

Service Accounts

Scenario

Time is precious and while I understand that many of you will want to skip to the section that is relevant for what you are wanting to do I would advise taking the time to read through this document at least once to ensure that you understand the reasons behind what you are doing. The scenario you are about to walk through is a real-life scenario that did actually happen for a £1b+ turnover company with huge IT resources. One man resolved these issues and that man was me and the following information gives you an insight into what I found during my attempts to sort things and the steps I took to get there. The knowledge you will gain is relevant for any size business. It doesn't matter how big you are, you still have the same issues to deal with. While I have made every effort to make sure these details are accurate and are taken directly from the notes I scribbled as I went, where possible you should test this in a dedicated test environment. I cannot be held accountable for any problems that could arise as a result of failing to test thoroughly. All I can say is it worked for me and I've used this document time and time again, not because I'm forgetful but because I wanted it to be all it could be.

Issues can arise with the Windows Service accounts that are used to run Open Edge and other components and add-ons for Epicor ERP products. Changes to these accounts can have a dramatic impact on the operation of your system and can render it useless unless you know how to put things right.

The client in this scenario had an issue with the user account that was used to start the Admin Service for Open Edge service (along with the Service Connect Services). The account was a general one that some users also used to log onto the network, typically Epicor Support/Consultants. It is not best-practice to set up a service account with credentials used by users and I would strongly advise against it. This account became compromised and the password was changed. On server reboot all of the services failed and their Epicor system was inaccessible. (This can also be an issue if your IT department enforces 90-day user password change.)

However, even after setting the new account and changing the Service logon information, the client was still unable to access the Open Edge Management Console despite the fact that the Admin Service for Open Edge appeared to be running and stopping and starting the Service manually appeared to be functioning as you would expect.

Note: Creating a domain user account is beyond the scope of this document. This scenario details the steps taken on a Windows Server 2008 R2 system and you may have to adjust them to suit your environment.

Symptoms

The following are symptoms that may arise: -

- Open Edge Management Console will not launch.
- Users unable to log into Epicor

Contents

CONTENTS

1.	Changing the Service Account	3
2.	Administering the Admin Service Using ProEnv	4
3.	Granting the Service Account Access to the Databases	5
4.	In Summary	5

1. CHANGING THE SERVICE ACCOUNT

The services that you have for Epicor and its components are many and varied but should be set up in the same way. Our primary focus here is the Admin Service for Open Edge. This is the main component and without it your Epicor product will fail.

It is important that you understand the conditions that must be met to change the Service Account. You can change this at any time but the changes will not take place until you restart the Service or reboot the server. Remember that this new account will also need permission to access your databases. In this scenario, the client was running Microsoft SQL Server 2008 R2 and when the Service Connect services tried to start, they failed with “Can’t connect to the database” errors. You can look for these in the Event Viewer. Also, it is absolutely critical that the Service Account be made a member of the Local Administrator group on the servers in your Epicor environment. As we continue through this scenario we’ll cover the symptoms and the methods to investigate and resolve.

OK, let us begin...

We have a new Service Account and password that we want to assign to the relevant services. We’ll start by applying this account to these services.

- Launch the Services console. (Start | Administrative Tools | Services)
- Locate the Admin Service for Open Edge service and right-click on it and select Properties.
- Select the Log On tab and enter your new Account information. When you click the Apply button you will receive notification that “The new logon name will not take effect until you stop and restart the service.” You should be aware that restarting this Service will disconnect all users as the AppServers will be stopped for all databases. If you haven’t set your AppServers to restart automatically you will need to start them once the Service is up and running. Be patient with the Open Edge Management Console, the service won’t necessarily be running fully despite it informing you that it is.
- Assign the account to any additional services that have been given the wrong account information.
- At this point in our scenario we’ve restarted the Admin Service for Open Edge but when we try to log into the Open Edge Management Console, the browser page tells us that we can’t connect. We need to assess whether or not the service has started correctly.

