
Article

[Patrick Dunn](#) · Sep 29, 2020 4m read

Debugging “ Server Availability Error ” message when loading Web Application

In the WRC, we frequently see customers contact us because their Web Gateway is unable to serve web pages. This article will explain a frequent reason why these errors can occur, and explain some tools which can be used to debug the problem. This explanation is focused on the Web Gateway serving InterSystems IRIS instances, but the same explanation should apply to the CSP Gateway serving Caché instances as well.



The Problem:

Attempting to load a Web Application (either a custom application or the System Management Portal) results in one of the following errors (depending on your browser):

Web Gateway Version 2019.1.1.612.0

Server Availability Error

Server is currently unavailable

 HTTP 500 Internal Server Err... × 




The website cannot display the page

HTTP 500

Most likely causes:

- The website is under maintenance.
- The website has a programming error.

What you can try:

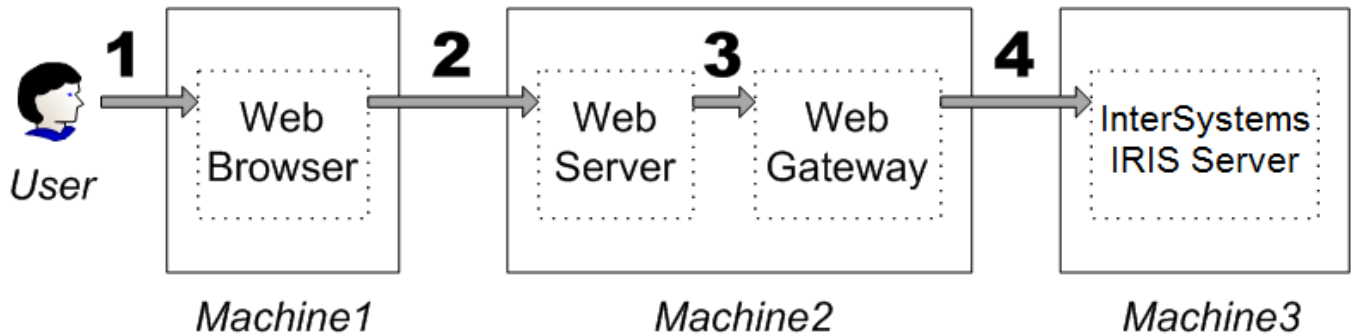
- Refresh the page.
- Go back to the previous page.
-  More information

In addition, the CSP.log file shows:

```
>>> Time: Thu May 21 11:55:07 2020; RT Build: 1901.1728 (linux/apapi:srv=2.4.6/apr=1.4.8/apu=1.5.2/mpm=prefork); Log-Level  
oFrcTjs9Ss; Remote-Addr: 172.16.62.165; Page: GET /csp/sys/UtilHome.csp  
Diagnostic  
Failed to connect to '20191' - Reason: 0 (Connection successfully made but server not responding) (No Retry)
```

Why this happens:

To understand why this happens, we need to take a look at the architecture which the Web Gateway functions in:



When you try to load your application in a browser, the browser sends a request to your Web Server. The Web Server passes this request off to the Web Gateway. The Web Gateway then has to reach out to InterSystems IRIS to understand what to do with the request. But given that the Web Gateway lives outside of InterSystems IRIS (and might be on another machine entirely), we require that the Web Gateway process authenticate to IRIS. This is the same as we would require for any other new processes connecting to IRIS, such as remote ODBC connections or a simple local IRIS Terminal Sessions.

The reason we are seeing the above errors when loading the application are because this authentication from the Web Gateway to IRIS is failing. The Web Gateway configuration stores within its CSP.ini file a set of credentials for each InterSystems IRIS server it connects to. Normally, these credentials are for the “ CSPSystem ” user, which is an account created by default when IRIS is installed. These credentials are then used to try and authenticate using the settings configured for the %ServiceWebGateway Service in IRIS.

To understand more information about why this authentication is failing, you can use the Audit capabilities offered by InterSystems IRIS. Given that you likely cannot use the Management Portal at this time, you can use the ^SECURITY routine in an IRIS Terminal Session in order to configure Auditing and view the Audit Log.

First off, you will need to Enable Auditing, if it has not already been enabled:

```
USER>zn "%SYS"

%SYS>d ^SECURITY

1) User setup
2) Role setup
3) Service setup
4) Resource setup
5) Application setup
6) Auditing setup
8) SSL configuration setup
9) Mobile phone service provider setup
10) OpenAM Identity Services setup
11) Encryption key setup
12) System parameter setup
13) X509 User setup
14) KMIP server setup
15) Exit

Option? 6

1) Enable auditing
2) Disable auditing
3) View system audit database
4) Configure auditing events
5) Manage audit logs
6) Exit

Option? 1

Enable auditing? No => yes
Freeze system on audit database error? No => No
Confirm changes? Yes => Yes
Auditing is enabled
```

Next, make sure that Auditing for the %System/%Login/LoginFailure Event is enabled:

```
%SYS>d ^SECURITY

1) User setup
2) Role setup
3) Service setup
4) Resource setup
5) Application setup
6) Auditing setup
8) SSL configuration setup
9) Mobile phone service provider setup
10) OpenAM Identity Services setup
11) Encryption key setup
12) System parameter setup
13) X509 User setup
14) KMIP server setup
15) Exit

Option? 6

1) Enable auditing
2) Disable auditing
3) View system audit database
4) Configure auditing events
5) Manage audit logs
6) Exit

Option? 4

1) Create audit event
2) Edit audit event
3) List audit events
4) Delete audit events
5) Reset audit event counters
6) Export audit events
7) Import audit events

Option? 2
Enter event source, type, and name as source/type/name

Event to edit? %System/%Login/LoginFailure
Enable auditing for event? No => yes
Confirm changes to Event %System/%Login/LoginFailure? Yes => Yes
Event %System/%Login/LoginFailure updated
Enter event source, type, and name as source/type/name
```

