

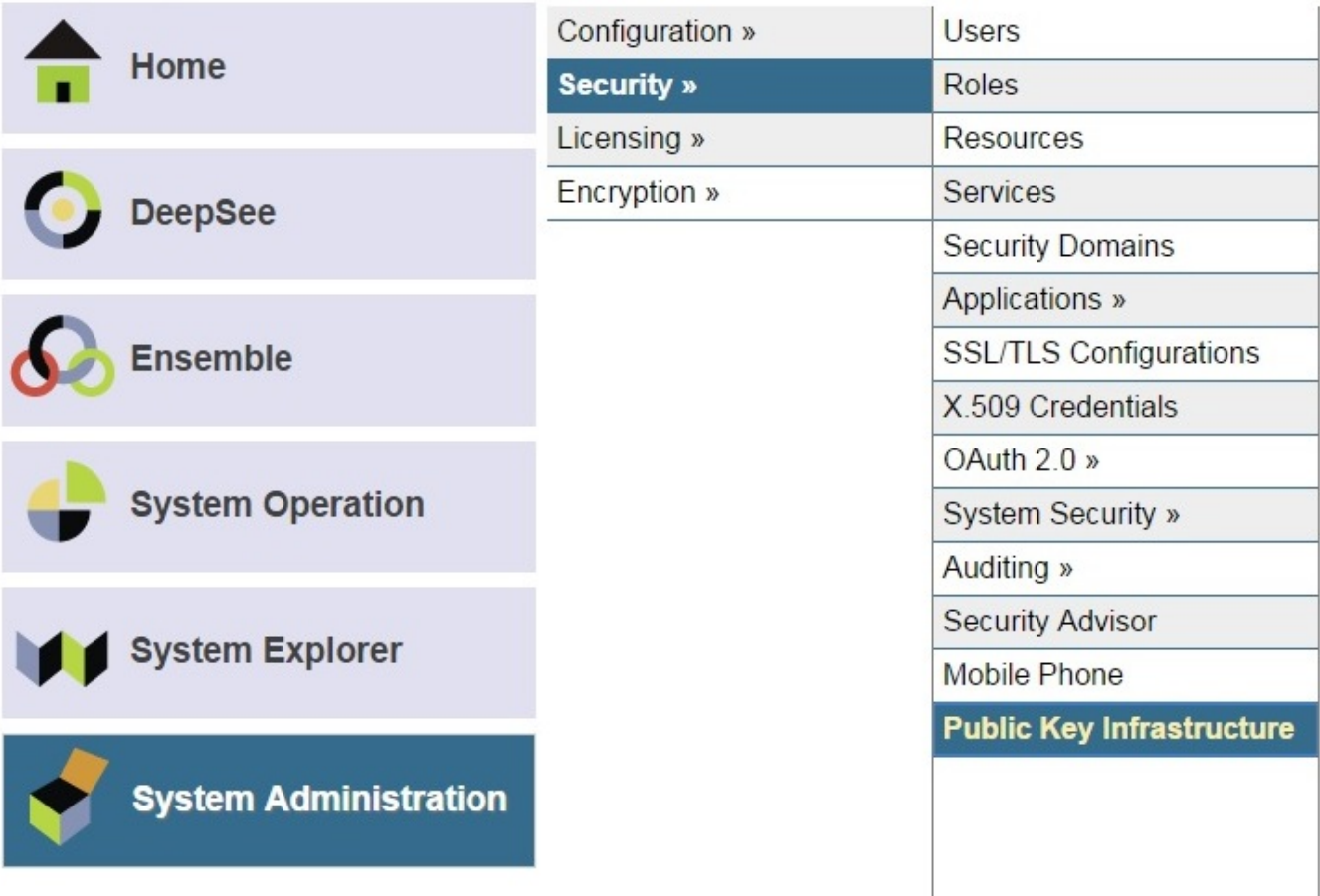
Article
[Pete Greskoff](#) · Jan 10, 2017 9m read

Creating SSL-Enabled Mirror Using Public Key Infrastructure (PKI)

In this post, I am going to detail how to set up a mirror using SSL, including generating the certificates and keys via the [Public Key Infrastructure](#) built in to Caché. The goal of this is to take you from new installations to a working mirror with SSL, including a primary, backup, and DR async member, along with a mirrored database. I will not go into security recommendations or restricting access to the files. This is meant to just simply get a mirror up and running. Example screenshots are taken on a 2016.1 version of Caché, so yours may look slightly different.

