Dom Moore
IAM- Docker

## Scenario

HappyCorp recently suffered an intrusion via a compromised email account because the user failed to establish a secure password on the email account, and reused the password across multiple web apps. The intruder was able to determine the password on the employee's personal music player app, then reused the password to successfully access the employee's company email account. The intruder used the hijacked account in order to spam the entire organization with phishing emails that appeared legitimate due to the authentic sender account, causing confusion and problems throughout the company.

The CEO would like to better manage all systems identities across the organization in order to prevent security breaches and asked you to model some kind of identity management system that would unify the disparate web app accounts under a single sign-on per employee.

### Problem Area

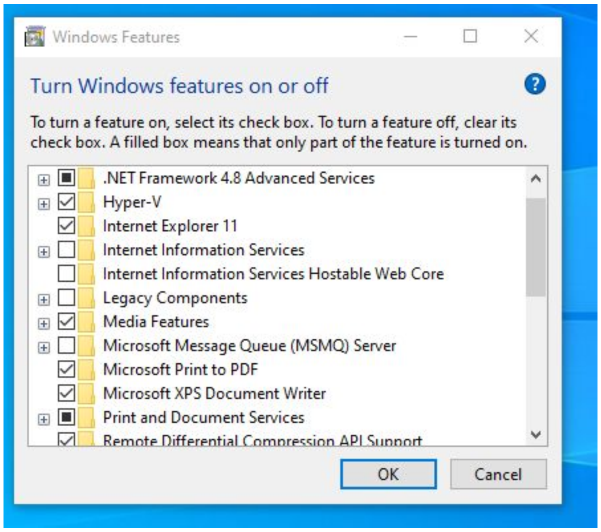
When starting to download lead docker to my windows pc I had some issues getting the program to deploy onto my os, I received error messages that my system did not allow virtual machines but this was not correct my system was configured in the BIOS to allow virtualization. After some research, I found out that docker is not natively supported on windows 10 home version but only on pro and enterprise editions.

I continued to research the problem and one of the issues that hyper- v is not installed on windows 10 home edition, but I was able to find steps to download a program that would allow hyper-v to be enabled on my windows pc, but after installing and enabling hyper-v I was still unable to find a solid solution for getting docker to deploy on my windows 10 home pc.

### Solution

After a number of hours trying to troubleshoot workarounds for my windows 10 PC, I decided to pivot to using my macOS and was able to install Docker, keycloak to complete the task of the lab.

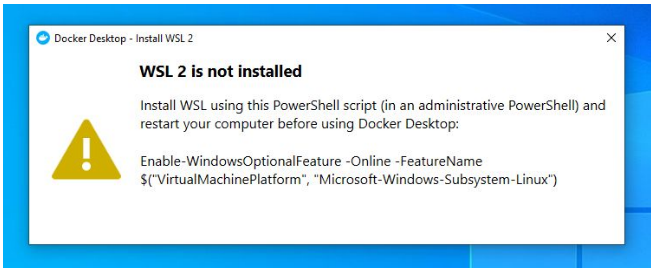
### Error Images



Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

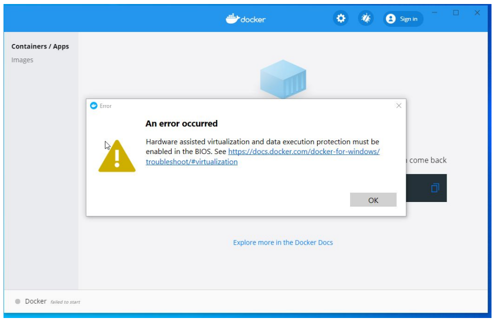
- ■ .NET Framework 4.8 Advanced Services
- ☑ Hyper-V
- ☑ Internet Explorer 11
- □ Internet Information Services
- □ Internet Information Services Hostable Web Core
- □ Legacy Components
- ☑ Media Features
- □ Microsoft Message Queue (MSMQ) Server
- ☑ Microsoft Print to PDF
- ☑ Microsoft XPS Document Writer
- ■ Print and Document Services
- ☑ Remote Differential Compression API Support



WSL 2 is not installed

Install WSL using this PowerShell script (in an administrative PowerShell) and restart your computer before using Docker Desktop:

```
Enable-WindowsOptionalFeature -Online -FeatureName
$("VirtualMachinePlatform", "Microsoft-Windows-Subsystem-Linux")
```



