**Cloud Strategy and**

**Intake Playbook**

**v1.0**

Revision Control:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision:** | **Date:** | **Author:** | **Change Summary:** | **Approval:** |
| 1.0 | 5/1/20 | Bryan Nieznajko | DRAFT | DRAFT |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[Overview 4](#_Toc53646947)

[Audience 4](#_Toc53646948)

[Objectives 4](#_Toc53646949)

[Cloud Intake Process 4](#_Toc53646950)

[Access Azure Portal 15](#_Toc53646951)

[Steps 15](#_Toc53646952)

[Request Azure Access Group Membership 15](#_Toc53646953)

[Request Primary and Secondary IDs 16](#_Toc53646954)

[Request Global Group Membership to Your Subscription 19](#_Toc53646955)

[Access the Portal 20](#_Toc53646956)

[Troubleshooting 21](#_Toc53646957)

[Authentication 23](#_Toc53646958)

[Financial Management 24](#_Toc53646959)

[Reconciling your GL charges with Finance 25](#_Toc53646960)

[Patterns and Practices 27](#_Toc53646961)

[Operations and Support 33](#_Toc53646962)

[Disaster Recovery 33](#_Toc53646963)

[Definitions 33](#_Toc53646964)

## Overview

## Audience

## Objectives

Define the Cloud Strategy for OptumCare, based on CDO-specific use-cases and existing Optum/UHG patterns, practices and policies

## Cloud Intake Process

Parallel

* Request MS ID
* Once MS ID is created, create Primary and Secondary ENT IDs **(Bryan Nieznajko will create ENT IDs for you once MS ID is created)**
* Request RSA token
* Request Citrix access and/or Optum laptop with VPN
  + Optum laptop/VPN is a better user experience for managing Azure portal
  + You must have access to Optum/UHG core network for authentication into Azure portal using secondary ENTID – See “Access Azure Portal” section

Sequential

* Create Solution Intent documentation, including network and architecture diagrams, security architecture, end users, test plan, timelines, etc.
* Complete Work Intake (Change Request) form
* Create ASK ID – need following information **(Bryan Nieznajko will create ASK ID and get GL account associated to it – need GL)**

A screenshot of a social media post

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

* Request Finance group to assign GL code to ASK ID (Assignment occurs overnight, once GL code is associated to ASK ID) for subscription billing
* Create intake.md file from Solution Intent Document **(Bryan Nieznajko)**
* Create GitHub repository for project **(Bryan Nieznajko)**
* Upload all documentation to GitHub repo **(Bryan Nieznajko)**
* Create ServiceNow ticket for Azure non-prod subscription (using URL for github repo/intake.md file as reference) **(Bryan Nieznajko)**

Health Care Cloud Intake Overview

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

**Access Azure Portal**

Complete the steps below for access to [Public Azure](https://portal.azure.com/) within UHG's tenant.

**Steps**

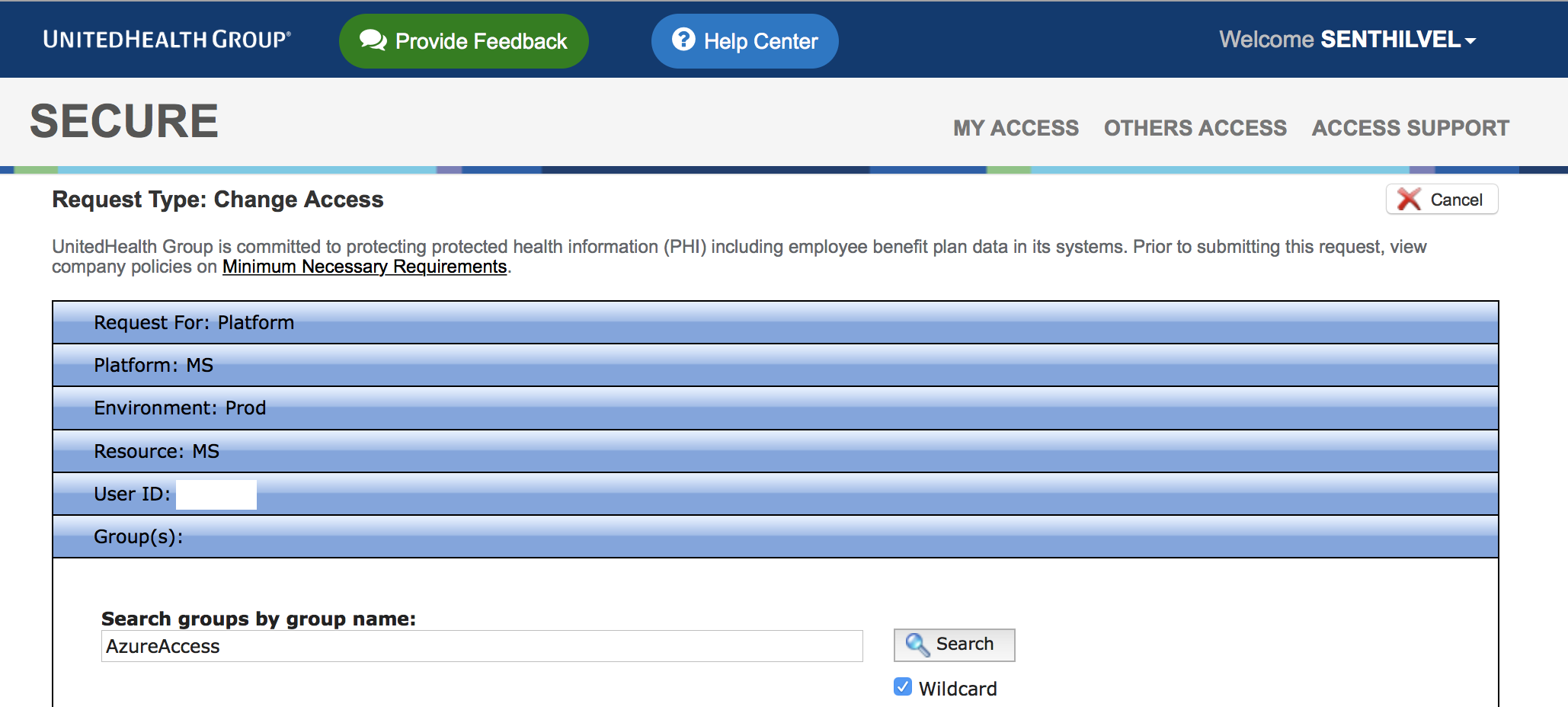
1. [Request AzureAccess global group with MSID](https://commercialcloud.optum.com/docs/getting-started/access-azure-portal/#request-azure-access-group-membership).
2. [Create your first (primary) ENTID](https://commercialcloud.optum.com/docs/getting-started/access-azure-portal/#request-primary-and-secondary-ids)
3. [Create your second (secondary) ENTID](https://commercialcloud.optum.com/docs/getting-started/access-azure-portal/#request-primary-and-secondary-ids)
   * This secondary id is used to access Azure, e.g. [mgrose3@entid.optumhub.net](mailto:mgrose3@entid.optumhub.net)
4. [Login to the azure portal using your full secondary ENTID](https://portal.azure.com/).