Step 1: Configure Certificate Authority (CA) Server

On one of your instances (in my case the one that will be the first mirror member configured), go to the System Management Portal and go to the [System Administration -> Security -> Public Key Infrastructure] page. Here you will 'Configure local Certificate Authority server'.



You can choose whatever File name root (this is the file name only, no path or extension) and Directory you want to have these files in. I ' ll use ' CAServer ' as the File name root, and the directory will be my <install-dir>/mgr/CAServer/. This will avoid future confusion when the client keys and certificates are put into the <install-dir>/mgr/ folder, as I ' ll be using my first mirror member as the CA Server. Go to the next page.

You will then need to enter a password, and I ' ll use ' serverpassword ' in my example. You can then assign attribute values for your Distinguished Name. I ' ll set Country to ' US ' and Common Name to ' CASrv '. You can accept defaults for validity periods, leave the email section blank, and save.

Configure local Certificate Authority server

| | | |
|---|------------------|---|
| Password to Certificate Authority's Private Key file | | |
| Confirm Password | | |
| Certificate Authority Subject Distinguished Name: | | |
| Attribute Type | Attribute Value | |
| Country | US | (Enter the two character country code only) |
| State or Province | | |
| Locality | | |
| Organization | | |
| Organizational Unit | | |
| Common Name | CASrv | |
| * Please enter at least one Attribute Value | | |
| Validity period for Certificate Authority's Certificate (days) | | 3650 |
| Validity period for Certificates issued by Certificate Authority (days) | | 365 |
| Configure email | | |
| SMTP server | SMTP username | |
| SMTP password | Confirm password | |
| Certificate Authority server administrator's email address | | |
| | | |
| Back | Save | Cancel |

You should see a message about files getting generated (.cer, .key, and .srl) in the directory you configured.

Step 2: Generate Key/Certificate For First Mirror Member

At this point, you need to generate the certificate and keys for the instance that will become your first mirror member. This time, go to the System Management Portal where you will set up the first mirror member, and go to the [System Administration -> Security -> Public Key Infrastructure] page again (see screenshot above). You need to 'Configure local Certificate Authority client'. For the 'Certificate Authority server hostname', you need to put either the machine name or IP address of the instance you used for step 1, and for the 'Certificate Authority WebServer port number' use that instance's web server port (you can get this from the URL in that instance's Management portal):

localhost57772/csp/sys/sec/%25CSP.UI.Portal.PKI.zen

Make sure you are using the port number for the instance you configured as the CA Server, not the one you are

setting up as the client (though they may be the same). You can put your own name as the technical contact (the phone number and email are optional) and save.

Now you should go to 'Submit Certificate Signing Request to Certificate Authority server'. You'll need a file name (I'm using 'MachineA_client') and password ('MachineApassword') as well as again setting values for a Distinguished Name (Country='US' and Common Name='MachineA'). Note that for each certificate you make, at least one of these values must be different than what was entered for the CA certificate. Otherwise, you may run into failures at a later step.

Submit Certificate Signing Request to Certificate Authority server

File name root for local Certificate and Private Key files (without extension)

Required. Valid characters: alphanumeric, hyphen or underscore.

