**Updated 1/25/2023**

**EDSNET Machine IDs password update process**

TOPPGVP

* Member portal for deductible balance
* ~~Salesforce Benefit Narrative (Velocity Connect~~) Confirmed 1/13/2023 that SF no longer uses the MV API
* Subscriber Service also uses it and IVR does use Subscriber Service.

TOPPIVR

* IVR

Metavance Batch IDs

* Need to match TOPPIVR and TOPPGVP in Production and MV Model Office and Region A-S.

In the future these password changes should be done on a weekend.

All users need to be kicked off the system prior to starting the password changes.

Production and lower environments all must be updated on the same day to prevent lock out violations.

All applications must have the passwords updated before anyone should begin validation of the new passwords. DXC will clear the lock out violations prior to validation beginning.

Impacted teams:

* CIA (IVR)
* ~~Velocity Connect (Salesforce Benefit narrative)~~ No longer uses MV API
* Team Alpha (Member portal)
* ISS (Metavance batch ids)
* DXC
* Operations
* Tech lead (Manjiri or Amber)
* Team Phoenix (Provider Portal) not affected they do not use benefit narrative or deductible balance.

**Steps each team needs to make to ensure all passwords are updated:**

**Operations**:

Ops has updated the TOPPGVP metavance and EDSNET password on “non-prod” web servers for the:

1. BenefitNarrarive services \*were these updated in Prod by Ops? Rob to check
2. DeductableBalance services \*Alpha is doing an update so they update these in 2023
3. SubscriberService services (Ops had to update this one for Prod servers) no source code for pipeline release has to be manually updated on the server. \* Nobody uses, but there is no job where we can update this and it has to be updated on config files. Can we add this to pipeline? Alpha is looking into this w/ Manjiri.
4. SubscriberService\_V3 services (This one use TOPPGVP password) \* could be new procedure if we move away from APO db

Dev

md-wss-fw01n01

md-wss-fw01n02

MO-Test

mt-wss-fw01n01 - 10.1.79.149

mt-wss-fw01n02 - 10.1.79.148

MO-UAT

mt-wss-fw02n01 - 10.1.79.147

mt-wss-fw02n02 - 10.1.79.146

Stage

ms-wss-fw01n01 - 10.1.79.142

ms-wss-fw01n02 - 10.1.79.143

ms-was-fw01n01 - 172.17.10.70 (these servers do not host any TOPPGVP services)

ms-was-fw01n02 - 172.17.10.71 (these servers do not host any TOPPGVP services)

PerfTest

ms-wss-fw02n01 - 10.1.79.140

ms-wss-fw02n02 - 10.1.79.141

ms-wss-fw02n03 - 10.1.79.139

Prod

MP-WSS-FW01N01

MP-WSS-FW01N02

MP-WSS-FW01N03

MP-WSS-FW01N04

MP-WSS-FW01N05

MP-WSS-FW01N06

**CIA**

1. Update APO db in all environments production down to dev, via SQL script.

Database name: APO

Server names:

MD-WAS-D02 - ETSDevWeb.aif.bcbsaz.com

MQ-WAS-D02 - ETSMOTestWeb.aif.bcbsaz.com

MU-WAS-D02 - ETSMOUATWeb.aif.bcbsaz.com

MF-WAS-D02 -  ETSPerfWeb.aif.bcbsaz.com

MS-WAS-D02- ETSStageWeb.aif.bcbsaz.com

MP-WAS-D03 - ETSProdWeb.aif.bcbsaz.com

Sample SQL Script:

USE APO

Update [APO].[dbo].[utb\_ConfigSettings] set value='XXXXXXX' where Name='MetaVanceIVRPwd' and Environment='ETSProd'

Update [APO].[dbo].[utb\_ConfigSettings] set value='XXXXXXX' where Name='MetaVanceGVPPwd'

1. Request IIS reset for servers to remove cache passwords to be coordinated with all teams to reset at the **end of all pws being updated**. This should be the last step in the process before validation.