Optional (Not Required for DCE):

1. [Request Global Group Membership to Your Subscription](https://commercialcloud.optum.com/docs/getting-started/access-azure-portal/#request-global-group-membership-to-your-subscription)

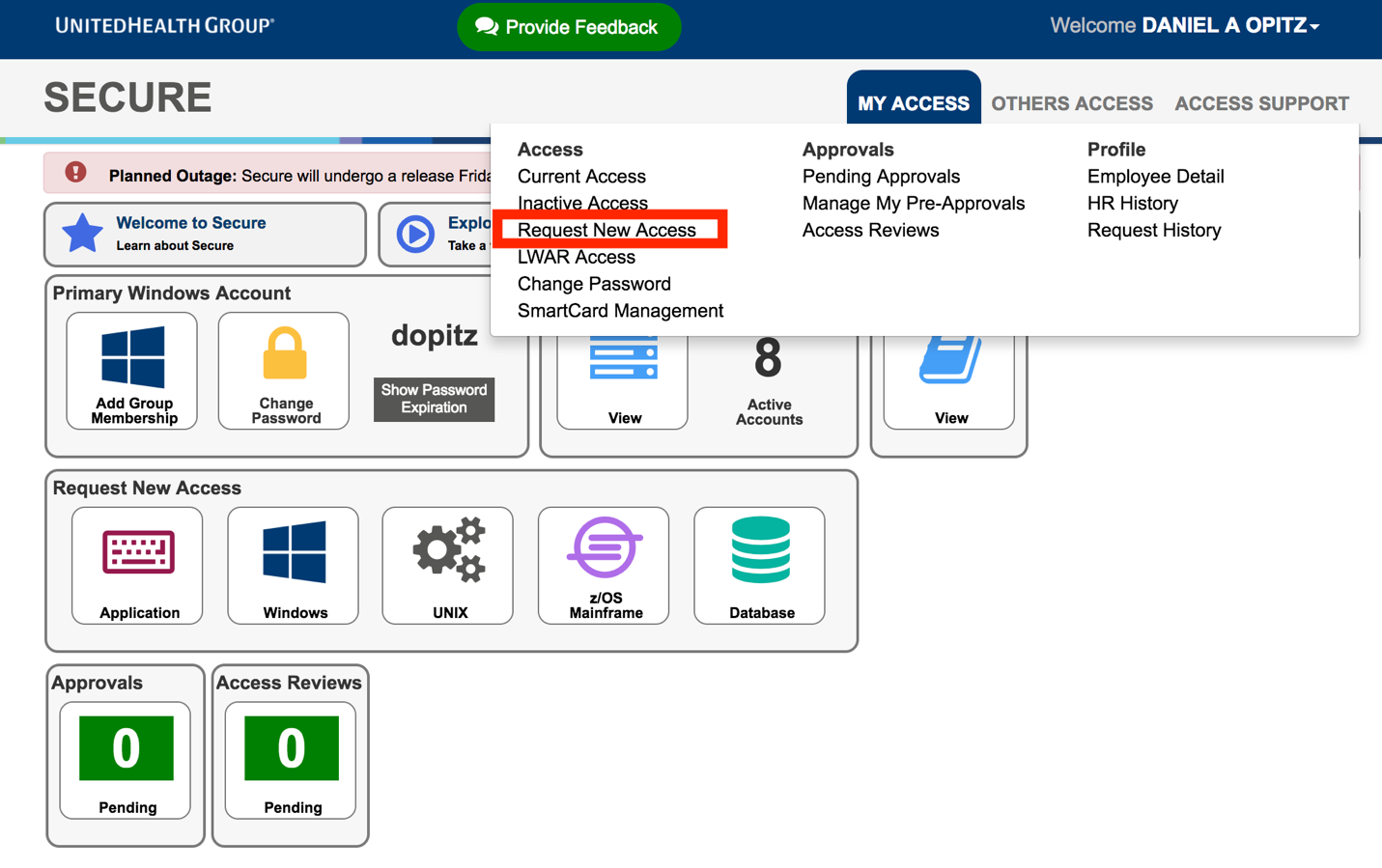
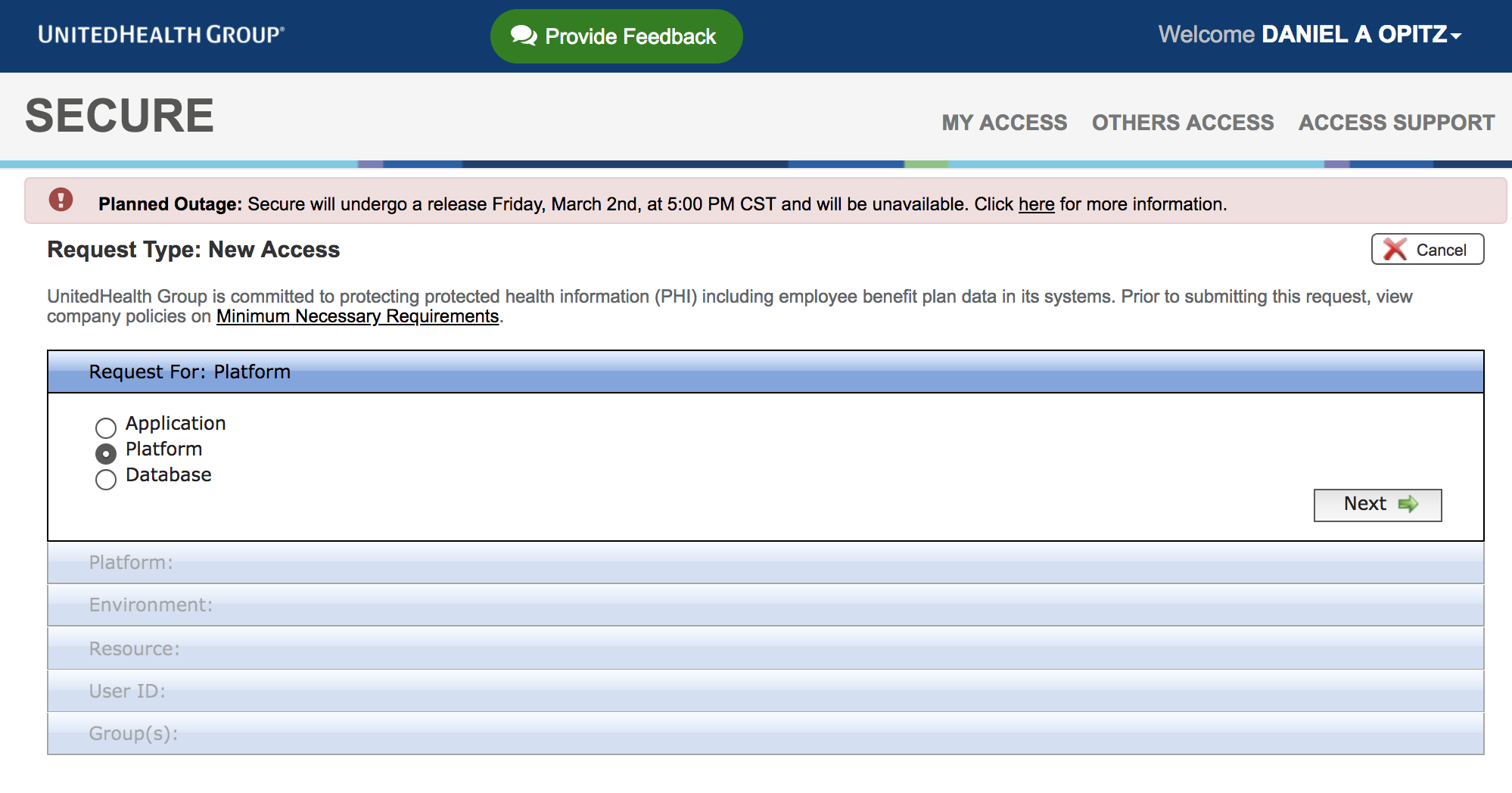