Password for Private Key file
Confirm Password

Subject Distinguished Name:

| Attribute Type | Attribute Value |
|---------------------|---|
| Country | <input type="text" value="US"/> (Enter the two character country code only) |
| State or Province | <input type="text"/> |
| Locality | <input type="text"/> |
| Organization | <input type="text"/> |
| Organizational Unit | <input type="text"/> |
| Common Name | <input type="text" value="MachineA"/> |

* Please enter at least one Attribute Value

Certificate Signing Request MachineA_client successfully submitted to the Certificate Authority at instance PRIM on node WIN7-64-BAS-001.ISCINTERNAL.COM. SHA-1 Fingerprint: BC:F6:23:6B:01:11:64:EB:6D:C7:F1:90:08:67:76:26:42:6B:BE:D0

At this point, you'll need to go to the machine you configured to be your CA Server. From the same page, you need to 'Process pending Certificate Signing Requests'. You should see one like this:

Process pending Certificate Signing Requests

| Hostname | Instance | Filename |
|---------------------------------|----------|--|
| WIN7-64-BAS-001.ISCINTERNAL.COM | PRIM | MachineA_client Process Delete |

You should process this request, leaving default values, and ' Issue Certificate '. You ' ll need to enter your CA Server password from step 1 (' serverpassword ' for me).

Finally, you need to get the certificate. Back on the first mirror member machine, from the same page, go to ' Get Certificate(s) from Certificate Authority server ', and click ' Get ' like here:

Get Certificate(s) from Certificate Authority server

Get Certificate Authority Certificate

show certificates for this instance

Issued Certificates

| Serial Number | Hostname | Instance | Filename | |
|---------------|---------------------------------|----------|-----------------|----------------|
| 2 | WIN7-64-BAS-001.ISCINTERNAL.COM | PRIM | MachineA_client | <div>Get</div> |

You should then see a message indicating that the certificate was saved in the <install>/mgr/ directory of your instance.

Step 3: Configure The Mirror On First Mirror Member

First, start the ISCAgent per [this documentation](#) (and set it to start automatically on system startup if you don ' t want to have to do this every time your machine reboots).

Then, in the System Management Portal, go to the [System Administration -> Configuration -> Mirror Settings -> Enable Mirror Service] page to enable the service (if it isn ' t already enabled). Next, go to the ' Create a Mirror ' page in the same menu.

| | | | |
|--|-----------------|------------------------------|-----------------------|
| <div>Home</div> <div>DeepSee</div> <div>Ensemble</div> <div>System Operation</div> <div>System Explorer</div> <div>System Administration</div> | Configuration » | System Configuration » | Enable Mirror Service |
| | Security » | Connectivity » | Create a Mirror |
| | Licensing » | Mirror Settings » | Edit Mirror |
| | Encryption » | Database Backup » | Edit Async |
| | | CSP Gateway Management | Join as Failover |
| | | SQL and Object Settings » | Join as Async |
| | | Device Settings » | |
| | | National Language Settings » | |
| | | Zen Reports » | |
| | | Additional Settings » | |

You will need to enter a mirror name (' PKIMIRROR ' in my case). You should click ' Set up SSL/TLS ' , and then enter the information there. If this is not the same machine where you configured the CA Server, you ' ll need to get a copy of the CA Server certificate (' CA_Server.cer ') on this machine. You can do this in the ' Get Certificate(s) from Certificate Authority server ' page:

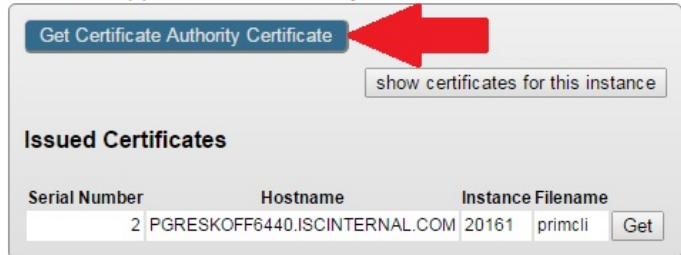
☐ Certificate Authority Client

- ▶ Submit Certificate Signing Request to Certificate Authority server
- ▶ Get Certificate(s) from Certificate Authority server
- ▶ Configure local Certificate Authority client