**Team Alpha**

1. Update the TOPPGVP password field of the web.config in the deductibles balance service and commcfg files dropped into the correct folders for the below services servers
2. Member portal also uses the subscriber service services for the deductible balance service to return data
3. Reset IIS

*Services servers*

1. \\md-wss-fw01n01.aif.bcbsaz.com\
2. [\\md-wss-fw01n02.aif.bcbsaz.com\](file:///\\md-wss-fw01n02.aif.bcbsaz.com\)
3. \\mt-wss-fw01n01.aif.bcbsaz.com\
4. [\\mt-wss-fw01n02.aif.bcbsaz.com\](file:///\\mt-wss-fw01n02.aif.bcbsaz.com\)
5. \\mt-wss-fw02n01.aif.bcbsaz.com\
6. \\mt-wss-fw02n02.aif.bcbsaz.com\
7. \\ms-wss-fw01n01.aif.bcbsaz.com\
8. [\\ms-wss-fw01n02.aif.bcbsaz.com](file:///\\ms-wss-fw01n02.aif.bcbsaz.com)\
9. \\ms-wss-fw02n01.aif.bcbsaz.com\
10. \\ms-wss-fw02n02.aif.bcbsaz.com\
11. [\\ms-wss-fw02n03.aif.bcbsaz.com\](file:///\\ms-wss-fw02n03.aif.bcbsaz.com\)
12. \\mp-wss-fw01n01.aif.bcbsaz.com\
13. \\mp-wss-fw01n02.aif.bcbsaz.com\
14. \\mp-wss-fw01n03.aif.bcbsaz.com\
15. \\mp-wss-fw01n04.aif.bcbsaz.com\
16. [\\mp-wss-fw01n05.aif.bcbsaz.com\](file:///\\mp-wss-fw01n05.aif.bcbsaz.com\)
17. [\\mp-wss-fw01n06.aif.bcbsaz.com\](file:///\\mp-wss-fw01n06.aif.bcbsaz.com\)

**~~Velocity Connect~~ No longer needed since SF is not using MV API**

1. ~~Update the “ProxyRequestorUserPassword” and “ProxyClientUserPassword” elements in the following JSON files located in the BenefitServices.API.Internal repository:~~

~~appsettings.Dev.json~~

~~appsettings.Perf.json~~

~~appsettings.Prod.json~~

~~appsettings.QA.json~~

~~appsettings.Stage.json~~

~~appsettings.UAT.json~~

1. ~~Create a new release version in Azure DevOps for BenefitServices.API.Internal.~~
2. ~~DevOps pushes the new release version to production.~~

**ISS**

1. At the appropriate time, DXC will provide ISS via email the Machine ID passwords for **TOPPIVR** and **TOPPGVP**
2. Login to the **MetaVance Regions** below
3. Go to **Configuration**, **Application Security**, **User Maintenance**
4. Change the **User Type** from **Operator** to **Batch/Web**
5. Search by User ID **TOPPGVP** or **TOPPIVR**
6. Update the **TOPPGVP** or **TOPPIVR** account password in **MetaVance Regions** below flagged **Y**:

|  |  |  |
| --- | --- | --- |
| **MetaVance Regions** | **TOPPGVP** | **TOPPIVR** |
| Production | Y | Y |
| Model Office | Y | N |
| UAT A | Y | N |
| UAT B | Y | Y |
| UAT J | Y | Y |
| UAT K | Y | Y |
| UAT S | Y | Y |

**DXC**

Pre-change tasks:

1. DXC BCBSAZ account team security creates new passwords for machine IDs. The new password for the machine IDs being changed is distributed securely to the DXC Mainframe Corporate Security and BCBSAZ resource implementing the change. Please note that the machine ID passwords are considered highly confidential and should not be know by anyone without absolute need to know.
2. DXC and BCBSAZ machine ID owners determine implementation window.
3. DXC BCBSAZ account team security engages DXC Mainframe Corporate Security to schedule resource to perform the change on request during a change window.

During the change:

1. DXC BCBSAZ account team notifies DXC Mainframe Corporate Security to update the password when requested by the BCBSAZ client during the change window.
2. DXC BCBSAZ account team security accesses the ID statistics in the mainframe application TSO ACF and lists the ID. They check the ACCESS parameters to determine the last date and time the ID was successfully accessed. They also check the PASSWORD parameters to determine if the ID is locked due to invalid password attempts. IF the PSWD-VIO parameter value is equal to (6) the ID is locked. DXC BCBSAZ account team security can then enter the command to CHANGE \* PSWD-VIO(0) to reset the counter to zero and unlock the account.
3. DXC security will continue to monitor the ID for violations and reset the counter as required while the BCBSAZ client performs validation testing and additional clean up as necessary.