Australian Government
Australian Digital Health Agency

Health API Gateway

Bundle 3 – My Health Record Software Vendor Test (SVT) environment

Vendor Release Notes

Version: 1.0
Date: 12/09/2022

Contents

1. Bundle 3 – SVT Deployment Schedule

Health API Gateway Project Bundle 3 will be deployed into the Software Vendor Test (SVT) environment in a 3-step process as illustrated in the table below.

Deployment Step	Description	Deployment Date	Deployment Window	Impact to Vendors
1	**DNS Cutover Deployment**: Deloitte takes the control of the gateway and ensures that the B2B traffic still flows through the NIO gateway	13 Sept 2022	6:00 PM - 9:00 PM	No
2	**SVT Cutover to all vendors except (ACT region):** B2B API's traffic cutover to Azure gateway	15 Sept 2022	6:00 PM – 11: 00 PM	No
3	**SVT Cutover to vendors in ACT region**: B2B API's traffic cutover to Azure gateway	20 Sept 2022	6:00 PM – 9:00 PM	No

This staged approach allows us to better manage the rollout of the changes to the vendors.

All functionality of the SVT environment will remain available during the deployment window (6 PM – 11 PM). Based on the testing we conducted in the non-prod deployment of the same, we are not anticipating any downtime for vendors during SVT deployment. The SVT environment upgrade is scheduled to happen outside of the advertised available hours (9 AM – 6 PM) for the SVT environment.

For technical support please contact healthapigatewaysvt@deloitte.com.au

2. Bundle 3 – Summary of Changes

Bundle 3 of the Health API Gateway will move Oracle API Gateway B2B API endpoints from MHR to the new Azure API Gateway. Once the change has been completed connected organisations will be able to:

- Perform testing activities against the Health API Gateway Software Vendor Testing environment operated and maintained by Deloitte.
- Contact Deloitte to initiate onboarding milestone activities including:
    - Self-Assessment Validation Requests
    - Notice of Connection Observation Sessions

Blackout Period

The blackout period will run from 15 September to 12 October inclusive. It is recommended that vendors perform testing during this time and report any issues directly using agreed channels (NOC testing is not allowed during blackout period).

2.1 B2B Web Service Consumer Changes

B2B web services have been re-platformed from Oracle API Gateway to the Azure-based Health API Gateway platform. Every care has been taken to ensure functional equivalence to eliminate impacts to B2B vendors wherever possible. However, there are a small set of changes that may impact your software's interactions with My Health Record via the B2B services. These are explained below.

2.1.1 Mutual TLS Handling

Mutual TLS connections are terminated by a different technology, which subtly changes how and when your NASH client TLS certificate is presented during the TLS session negotiation. Some vendors using legacy Gateway appliances have observed connectivity issues due to this change and had to upgrade to a newer more standards-compliant HTTPS client library.

It is highly unlikely you will be affected by this change. However, if your software is impacted you will observe **403 Forbidden** HTTP error responses returned from the Azure Application Gateway to your application. If you observe this error, please email the technical support address above.

2.1.2 Global Security Checks

Some low-level security checks have been re-implemented and may return different error messages if these critical security checks are violated.

You may observe the following,

400 Bad Request HTTP response from the Azure Application Gateway

```
HTTP/1.1 400 Bad Request
Server: Microsoft-Azure-Application-Gateway/v2
Date: Thu, 25 Aug 2022 04:28:09 GMT
Content-Type: text/html
Content-Length: 263
Connection: close

<html>
<head><title>400 No required SSL certificate was sent</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>No required SSL certificate was sent</center>
<hr><center>Microsoft-Azure-Application-Gateway/v2</center>
</body>
</html>
```

403 Forbidden HTTP response from the Azure Application Gateway

HTTP/1.1 403 Forbidden
Server: Microsoft-Azure-Application-Gateway/v2
Date: Sun, 21 Aug 2022 23:01:07 GMT
Content-Type: text/html
Content-Length: 179
Connection: keep-alive

<html>
<head><title>403 Forbidden</title></head>
<body>
<h1>403 Forbidden</h1>
<hr> Microsoft-Azure-Application-Gateway/v2
</body>
</html>

502 Bad Gateway HTTP response from the Azure Application Gateway

HTTP/1.1 502 Bad Gateway
Server: Microsoft-Azure-Application-Gateway/v2
Date: Wed, 17 Aug 2022 00:26:35 GMT
Content-Type: text/html
Content-Length: 183
Connection: keep-alive

<html>
<head><title>502 Bad Gateway</title></head>
<body>
<h1>502 Bad Gateway</h1>
<hr> Microsoft-Azure-Application-Gateway/v2
</body>
</html>

SOAP Fault as shown below

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <soap:Header />
    <soap:Body>
        <soap:Fault>
            <soap:Code>
                <soap:Value>soap:Receiver</soap:Value>
            </soap:Code>
            <soap:Reason>
                <soap:Text xml:lang="en-AU">PCEHR_ERROR</soap:Text>
            </soap:Reason>
            <soap:Detail>
                <ns2:standardError
xmlns:ns2="http://ns.electronichealth.net.au/wsp/xsd/StandardError/2010">
                    <ns2:errorCode>badlyFormedMsg</ns2:errorCode>
                    <ns2:message>messageBlocked</ns2:message>
                </ns2:standardError>
            </soap:Detail>
        </soap:Fault>
    </soap:Body>
</soap:Envelope>
```

The logic of the security checks themselves has not altered – you should expect all well-formed, legitimate B2B web service requests to continue to be processed successfully.

2.1.3 B2B Error Code Changes

The following error scenarios have been altered:

Interface ID	Interface Name	New/Changed/Removed Error Codes
SOAP inbound	All	Error response format for Global Security Checks is as mentioned above. This is different to the previously provided error response
	Notify Change Account Notify Customer Details Change	Some errors previously returned 200 OK as HTTP status in the response. Now all the error responses return 500 Internal Server Error in the response
	Notify Change Account Notify Customer Details Change	SOAP Action header in the response was previously returning response action, which has been now corrected to return http://ns.services.my.gov.au/svc/commonmessages/2013/09/07/standardfault
	Upload Document	Threatening content errors that were previously returned as PCEHR_ERROR_0529, now instead will be blocked before entering the service and will respond with a 403 forbidden error
REST Inbound	Get Medicines View	PCEHR_ERROR_0004 is now in FHIR Bundle format rather than operation outcome
	CIStoNPP	New 400 Bad Request error exception is raised when the Content-Type header does not match application/x-www-form-urlencoded

2.2 Internal Change Summary

In addition to the changes in the Summary section above, the Bundle 3 SVT Cutover will introduce additional Fuse microservices to support B2B inbound and outbound APIs.

2.4 Acronyms

Acronym	Definition
SVT	Software Vendor Testing
DNS	Domain Name System
SOAP	Simple Object Access Protocol
REST	REpresentational State Transfer
HTTP	Hypertext Transfer Protocol
NIO	National infrastructure operator
TLS	Transport Layer Security