☐ Certificate Authority Server

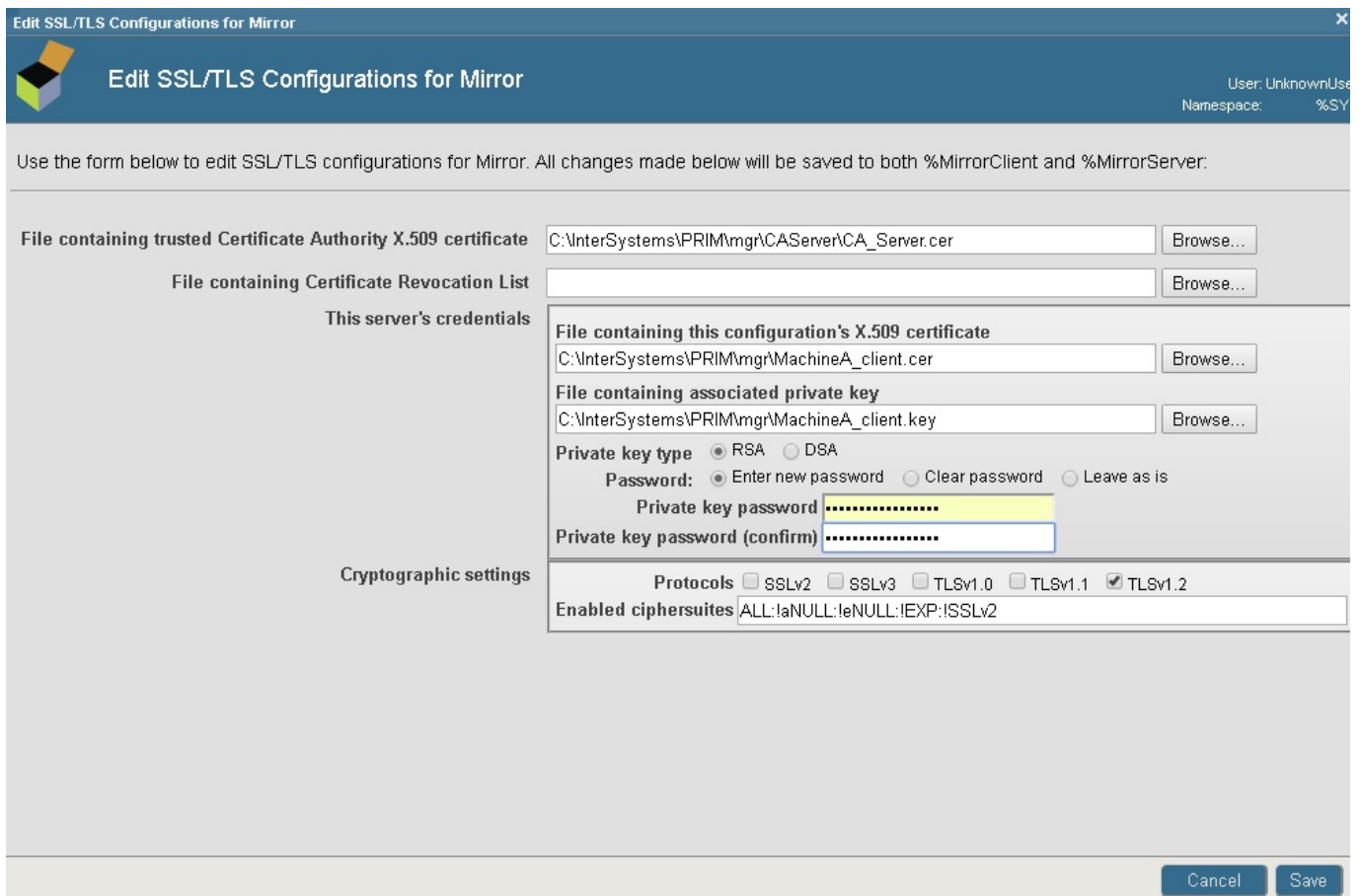
- ▶ Process pending Certificate Signing Requests
- ▶ Configure local Certificate Authority server