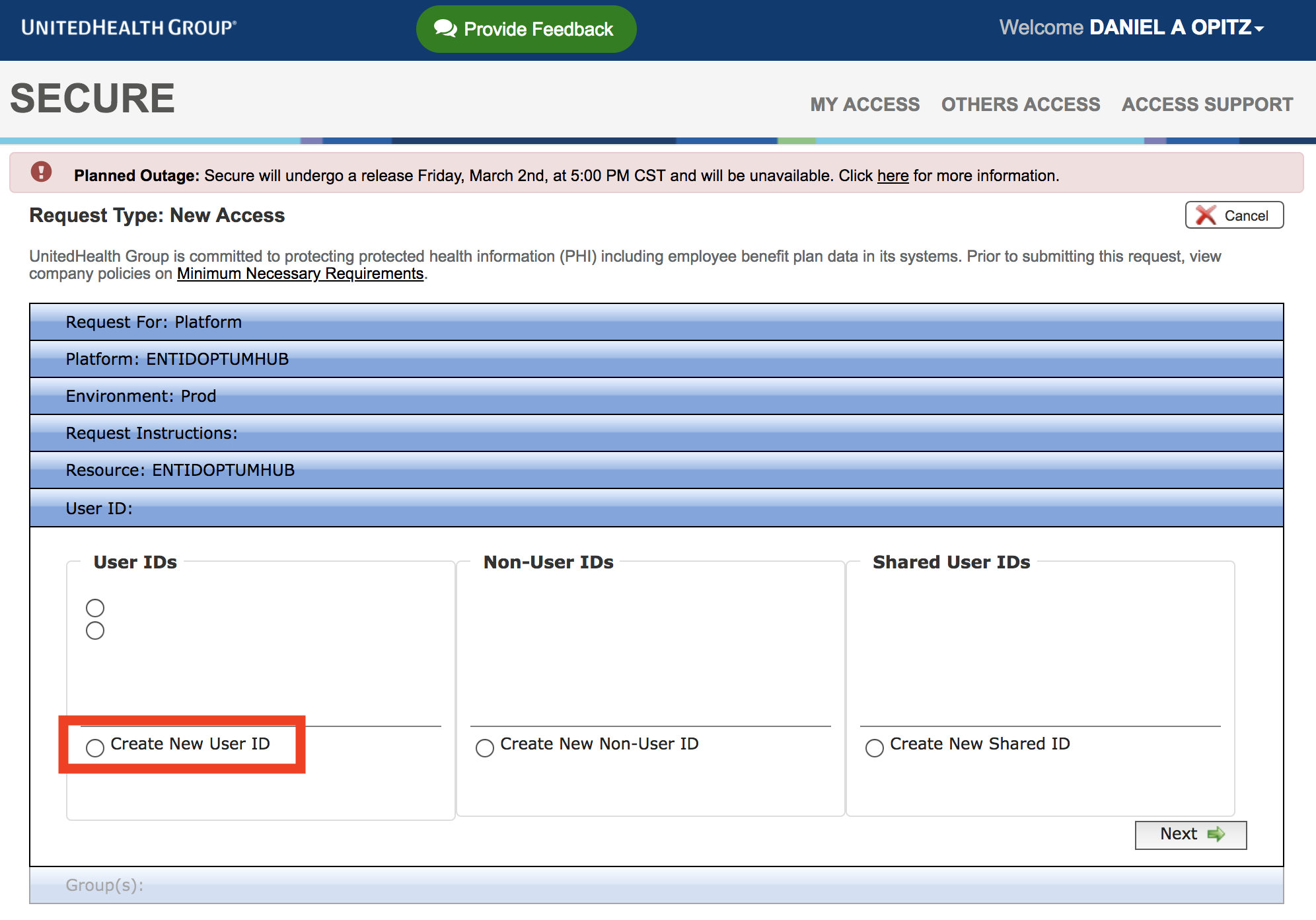
**Request Azure Access Group Membership**

Your primary **MS** ID must be added to the MS global group AzureAccess.

* Click on *Secure Home Page > Primary Windows Account > Add Group Membership* and fill out the form as shown below:
* Provide business justification and submit the request.