An error occurred

Hardware assisted virtualization and data execution protection must be enabled in the BIOS. See https://docs.docker.com/docker-for-windows/troubleshoot/#virtualization

Docker failed to start

# Part 1: Deploying Keycloak as a Docker Container

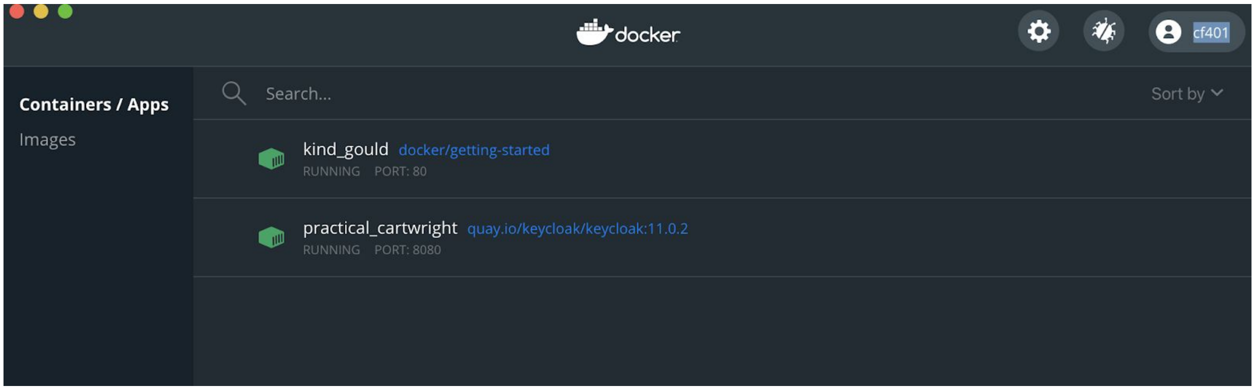
Step 1- Sign Up for a Docker ID.

Step 2- Install Docker Desktop on your host system.

Step 3- Deploy Keycloak SSO to your host PC

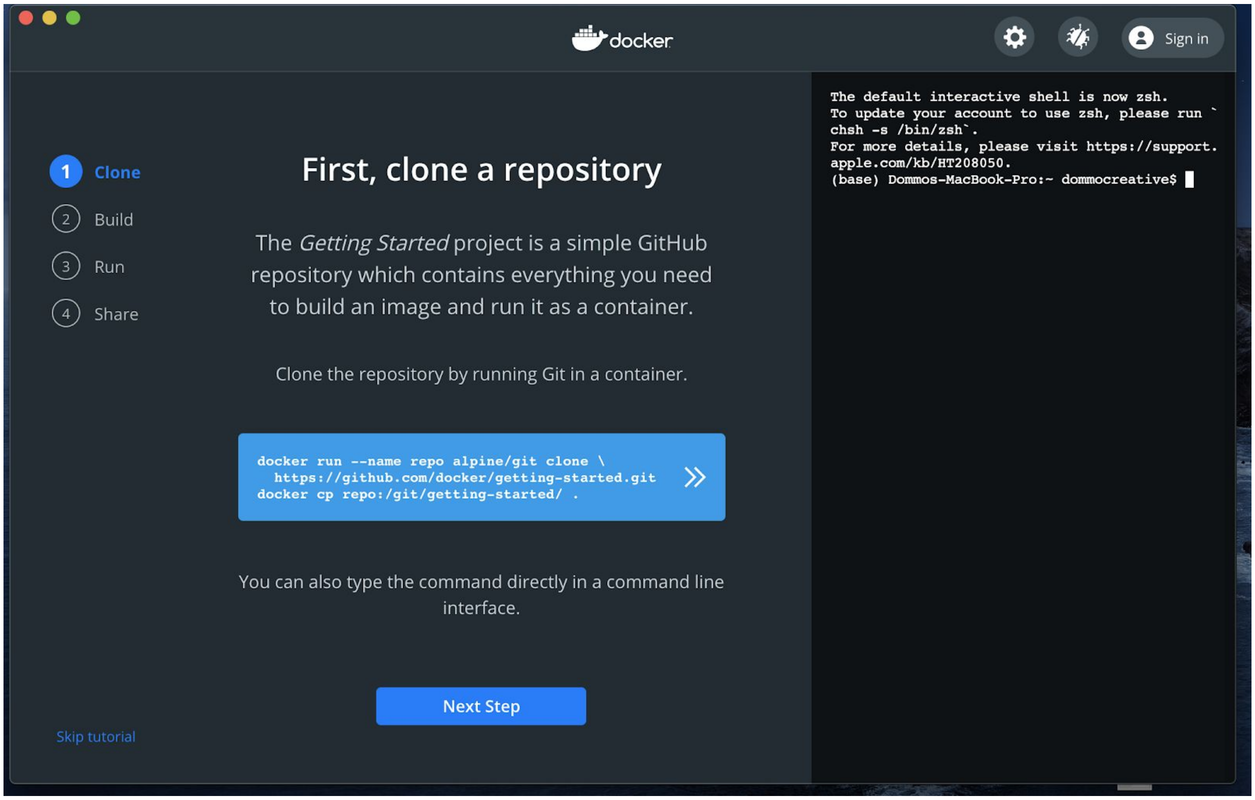
Step 4- Issue the appropriate Docker commands in GIT Bash