Get Certificate(s) from Certificate Authority server



| Serial Number | Hostname | Instance Filename |
|---------------|-------------------------------|-------------------|
| 2 | PGRESKOFF6440.ISCINTERNAL.COM | 20161.primcli |

Back in the ' Set up SSL/TLS ' page, the first line is asking for that CA server certificate. You should leave the ' Certificate Revocation list ' blank. If you want to use this, please contact the WRC. For ' This server ' s credentials ' , you ' ll need to enter the certificate and key that we generated in step 2. They will be in the <install>/mgr/ directory. You ' ll also need to enter your password here (click the ' Enter new password ' button as shown). This password is the one you chose in step 2 (' MachineApassword ' for me). In my example, I am only allowing TLS v1.2 protocol as shown below.



For this example, I won ' t use an arbiter or a Virtual IP, so you can un-check those boxes in the ' Create Mirror ' page. We ' ll accept the defaults for ' Compression ' , ' Mirror Member Name ' , and ' Mirror Agent Port ' (since I didn ' t configure the ISCAgent to be on a different port), but I ' m going to change the ' Superserver Address ' to use an IP instead of a host name (personal preference). Just make sure that the other future mirror members are able to reach this machine at the address you choose. Once you save this, take a look at the mirror monitor [System Operation -> Mirror Monitor]. It should look something like this:

This system is a failover member in mirror PKIMIRROR

Mirror Failover Member Information

| | This Failover Member | Other Failover Member |
|------------------------|----------------------|-----------------------|
| Mirror Member Name | WIN7-64-BAS-001/PRIM | n/a |
| Superserver Address | 192.168.2.100 | n/a |
| Mirror Private Address | 192.168.2.100 | n/a |

Arbiter Connection Status

| | |
|-------------------|---|
| Arbiter Address | Arbiter not configured |
| Failover Mode | Agent Controlled |
| Connection Status | This member is not connected to the arbiter |

Mirror Member Status

| Member Name | Member Type | Status | Journal Transfer | Dejournaling | X.509 DN |
|----------------------|-------------|---------|------------------|--------------|----------|
| WIN7-64-BAS-001/PRIM | Failover | Primary | N/A | N/A | N/A |

Mirrored Databases

Filter: Page size: Max rows: Results: 0 Page: of 1

| Name | Directory | Status | Next Record To Dejournal (Time, Filename, Offset) |
|------------|-----------|--------|---|
| No Results | | | |

Click 'Go' to perform an action on multiple databases

--Select an action--







If you see that it 's still in a ' Transition ' status, wait a few seconds and refresh the page. Note that these statuses were enhanced in 2016.2. You can see what they look like in the latest released version [here](#).

Step 4: Generate Key/Certificate For Second Failover Mirror Member

This is the same process as step 2, but I ' ll replace anything with ' MachineA ' in the name with ' MachineB ' . As I mentioned before, make sure you change at least 1 of the fields in the Distinguished Name section from the CA certificate. You also need to be sure you get the correct certificate in the Get Certificate step, as you may see more than one option.