**Request Primary and Secondary IDs**

This process assumes you don't have a Primary or Secondary ENTIDOPTUMHUB User ID.

* Log in to secure.uhc.com.
* Navigate to *Request New Access*. 
* Choose request access for *Platform* and click next. 
* Choose *Windows* and *ENTIDOPTUMHUB* on the Platform page. 
* Proceed to the User ID page and select *Create New User ID*. 
* There is no need to add any Group access at this point.
* Fill in your Business Justification for requesting your User ID.
* Submit the Secure Request.

Note: You must create your Primary User ID first and complete the request, and then go through the process again to create your Secondary User ID and complete the request. Please wait at least 4 hours before attempting to sign in as an RSA sync is occurring behind the scenes.

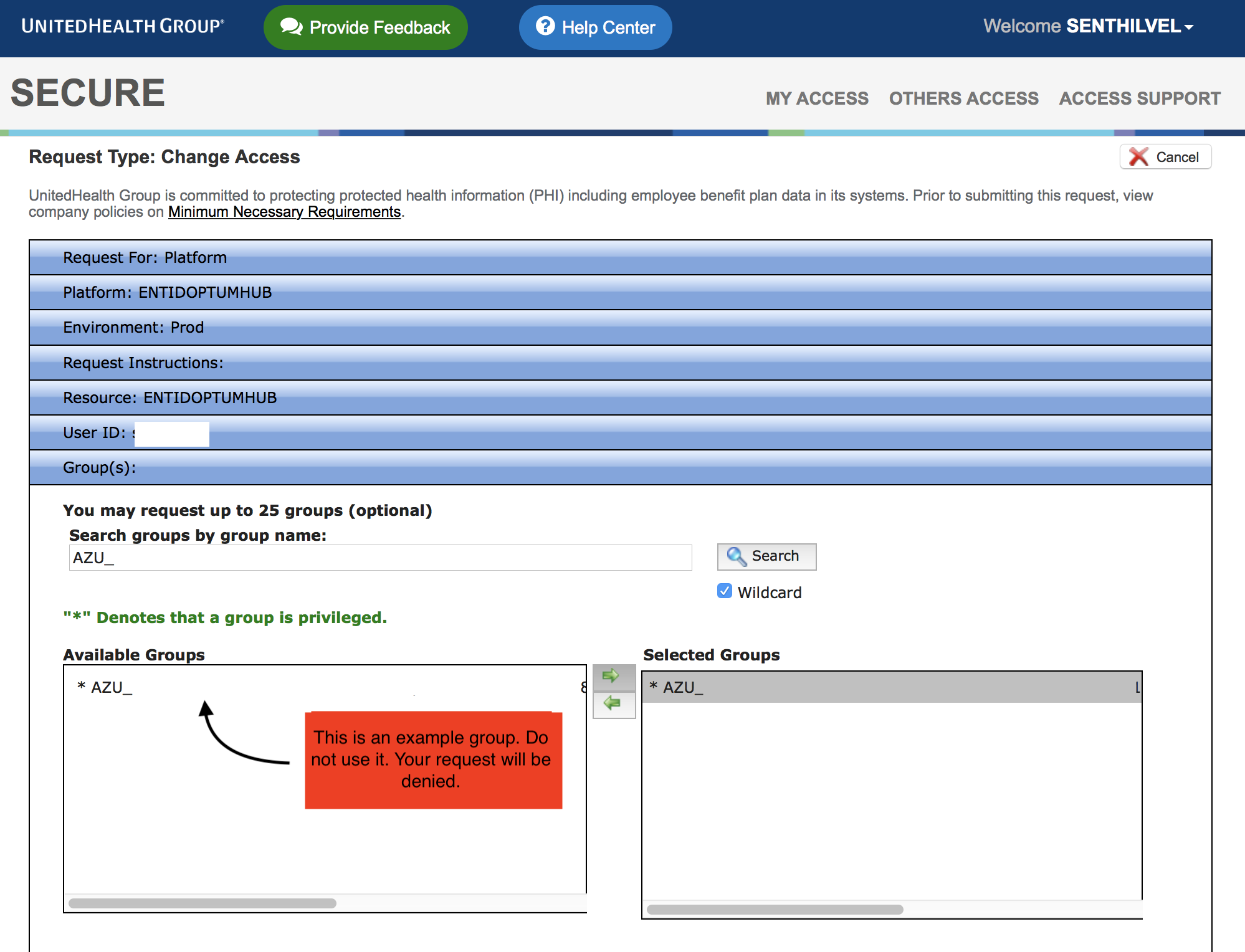
This is how you create ENTIDOPTUMHUB User IDs. It is the same process for both however the User ID will differ by one character/number.

**Request Global Group Membership to Your Subscription**

Note: If you are following this guide to set up your DCE account, you **DO NOT** need to complete this section. Please skip and continue to [accessing the portal](https://commercialcloud.optum.com/docs/getting-started/access-azure-portal/#access-the-portal).

*Once your subscription is provisioned*, you can request membership to your *Secondary ENTID* AD global groups that control access to your subscription. You can also direct your team members to do so.

**Note**: Two groups are created for your subscription, \_Owner and \_Contributor. The groups are mapped to Azure's built-in roles named the same. We recommend only a select few having \_Owner access per subscription. **These groups are unique to your subscription**.

* Click on *Secure Home Page > My Access > Request New Access* and fill out the form as shown below:
* Provide business justification and submit the request.

**NOTE**: You can create additional built-in or custom Azure roles as necessary. Once the groups are present in Secure, team members can request membership as needed. Please see [this guide](https://github.optum.com/dhoude/Guides/blob/master/AzureSecureGroup.md) for set up instructions.

