Licensing »	Resources	View Audit Database
 System Operation	Encryption »	Services	Configure System Events
 System Explorer	Enterprise Manager	Security Domains	Configure User Events
 System Administration		Applications »	Copy Audit Log
		SSL/TLS Configurations	Export Audit Log
		X.509 Credentials	Purge Audit Log
		OAuth 2.0 »	
		System Security »	
		Auditing »	
		Security Advisor	
		Mobile Phone	
		Public Key Infrastructure	

Then use "Configure System Events" (highlighted above) and locate the event named %System/%Security/Protect. In the screenshot below I used the Filter field to do this (type "protect" - highlighted below - and press TAB):

The following is a list of system audit events:

Filter: protect	Page size: 10	Max rows: 1000	Results: 1	Page: < << 1 >> > of 1
Event Name	Enabled	Total	Written	
%System/%Security/Protect	No	2	0	Reset Change Status

Notice that the Enabled column shows a value "No". By default <PROTECT> errors are not logged in the audit. So though my system has seen a total of 2 of the associated events, 0 have been written.

Use the "Change Status" link to toggle the Enabled value to "Yes".

Now do whatever causes your application to raise a <PROTECT> error.

Back in Portal, use the View Audit Database option and search for Protect events:

Menu Home | About | Help | Logout System > Security Management > View Audit Database

View Audit Database Server: **TIN** Namespace: **%SYS**
User: **UnknownUser** Licensed to: [REDACTED] Instance: **ENS171**

Event Source: *
Event Type: *
Event Name: **Protect**
System IDs: *
PIDs: *
Users: * (All), Admin, CSPSystem, johnm, SuperUser, UnknownUser
Authentications: * (All), Operating System, Password, Unauthenticated
Begin Date/Time: [REDACTED]
End Date/Time: [REDACTED]
Maximum Rows: 1000
[Reset Values](#) [Search](#)

Page size: 1000 Results: 1 Page: |< << **1** >> >| of 1

Time	Event Source	Event Type	Event	PID	CSP Session	User	Description	Details
2017-04-24 12:13:24.039	%System	%Security	Protect	2712		johnm	Attempt to access a protected global	

The Details link reveals more:

Audit Details

[Close](#)

Audit Details:

Description	Attempt to access a protected global
Timestamp	2017-04-24 12:13:24.039
UTCTimestamp	2017-04-24 11:13:24.039
Event Source	%System
Event Type	%Security
Event	Protect
Username	johnm
Pid	2712
JobId	131094
JobNumber	22
IP Address	127.0.0.1
Executable	
System ID	TIN:ENS171
Index	64
Roles	%Developer
Authentication	Password
Namespace	USER
Routine	
User Info	
O/S Username	johnm
Status	
Event Data	<PROTECT> ^Foo,c:\intersystems\ens171\mgr\ensdemo\

Afterwards you may want to put things back to how they were, disabling logging of %System/%Security/Protect events, and turning off auditing entirely if it wasn't previously enabled.

[#Caché](#) [#Ensemble](#) [#HealthShare](#) [#Tips & Tricks](#)

Source URL: <https://community.intersystems.com/post/diagnosing-cause-errors>