Step 5: Join Mirror as Failover Member

Just like you did for the first mirror member, you need to start the ISCAgent and enable the mirror service for this instance (refer to step 3 for details on how to do this). Then, you can join the mirror as a failover member at [System Administration -> Configuration -> Mirror Settings -> Join as Failover].

| | | | |
|---|------------------------|------------------------------|-------------------------|
|  Home  DeepSee  Ensemble  System Operation  System Explorer  System Administration | Configuration » | System Configuration » | Enable Mirror Service |
| | Security » | Connectivity » | Create a Mirror |
| | Licensing » | Mirror Settings » | Edit Mirror |
| | Encryption » | Database Backup » | Edit Async |
| | | CSP Gateway Management | Join as Failover |
| | | SQL and Object Settings » | Join as Async |
| | | Device Settings » | |
| | | National Language Settings » | |
| | | Zen Reports » | |
| | | Additional Settings » | |

You ' ll need the ' Mirror Name ' , ' Agent Address on Other System ' (the same as the one you configured as the Superserver address for the other member), and the instance name of the now-primary instance.

Mirror Information

Mirror Name
Required.

Other Mirror Failover Member's Info

Agent Address on Other System
Required.

Mirror Agent Port
Required.

Caché Instance Name
Required.

Provide required information then click **[Next]** to retrieve data

After you click ' Next ' , you should see a message indicating that the mirror requires SSL, so you should again use the ' Set up SSL/TLS ' link. As in step 3, you ' ll need the CA Server certificate (same file we used in step 3, refer to that step for how to retrieve it), and you ' ll replace machine A ' s files and password with machine B ' s for this dialog.

| | | |
|---|---|-----------|
| File containing trusted Certificate Authority X.509 certificate | C:\InterSystems\PRIM\mgr\CAServer\CA_Server.cer | Browse... |
| File containing Certificate Revocation List | | Browse... |
| This server's credentials | | |
| File containing this configuration's X.509 certificate | C:\InterSystems\BACK\mgr\MachineB_client.cer | Browse... |
| File containing associated private key | C:\InterSystems\BACK\mgr\MachineB_client.key | Browse... |
| Private key type | <input checked="" type="radio"/> RSA <input type="radio"/> DSA | |
| Password: | <input checked="" type="radio"/> Enter new password <input type="radio"/> Clear password <input type="radio"/> Leave as is | |
| Private key password | | |
| Private key password (confirm) | | |
| Cryptographic settings | | |
| Protocols | <input type="checkbox"/> SSLv2 <input type="checkbox"/> SSLv3 <input type="checkbox"/> TLSv1.0 <input type="checkbox"/> TLSv1.1 <input checked="" type="checkbox"/> TLSv1.2 | |
| Enabled ciphersuites | ALL:!aNULL:!eNULL:!EXP:!SSLv2 | |

Again, I ' m only using TLSv1.2. Once you ' ve saved that, you should be able to add information about this mirror member. Again, I ' m going to change the hostnames to IP ' s, but feel free to use any IP/hostname that the other member can contact this machine on. Note that the IP ' s are the same for my members, as I have set this up with multiple instances on the same server.

| Mirror Failover Member Information | | |
|------------------------------------|--|----------------------|
| | <u>This System</u> | <u>Other System</u> |
| Mirror Member Name | WIN7-64-BAS-001/BACK | WIN7-64-BAS-001/PRIM |
| Superserver Address | 192.168.2.100 | 192.168.2.100 |
| Mirror Agent Port | 2188 | 2188 |
| SSL/TLS Requirement | The mirror requires SSL/TLS. Edit SSL/TLS | |
| Mirror Private Address | 192.168.2.100 | 192.168.2.100 |

[Advanced Settings](#)

When you save this, you should see a message telling you not to forget to add this node to the primary ' s configuration.