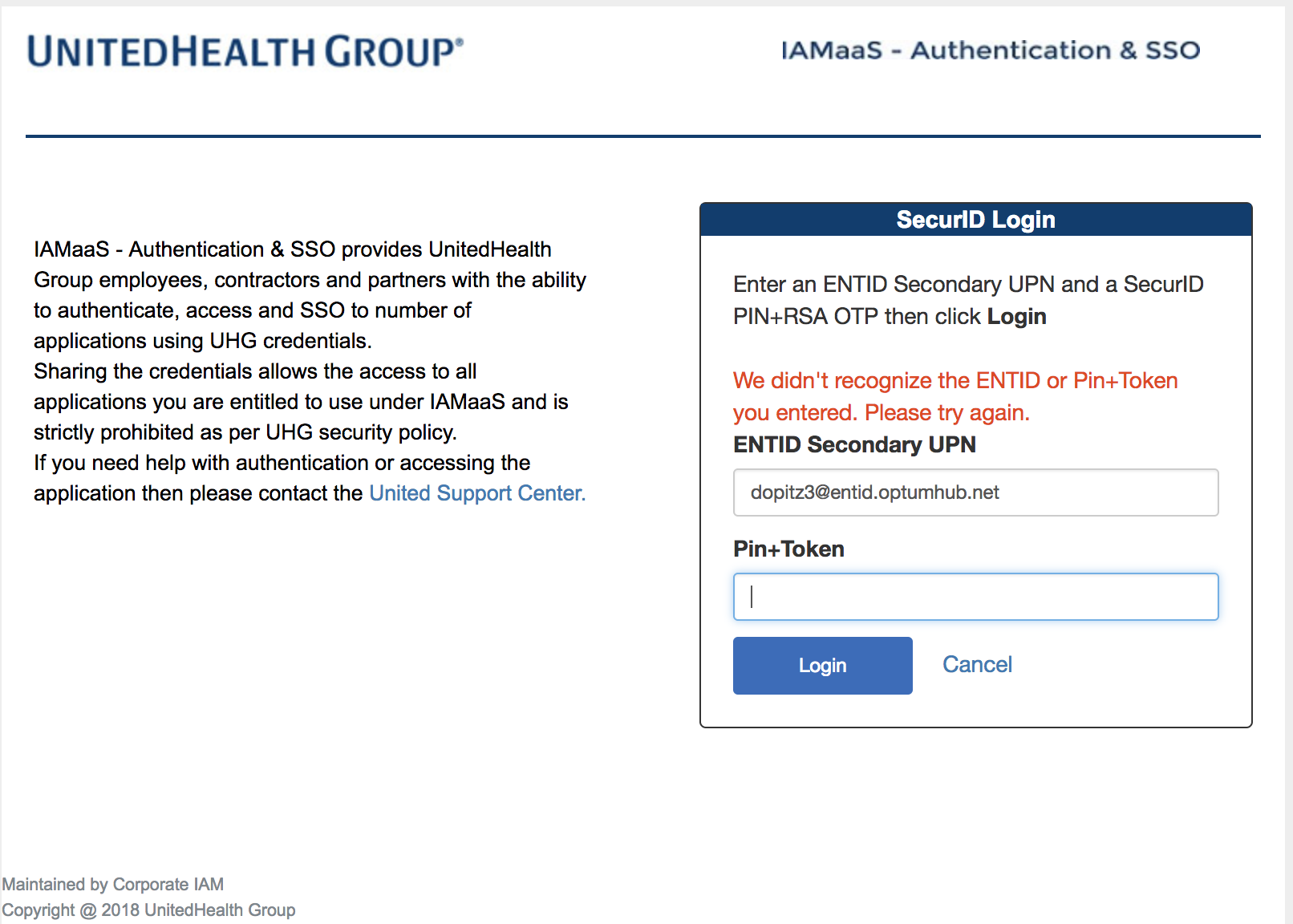
**Access the Portal**

After finishing the above steps, allow for ~3 hours to pass for RSA to properly sync with your secondary ENTID prior to logging into Azure.

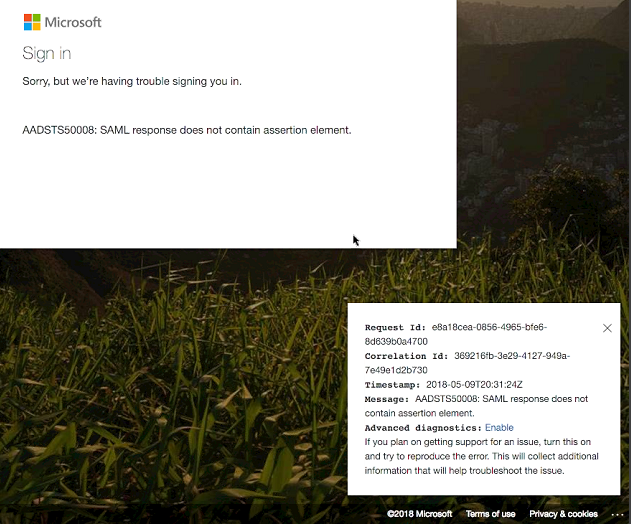
* Navigate to [https://portal.azure.com](https://portal.azure.com/).
  + If you have multiple Azure user accounts, you will be presented with the *Pick an account* dialog. Choose the *Use another account* option, when you login with this account for the first time.
* This will redirect you to *Sign in to Microsoft Azure* dialog. Here, enter your **Secondary ENTIDOPTUMHUB User ID** followed by the *entid.optumhub.net* domain as shown below and click *Next*.
  + *<your-entid-secondary-id>@entid.optumhub.net*
  + Example: [*sthang15@entid.optumhub.net*](mailto:sthang15@entid.optumhub.net)
* You will be taken to **SecureID Login** page. On this page, enter the *same* secondary ENTID login and your RSA token
  + **ENTID SECONDARY UPN**
    - \*<your-entid-secondary-id>@entid.optumhub.net
  + **PIN+TOKEN**
    - If you have **RSA Hard Token**, enter your Pin + RSA token code.
    - If you have **RSA Soft Token**, enter the RSA token code.
* Click *Login* to sign in to Azure.

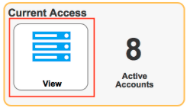
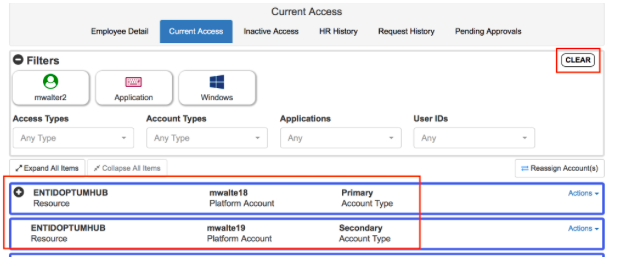
**Troubleshooting**

* ***We didn't recognize the ENTID or Pin+Token you entered. Please try again.***



* + Check that you are entering your correct UPN (*<your-entid-secondary-id>@entid.optumhub.net*).
  + Check that you are entering just your token (No Pin) if you are using a Soft Token.
  + Check that you are entering your Pin+Token if you are using a Hard Token.
  + Check that your MS ID was succesfully added to the AzureAccess Global Group.
  + If you have multiple secondary ENTID's, use your primary secondary ENTID. Additional secondary ENTID's do not have RSA authentication access.
* ***SAML response does not contain assertion element.***



* + This error usually indicates the username (UPN) entered doesn't match with any identity that has been synced with Azure.
  + Wait 30 Minutes to allow for a sync to occur and try again.
  + If you still recieve the error be sure that you created the Secondary ID in the correct domain (ENTIDOPTUMHUB).
* ***How do I check if I have a primary and/or secondary ENTID created?***
  + In [Secure](https://secure.uhc.com/) click the "View" button under current access.  
    