2. ADMINISTERING THE ADMIN SERVICE USING PROENV

We've already established that as far as the Services console is concerned the Admin Service for Open Edge has started and is running. I don't want to ruin your faith and trust in this console but what we really need to do is determine whether it actually has or not. To do this we use the Proenv utility provided with Progress. Make sure that you are logged onto the server as a Local Administrator.

- Launch Proenv from Start | All Programs | OpenEdge 10.2A | Proenv. A window similar to a command prompt will open.
- Enter the following command `proadsv -q` This command queries the service directly to establish its status. You will see one of the following responses.
 - AdminServer is not alive – This informs you that the service isn't running.
 - AdminServer is alive – This informs you that the service is running.
- To start the service enter `proadsv -start` and then run the `proadsv -q` query command again to make sure it has started.
- To stop the service enter `proadsv -stop` and then run the `proadsv -q` query command again to make sure it has stopped.

Once you have started the service you should now be able to launch the Open Edge Management Console.

So why did this work through Proenv but not through the Services console? I'll be honest and say that this took a little to work out but it all boils down to this....

When you start the Service through the Services console you are starting it using the credentials you provided when you set up the logon credentials in step 1. When you start it using the Proenv utility you are doing it with the credentials of the user you are logged in as. I'd asked you to make sure that you were logged onto the server as a local administrator and this was and is the primary reason. In our scenario, the credentials provided to the service were not those of a local administrator, and these are required permissions for the Admin Service to start. Had you have logged into the server as a "normal" user, the Proenv commands would more than likely have failed too. So in summary, make sure that whoever sets up this Service Account gives it Local Administrator rights on all of the Epicor servers in your environment. There will be an Admin Service for Open Edge on every server that has Epicor and/or Open Edge installed. Once the permissions have been granted to the Service account you should restart the Admin Service, and launch the Open Edge Management Console, or try logging into Epicor.

I mentioned earlier that the services that need access to the databases must be granted that permission. In our scenario, the user had not been. This manifested itself in the failure of the Service Connect services.

3. GRANTING THE SERVICE ACCOUNT ACCESS TO THE DATABASES

Without permission to access the databases, some services will fail. To explain a little further, the Service Connect services need to have access to the ESCDB (the Epicor Service Connect Database). Not all services for Service Connect actually need to be started. They are triggered by the application. To test whether or not the Service Connect services are running or can be started you should launch the SC Services Manager. This can typically be found by clicking Start | All Programs | Epicor Software | Epicor Service Connect. This will place the SC Services Manager icon in the tray on your task bar (bottom-right of your screen). The icon will probably be white at this point. Right-click this icon and select Start Epicor Services. If, after a period of time, the icon goes green then the Services have started successfully. If it remains white then the services cannot be started.

As mentioned earlier, our client is using MS SQL2008 R2. We'll continue with our configuration by granting access.

- Log into your database server using a local administrator account.
- Click Start | All Programs | Microsoft SQL Server 2008 | SQL Server Management Studio, and log into your SQL instance.
- Expand the instance, then Security, then Logins, and see if the new Service account has been added to the list.
- Add the new account by Right-clicking Logins and selecting New Login. On the General tab, enter the login name of the account. Leave all checkboxes unchecked, set the Default database to Master and choose a default language (Optional).
- Click the User Mapping tab and check the boxes for each database that you want this account to have access. As you are doing this you could set the account to be the owner of each database (db_owner).
- Click the Status tab and make sure that the Grant and Enabled options are selected.
- Click OK.

These changes are immediate and do not require a restart of SQL or the Server.

Go back to the server that hosts the Service Connect services and try starting the Epicor services using the sc Services Manager. If they do, then you're all set and can continue to enjoy Epicor.

4. IN SUMMARY

Service Accounts are a critical part of the implementation and administration of your Epicor ERP system. You could save yourself a lot of pain if you ensure that these are set up correctly from the off. When they work and there are no factors influencing change to them the chances are you'll never need to do anything other than stop and start them. I hope this document has helped you gain an understanding of what can go wrong and what you can do to put it right.

If you have any further questions please feel free to email me at mike.armstrong@bpmtechnicalsolutions.com

Remember, work smarter, not harder.