Step 6: Authorize 2nd Failover Member on the Primary Member

Now we need to go back to the now primary instance where we created the mirror. From the [System Administration -> Configuration -> Mirror Settings -> Edit Mirror] page, you should see a box at the bottom titled ' Pending New Members ' including the failover member that you just added. Check the box for that member and click Authorize (there should be a dialog popup to confirm).

| Pending New Members | | |
|---|----------------------|------------------|
| Select the member(s) you wish to authorize or reject: | | |
| <input type="checkbox"/> | Name | Member Type |
| <input checked="" type="checkbox"/> | WIN7-64-BAS-001/BACK | Failover |
| | | DN |
| | | CN=MachineB,C=US |

Now if you go back to [System Operation -> Mirror Monitor], it should look like this (similar on both instances):

This system is a failover member in mirror PKIMIRROR

Mirror Failover Member Information

| | <u>This Failover Member</u> | <u>Other Failover Member</u> |
|-------------------------------|-----------------------------|------------------------------|
| Mirror Member Name | WIN7-64-BAS-001/PRIM | WIN7-64-BAS-001/BACK |
| Superserver Address | 192.168.2.100 | 192.168.2.100 |
| Mirror Private Address | 192.168.2.100 | 192.168.2.100 |

Arbiter Connection Status

| | |
|--------------------------|---|
| Arbiter Address | Arbiter not configured |
| Failover Mode | Agent Controlled |
| Connection Status | This member is not connected to the arbiter |

Mirror Member Status

| Member Name | Member Type | Status | Journal Transfer | Dejournaling | X.509 DN |
|----------------------|-------------|---------|------------------|--------------|----------|
| WIN7-64-BAS-001/PRIM | Failover | Primary | N/A | N/A | N/A |
| WIN7-64-BAS-001/BACK | Failover | Backup | Active | Caught up | N/A |

Again, if you see a ' Transition ' status, wait a few seconds and refresh the page.

Step 7: Generate Key/Certificate for Async Member

This is the same as step 2, but I ' ll replace anything with ' MachineA ' in the name with ' MachineC ' . As I mentioned before, make sure you change at least 1 of the fields in the Distinguished Name section from the CA certificate. Make sure you get the correct certificate in the ' Get Certificate ' page, as you may see more than one option.

Step 8: Join Mirror as Async Member

This is similar to step 5. The only difference is that you may only be asked to configure 1 address (this depends what version you ' re running), and you have the added option for an Async Member System Type (I will use Disaster Recovery, but you ' re welcome to use one of the reporting options). You ' ll again see a message about requiring SSL, and you ' ll need to set that up similarly (MachineC instead of MachineB). Again, you ' ll see a message after saving the configuration indicating that you should add this instance as an authorized async on the failover nodes.

Step 9: Authorize Async Member on the Primary Member

Follow the same procedure as in step 6. Note that this procedure has been simplified in recent versions to match behavior for a 2nd failover member. Previously, you needed to manually add authorized async member information. Once this complete, there is one extra step to make sure the mirror monitors are in sync. You should go to the [System Operation -> Mirror Monitor] on the 2nd failover member (now the backup), and click ' Stop mirror ' . After that ' s complete, you should then click ' Start mirror ' . This is just to make sure that instance retrieves the information about the async member. It should not be required in later versions. The mirror monitor should now look like this:

This system is a failover member in mirror PKIMIRROR

Mirror Failover Member Information

| | <u>This Failover Member</u> | <u>Other Failover Member</u> |
|-------------------------------|-----------------------------|------------------------------|
| Mirror Member Name | WIN7-64-BAS-001/BACK | WIN7-64-BAS-001/PRIM |
| Superserver Address | 192.168.2.100 | 192.168.2.100 |
| Mirror Private Address | 192.168.2.100 | 192.168.2.100 |

Arbiter Connection Status

| | |
|--------------------------|---|
| Arbiter Address | Arbiter not configured |
| Failover Mode | Agent Controlled |
| Connection Status | This member is not connected to the arbiter |

Mirror Member Status

| Member Name | Member Type | Status | Journal Transfer | Dejournaling | X.509 DN |
|----------------------|-------------------|-----------|------------------|--------------|------------------|
| WIN7-64-BAS-001/PRIM | Failover | Primary | N/A | N/A | N/A |
| WIN7-64-BAS-001/BACK | Failover | Backup | Active | Caught up | N/A |
| WIN7-64-BAS-001/ASY | Disaster Recovery | Connected | Caught up | Caught up | CN=MachineC,C=US |

Incoming Journal Transfer Rate for This Member (over refresh interval)
--- (will be displayed on refresh)

Step 10: Add a Mirrored Database

Having a mirror is no fun if you can't mirror any data, so we may as well create a mirrored database. We will also create a namespace for this database. Go to your primary instance. First, go to [System Administration -> Configuration -> System Configuration -> Namespaces] and click 'Create New Namespace' from that page.