  + Click "Clear" in the top right corner. If you have IDs associated with the ENTID domain they will appear as shown below. 

## Authentication

MSID

ENTID

Citrix with ODA

Optum Laptop with VPN

## Financial Management

#### Regions and Pricing

#### Regional Uptime Statistics

#### Monthly billing

#### Data Ingress/Egress Costs

<https://azure.microsoft.com/en-gb/pricing/details/bandwidth/>

#### Chargeback Costs

Enterprise Technology will facilitate the billing and chargeback for resources (compute, memory, storage etc.) used on public cloud. To enable a streamlined process for reporting, the following processes are put in place:

* Optum Technology manages the Public Cloud Master accounts.
  + An enterprise requirement - no standalone accts are allowed per: EIS, Legal, and ES&P policies
* Individual cloud accounts will be provided to Application Development Teams so they may provision their application components using IaC (Infrastructure as Code).
* Chargeback/finance reporting will be done by Optum Technology in collaboration with Optum Finance.
* Licensing of any specific software/services purchased from the public cloud catalogs will be the responsibility, including compliance, of the application teams.
* Bottom-line, the chargeback is two-fold ($1.50 rate card applied to actual CSP usage and a $1k fixed/mo/acct enablement)

**Estimating Chargeback Costs**

* Use the [Azure](https://azure.microsoft.com/en-us/pricing/#explore-cost) or [AWS](https://calculator.s3.amazonaws.com/index.html) Cost Calculators to estimate your hosting costs
  + Subtract 15% from the estimated cost (or multiply by 0.85)(this is our private CSP discount rates)
* Multiply by 1.50 (this gives you the rate card amount)
* Finally, there is a Per-Account/Per-Subscription enablement charge set @ $1,000 per month
  + This is Optum's charge which covers: Cloud service provider enterprise support agreements, central logging infrastructure, launchpad polices and deployment, administrative costs. This includes green dollar expense to Microsoft and AWS, as well as the supporting resources and components of Optum Technology and enterprise security.

**Example/Hypothetical of a Product's Charge Breakdown**

* 2 AWS accounts (1 for Prod workload, 1 for non-prod) = $2,000/mo.
  + Prod account Actuals 'usage' as charged by AWS = $6,000
  + Non-Prod account Actuals 'usage' as charged by AWS = $2,500
  + Total accounts' Actuals 'usage' = $8,500
  + -15% Cloud Service Provider Discount = ($1,275)
  + +50% Enablement (Optum rate card) = $3,612.50
  + Total Enablement + Actuals = $10,837.50
  + TOTAL for the month, as examples above = $12,837.50

## Reconciling your GL charges with Finance

Chargebacks are billed for the previous month’s usage (1 mo in arrears). Meaning, for example - February’s bill (what you and your Finance team see on your ledger on the Feb line) will actually be for January’s Cloud usage.

Once an account is closed you should expect to receive your last bill the month after your close date.

#### Costs and Chargeback

<https://cloud.optum.com/docs/getting-started/chargeback/>

##### Health Care Cloud Capability Costs

Launchpad automates key security and compliance requirements to accelerate the adoption of Public Cloud. As with all cloud services, [Launchpad capabilities](https://cloud.optum.com/docs/launchpad/overview) contribute incremental direct costs that are aggregated into the total enabling costs of Optum Technology. The Optum Technology (OT) rate card of $1.50 is derived from a holistic view of OT’s financial expectations, **NOT** the direct costs of a single service such as Public Cloud Enablement.

With July 2020 actual results the normalized Public Cloud direct costs are:

* $1.00 is the direct cloud vendors’ costs (an application’s cloud usage after enterprise discounts)
* $0.30 in additional Optum Technology direct costs to enable public cloud broken into 3 catagories
  + $0.08 in additional direct cloud vendors costs (Launchpad: logging, monitoring, security)
  + $0.05 in additional direct cloud vendor costs for enterprise support
  + $0.17 in other HCC Public Cloud direct costs (IT labor, professional services, etc.)

##### Estimating Chargeback Costs

* Use the [Azure](https://azure.microsoft.com/en-us/pricing/#explore-cost) or [AWS](https://calculator.aws/#/) calculators to estimate your hosting costs
* Subtract 15% (Azure) or 16% (AWS) from this estimated cost (UHG Enterprise Discounts)
* Add $500 (Azure) or $200 (AWS) for in subscription/account [Security Costs](https://cloud.optum.com/docs/getting-started/chargeback/#in-subscription-security-costs)
* Multiply this number by 1.50 Optum Technology rate card
* Finally, there is a per-account/per-subscription enablement charge set @ $1,000 per month
  + This $1000 is being removed on January 1st 2021 when we transition in account/subscription Launchpad costs to customer usage similar to [*Security Costs*](https://cloud.optum.com/docs/getting-started/chargeback/#in-subscription-security-costs).

##### Example Application Charge Breakdown:

#### Azure Non-Prod Subscription

| **Detailed Item** | **Amount** |
| --- | --- |
| Application Cloud Usage (list price) | $2,500 |
| -15% Cloud Service Provider Discount | -$375 |
| Estimated Azure Security Center Costs | +$500 |
| Optum Technology rate card ($2,625 \* 50%) | +$1,313 |
| Per subscription enablement charge | +$1,000 |
| **Non-Prod Charges** | **$4,938** |

#### Azure Prod Subscription

| **Detailed Item** | **Amount** |
| --- | --- |
| Application Cloud Usage (list price) | $6,000 |
| -15% Cloud Service Provider Discount | -$900 |
| Estimated Azure Security Center Costs | +$500 |
| Optum Technology rate card ($5,600 \* 50%) | +$2,800 |
| Per subscription enablement charge | +$1,000 |
| **Prod Charges** | **$9,400** |

#### Total Public Cloud Charges: $14,338

##### Reconciling your GL charges with Finance

Chargebacks are billed for the previous month’s usage (1 mo in arrears). February’s bill (what you and your Finance team see on your ledger on the Feb line) will actually be for January’s Cloud usage. Once an account is closed you should expect to receive your last bill the month after your close date.