Once you ' ve done that, you can reproduce the “ Server Availability Error ” problem. This should result in a LoginFailure Audit Event being logged, and you can examine the details for this event to find out more:

```
Option? 6

1) Enable auditing
2) Disable auditing
3) View system audit database
4) Configure auditing events
5) Manage audit logs
6) Exit

Option? 3

1) Audit list
2) Audit list by event
3) Audit list by username
4) Audit list by pid
5) Exit

Option? 1
Users? * =>
Event Names? * =>
Event Types? * =>
Event Sources? * =>
System IDs? * =>
Pids? * =>
Groups? * =>
Beginning date and time? 2020-05-21 00:00:00 =>
Ending date and time? 2020-05-21 12:03:47 =>
Number of records to display? 20 =>
Num   Timestamp                Event Name                                Username
1     2020-05-21 12:03:35.969 %System/%Login/LoginFailure      CSPSystem
2     2020-05-21 12:01:47.844 %System/%Security/AuditChange   UnknownUser
3     2020-05-21 12:00:06.802 %System/%Security/AuditChange   UnknownUser
4     2020-05-21 11:58:47.152 %System/%Security/AuditChange   UnknownUser
Display detail of which record (0=End)?  => 1

Description:  %Service_WebGateway login failure
Timestamp:    2020-05-21 12:03:35.969   Username:    CSPSystem
UTCTimestamp: 2020-05-21 16:03:35.969   Pid:         36349
Event Source: %System                   JobId/JobNum: 65578/42
Event Type:   %Login                     Session ID:
Event:        LoginFailure                IPAddress:   127.0.0.1
System ID:    RH7-64-001:20191            Executable:  CSPap.so
Namespace:    %SYS                       Index:       4
Roles:
User Info:    Start CSP                   O/S User:    CSP Gateway
Routine:
Authentication: Password
Event Data:
Error message: ERROR #798: Password login failed
ERROR #952: Invalid password
Service name:  %Service_WebGateway
$I:            |TCP|51774|36349
$P:            |TCP|51774|36349
```

The “ Error message ” section should provide more information about why we are seeing the LoginFailure. Common problems include “ User CSPSystem is disabled ” or “ Service %Service_WebGateway is not

enabled for Password authentication ” , which suggest changes which should be made to the IRIS Security Settings.

The most common problem that we see in the WRC is that authentication is failing due to “ Invalid password ” . This means that the CSPSystem password stored in the Web Gateway does not match the CSPSystem password stored in IRIS.

How to fix the problem:

Now that the Audit Log entry gives you a clear indication of what the mismatch is between the Web Gateway and InterSystems IRIS, you have to fix that mismatch. The IRIS-side CSPSystem credentials can be modified through the ^SECURITY menu in a Terminal session.

There are a few ways to modify the CSPSystem credentials stored in the Web Gateway. The easiest way will be to access the Web Gateway Management Portal, which is documented here: <https://docs.intersystems.com/irislatest/csp/docbook/DocBook.UI.Page.cls?KEY=GCGloperconfig> Once you ’ ve loaded the Web Gateway Management Page, you can edit the credentials used to authenticate to IRIS by clicking the Server Access link, and editing the Connection Security settings for the relevant Server.

If you are not able to access the Web Gateway Management Page, then you are left with editing the CSP.ini file. The CSP.ini file should have sections for each Server Definition configured in the Web Gateway. You should be able to edit the “ Username ” and “ Password ” sections in the relevant section to match what is stored in InterSystems IRIS. Note that the [SYSTEM] section controls access to the Web Gateway Management Portal, not an InterSystems IRIS instance named [SYSTEM].

For example, if you have a definition to server “ Test ” where the CSPSystem password is incorrect:

```
[Test]
Ip_Address=192.168.2.100
TCP_Port=51774
Connection_Security_Level=0
Username=CSPSystem
Password=]]]AQAAANCmnd8BFdERjHoAwE/C1+sBAAAAOKaINtYnH0GE0tXD0jBvgQAAAAACAAAAAAQZgAAAAEAACAAAABmndMZIcc+3k2it+7umtIZa0EzLh0
```

You can edit the CSP.ini file to have the correct plaintext password:

```
[Test]
Ip_Address=192.168.2.100
TCP_Port=51774
Connection_Security_Level=0
Username=CSPSystem
Password=ActualPlaintextPassword
```

The next time you try to authenticate from the Web Gateway to InterSystems IRIS, the password will be encrypted:

```
[Test]
Ip_Address=192.168.2.100
TCP_Port=51774
Connection_Security_Level=0
Username=CSPSystem
Password=]]]AQAAANCmnd8BFdERjHoAwE/C1+sBAAAAOKaINtYnH0GE0tXD0jBvgQAAAAACAAAAAAQZgAAAAEAACAAACHTkLzHGg3hPoupYZtGI8RNUE/ESfTKG0vX18uuU1ql
```

[#CSP](#) [#Debugging](#) [#Web Gateway](#) [#InterSystems IRIS](#)

Source

URL:<https://community.intersystems.com/post/debugging-%E2%80%9Cserver-availability-error%E2%80%9D-message-when-loading-web-application>