View:

Search:

| | | | |
|--|------------------------|-------------------------------|--------------------|
| <div style="margin-bottom: 5px;"> Home</div> <div style="margin-bottom: 5px;"> DeepSee</div> <div style="margin-bottom: 5px;"> Ensemble</div> <div style="margin-bottom: 5px;"> System Operation</div> <div style="margin-bottom: 5px;"> System Explorer</div> <div style="margin-bottom: 5px;"> System Administration</div> | Configuration » | System Configuration » | Memory and Startup |
| | Security » | Connectivity » | Namespaces |
| | Licensing » | Mirror Settings » | Local Databases |
| | Encryption » | Database Backup » | Remote Databases |
| | Enterprise Manager | CSP Gateway Management | Journal Settings |
| | | SQL and Object Settings » | |
| | | Device Settings » | |
| | | National Language Settings » | |
| | | Zen Reports » | |
| | | Additional Settings » | |

We'll call this 'MIRROR', and we'll need to click 'Create New Database' next to 'Select an existing database for Globals'. You'll need to enter a name ('MIRROR') and directory for this new database. On the next page, be sure to change the 'Mirrored database?' drop-down to yes (THIS IS ESSENTIAL). The mirror name will default to the database name you chose. You can change it if you wish. We will use the default setting for all other options for the database (you can change them if you want, but this database must be journaled, as it is mirrored). Once you finish that, you will return to the namespace creation page, where you should select this new database for both 'Globals' and 'Routines'. You can accept the defaults for the other options (don't copy the namespace from anywhere).

Use the form below to create a new namespace:

The screenshot shows a web form for creating a new namespace. The form is titled "Name of the namespace" and has a text input field containing "MIRROR". Below the input field is the text "Required.". To the right of the input field is a dropdown menu labeled "Copy from". Below the "Copy from" dropdown is a section titled "The default database for Globals in this namespace is a" with two radio buttons: "Local Database" (selected) and "Remote Database". Below this section is a section titled "Select an existing database for Globals" with a text input field containing "MIRROR" and a dropdown menu. To the right of the input field is the text "Required.". To the right of the dropdown menu is a button labeled "Create New Database...". Below this section is a section titled "The default database for Routines in this namespace is a" with two radio buttons: "Local Database" (selected) and "Remote Database". Below this section is a section titled "Select an existing database for Routines" with a text input field containing "MIRROR" and a dropdown menu. To the right of the input field is the text "Required.". To the right of the dropdown menu is a button labeled "Create New Database...". Below this section is a section titled "Create a default Web application for this namespace" with a checkbox that is checked. Below this section is a section titled "Copy namespace mappings from" with a dropdown menu.

Repeat this process for the backup and async. Make sure to use the same mirror name for the database. Since it ' s a newly created mirrored database, there is no need to take a backup of the file and restore onto the other members.

Congratulations, you now have a working mirror using SSL with 3 members sharing a mirrored database!

Other reference documentation:

[Create a mirror](#)

[Create mirrored database](#)

[Create namespace and database](#)

[Edit failover member](#) (contains some information on adding SSL to an existing mirror)

[#Best Practices](#) [#Caché](#) [#High Availability](#) [#Mirroring](#) [#InterSystems IRIS](#) [#SSL](#) [#System Administration](#)

Source

URL:<https://community.intersystems.com/post/creating-ssl-enabled-mirror-using-public-key-infrastructure-pki>