#### Launchpad Resource Costs

Three sets of capabilities are deployed and managed by Launchpad that contribute incremental costs.

##### In Account/Subscription Security

HITRUST and SOX require the implementation of [Azure Security Center](https://azure.microsoft.com/en-us/services/security-center/) and [AWS GuardDuty](https://aws.amazon.com/guardduty/). These services create incremental usage costs that are billed to subscriptions or accounts directly based on their respective pricing models.

The average Azure team will see an Azure Security Center cost of $500\* per month per subscription.  
The average AWS team will see an AWS Guard Duty cost of $200\* per month per account.

##### In Account/Subscription Launchpad Centralized Logging Resources

Several Azure and AWS resources are deployed into every account or subscription to facilitate HITRUST and SOX required logging and monitoring. A detailed overview is available in the [launchpad documentation](https://github.optum.com/healthcarecloud/launchpad_documentation#launchpad-services). These costs ($1,200\* in Azure and $800\* in AWS) are paid by Optum Technology, not application teams, and are covered by the Optum Technology rate card. As this implementation is further optimized (below $1,000) these costs will transition to customer usage and the $1,000 enabling fee will be removed.

All the Launchpad resources are tagged with ASK ID (UHGWM110-021452, UHGWM110-020631) and have resources naming prefix of "lpcl".

##### In Subscription Launchpad Centralized Logging Resources

Estimated cost to support backend Centralized Logging data streams, log retention and Splunk hosting is ~$800\* per month per account or subscription. These costs are paid by Optum Technology, not application teams, and are covered by the Optum Technology rate card.

\*Cost estimated based on actual usage of an typical application ($10k per month) for July 2020

## Patterns and Practices

#### Reference Architectures

#### Infrastructure-as-Code (Terraform)

#### Workload placement

*Workload Placement* is the thoughtful positioning of technical workloads and data across the whole of the UHG landscape, inclusive of public cloud, private cloud, traditional Optum data centers, and SaaS. Teams need to balance the advantages of public cloud, the economics of the company, and the location of the data and the users. Ultimately, the teams are fully accountable for their application placement and operations. At this time, initial bias is to maximize the advantages of public cloud where responsible to do so. The advantages of public cloud come from building cloud-native applications and operating them effectively (not lift-and-shift of VMs). At the time of this revision (Q2 2019), the greatest barriers to having cloud-native apps and cloud-native operations is the team readiness. Despite the bias for public cloud, dev teams that attempt to lift-and-shift VMs, or build non-cloud-native applications, are not using the public cloud responsibly.

**Workload Placement Governance**

Workloads will not be deployed to the public cloud without appropriate oversight and guardrails. The goals of public cloud governance and monitoring are to:

* Provide for an orderly adoption of public cloud services with visibility into who is utilizing? what is being used? how much we are spending? and what risks we are exposing?
* Provide key stakeholders approval at point of decision for workload placement
* Provide for the on-going monitoring and review of products and services used on public cloud for risk evaluation, financial oversight, and future contract negotiations
* Public cloud governance is predicated on enabling code and platforms (i.e. [Commercial Cloud](https://github.optum.com/CommercialCloud-EAC) - <https://github.optum.com/CommercialCloud-EAC>) that accelerate adoption. Teams must use [LaunchPad](https://commercialcloud.optum.com/) (<https://commercialcloud.optum.com/>) to provision, deploy, and manage their public cloud accounts

**Workload Placement Criteria**

There are some critical criteria that teams need to consider when placing workload. Application teams may demonstrate a use case for the Optum Public Cloud offerings based upon one or more of the following.

|  |  |  |
| --- | --- | --- |
| **Criteria** | **Observations** | **Place Workload in Private Cloud/Optum DC If..** |
| Commerciality | This is a proxy for “how much does UHG control the size and intensity of the usage curve” | The software is NOT licensed to another party  The software is NOT used by large or unmanaged populations (i.e. the internet)  The software is NOT at risk for "going viral" (such as a portal) |
| Volatility/Instability | We don’t want volatile workload in Optum data centers because it likely ties-up capacity in services that are frequently idle.  It's hard to manage data centers effectively in the face of highly volatile loads | The application has stable, forecastable capacity utilization over the course of the year.  The application has minimal seasonal or other volatility |
| Data Gravity | Big data is often challenging to schlep (carry/move) back and forth between data centers and AZsData that is heavily integrated is bad to draw out from the gravity of the integrations. Teams often underestimate the cost of data egress or hybrid connectivity | Heavy data dependency on unmovable legacy sources (i.e. MF) |
| Integration Gravity | Applications that are deployed to public cloud should not have multiple dependencies on integrations located in the Optum data center | Heavy integration dependency on unmovable legacy sources (i.e. MF) |
| User Gravity | If the users are all in the UHG network (and if the data is all in the data center), then it’s kind of silly to move the app to public cloud.  This is because we would move the data twice – once to get to the compute in the cloud, and again when it is used inside the UHG network | Users are all in the UHG network AND there is significant data or integration gravity |

**Idealized Workload Placement Decision Tree**

A close up of a map

Description automatically generated

**Idealized Workload Placement Decision Tree – Private Cloud**

A screenshot of a cell phone

Description automatically generated

**Secondary Considerations**

* Workload Quarantine.  Is this something that we don’t trust in our (very flat) internal network?
* Internet-facing B2C or geographically sensitive consumption.  And isn’t just because the team doesn’t know how to use a CDN
* Un-adopted/emerging Tech or Critical feature availability.  Is there something that you need at a CSP (Cloud Service Provider) that is unavailable in our datacenters?  Are you experimenting with new technology that has significant barriers to use in our data centers?  This also includes needing a cloud native service, such as Azure IOT, Azure Data Factory, etc.

**What Factors Suggest Fast-track Workload Placement to Public Cloud**

Some projects may qualify for “fast-track” handling.  Generally, a “fast-track YES” comes from readily apparent factors such as:

* The data is already in the cloud, or is minimal to synchronize
* The integrations are already internet-facing
* The user-base is internet-based
* Majority of the system in the cloud (don’t take one part of an overall system and stick it in cloud, to the detriment of the whole)
* Workload volatility is 1+ orders of magnitude variability (i.e. the peak load is at least 10x the average load) and is less than 50% of the overall time
* User-base is all over the world AND THEY HAVE A REASON THAT CDN WON’T SOLVE
* Modern, cloud-native architecture (including externalized config, stateless containers, proper secrets management, log shipping, etc.

**What Factors Oppose Fast-track Workload Placement to Public Cloud**

Some factors do not support a fast-track disposition.  Either the “quick no” or the “quick maybe” really just mean “we should talk about this”.

* Factors that suggest a “Quick No” for Workload Placement comes from:
  + All/most of the data and integrations are in a UHG Datacenter
  + All/most of the users are on our network
  + Stateful/old school architecture (e.g. stateful VMs vs. stateless containers/functions)
  + Recreating significant existing features of the cloud platform (<-- Don't do this.  See the [Tech Taxonomy](http://technology.optum.com/) (<https://tech.optum.com/login>) and filter by your environment.)
* “Quick Maybe” for Workload Placement comes from:
  + Workload Quarantine (this requires EIS input) – EIS already has some criteria here
  + “Critical feature availability” (this is as often the result of ignorance as need)
  + Same ^^ with un-adopted/emerging tech.
  + A commercial app that we’re already selling from out of our datacenter that we want to move to cloud. (EA is usually in-favor of these, but it’s worth a conversation about data gravity)

**Where can I find more information about Workload Placement and Public Cloud?**

Visit the [Workload Placement](https://cloud.optum.com/docs/getting-started/workload-placement) (<https://cloud.optum.com/docs/getting-started/workload-placement/>) document for [Health Care Cloud (HCC)](https://cloud.optum.com/) (<https://cloud.optum.com/>).

**Cloud Considerations for Government Agencies**

When dealing with customers that are government agencies, are heavily regulated, or simply have contracts that look like a government agency, there are some specific considerations. Many of these customers have physical data storage, location, and handling requirements that constrain geography or other parameters for our use. Some want us to use public cloud, some prevent us from using public cloud, and some don't care. As a bidder/provider of our products and services, we need to be able to present a variety of hosting and workload placement options to suit this variation. In addition, our Public Cloud onramp (LaunchPad) does not distinguish the specific FISMA/FedRamp offerings from AWS and Azure. This may change as LaunchPad evolves. Bottom line, it depends. But here are some considerations to keep in mind as you solution:

* Because this is for a government or similar external client, this case ticks the box for commerciality noted above, so the default position is public cloud (Azure, then AWS). Of course, this is a bias, and should adjust in the face of customer requirements
* Requirements are very consistent between FedRamp/FISMA controls with about 35% of the requirements focused on infrastructure and 65% of the requirements on process. For the things that a CSP can control, their implementations are very consistent. But, there's a lot that are on us to own
* At this time, Azure still presents (generally) better risk/cost terms. Start there if your customer is looking for Public Cloud
* Don't forget the other aspects above, such as volatility of the workload and data/user/integration gravity. Gravity might be challenging to pin down

Reference:

<https://architecture.uhg.com/docs/ea-workload-placement-guidance.html>

<https://commercialcloud.optum.com/docs/getting-started/workload-placement>

#### Best practices

#### Configuration management

#### Desired State Configuration

#### Use cases

WVD

Good morning all,

Thanks for the time yesterday.  With respect to getting started with WVD, I wanted to share a few resources with you:

* Primary [documentation site](https://docs.microsoft.com/en-us/azure/virtual-desktop/), which can be a go-to resource for you.
* Going beyond core documentation, we have a new [“Quickstart”](https://www.wvdquickstart.com/index) site that is perfect for what you’re trying to do, which includes:
  + pre-reqs and establishing necessary connectivity
  + Automated provisioning with templates
  + Devops pipeline for adding users, etc.  
      
    Note – strongly suggest you consider testing [multi-session](https://docs.microsoft.com/en-us/azure/virtual-desktop/windows-10-multisession-faq) configuration in your evaluation plans, as its one of the most impactful ways to manage your costs.
* For those of you that like to learn via videos, there’s a robust [video playlist about Windows Virtual Desktop](https://www.youtube.com/playlist?list=PLXtHYVsvn_b8KAKw44YUpghpD6lg-EHev), which includes some instructional guidance, including:
  + Part 1 – [preparation](https://youtu.be/yAKmuZpwVyg) (< 10 minutes)
  + Part 2 - [Deploying](https://www.youtube.com/watch?v=Xhu7CltjS8w) (< 12 minutes)
  + Part 3 - [Optimizing](https://youtu.be/I8gcl8Zvcps) (< 13 minutes)

I’d like to suggest we setup periodic check ins for a few weeks while you’re running your evaluation.  Tuesday or Wednesday afternoons?

Also, to help us provide you the best guidance and support, in our next conversation, I’d like to get more details on:

* Details your specific user profiles, and how we can evaluate the experience  (e.g., ease of setup, performance, app compatibility, unique monitor/input device needs, etc.) for each user profile (e.g., regular PC users, contractors, clinical site scenarios, etc.)
* Complete evaluation criteria you’ll use to define ‘success’
  + Ease of management for your virtual desktop engineering team – we discussed this as a high priority
    - Setup, deployment
    - Monitoring/management
    - Scaling
  + Overall costs?
  + ???
* Role of partners?  As we think beyond evaluation period, are you considering engaging help in executing your deployment?  We can help you in finding partners with expertise.

## Operations and Support

Governance

RACI

Solutions Architecture/Engineering Support

Pre-implementation

Post-implementation

## Disaster Recovery

## Future State

MSO

## Definitions

<https://commercialcloud.optum.com/docs/intro/public-cloud-terms-and-conditions#cloud-user>

#### API Adoption

Legacy services exposed via APIs to cloud; no new infrastructure deployments; proxy deployment on API gateway; APIs exposed using gateway bridge

#### Cloud Bridge

Hybrid-bridge solution utilizing both legacy infrastructure and cloud VMs for augmentation of existing systems; partial deployment/partial environment in cloud

#### Cloud Enabled

Fully deployed cloud solutions on UCI/NGIS; greenfield applications; cloud provisioned environments

#### Non-adopters

Legacy systems/applications; hosted on physical servers or in external data center of hosting provider; not creating or using APIs