## Deploy Docker / Keycloak Images



kind_gould docker/getting-started
RUNNING PORT: 80

practical_cartwright quay.io/keycloak/keycloak:11.0.2
RUNNING PORT: 8080



First, clone a repository

The *Getting Started* project is a simple GitHub repository which contains everything you need to build an image and run it as a container.

Clone the repository by running Git in a container.

```
docker run --name repo alpine/git clone \
  https://github.com/docker/getting-started.git
docker cp repo:/git/getting-started/ .
```

You can also type the command directly in a command line interface.

```
The default interactive shell is now zsh.
To update your account to use zsh, please run `
chsh -s /bin/zsh`.
For more details, please visit https://support.
apple.com/kb/HT208050.
(base) Dommos-MacBook-Pro:~ dommocreative$ 
```

# Part 2: Keycloak SSO Server Operation

Step 1- Access Keycloak via the web browser

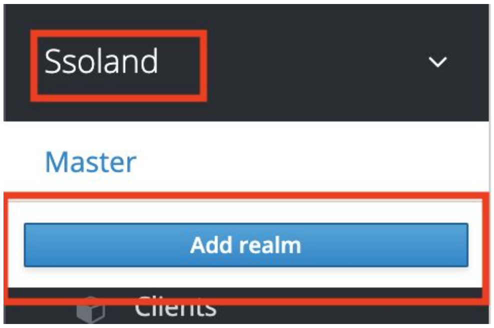
Step 2- Create a realm

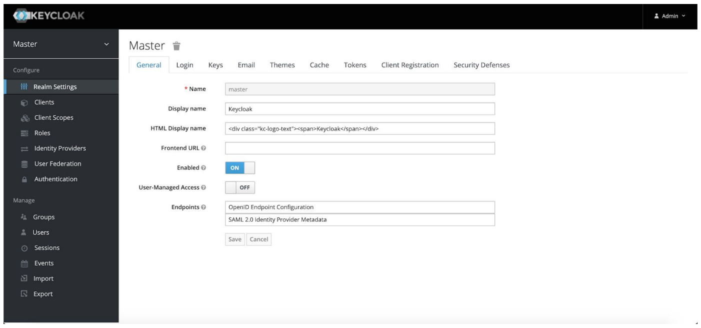
Step 3- Create a user

Step 4- Associate a web app to your Keycloak

Step 5- Add multi-factor authentication to your user by implementing an OTP policy in Keycloak

### Create realm





* Name: master

Display name: Keycloak

HTML Display name: <div class="kc-logo-text"><span>Keycloak</span></div>

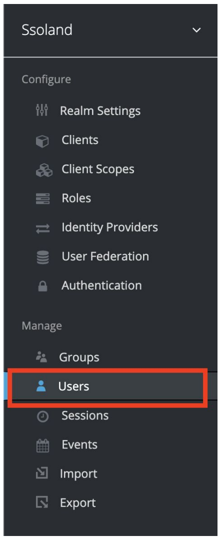
Frontend URL:

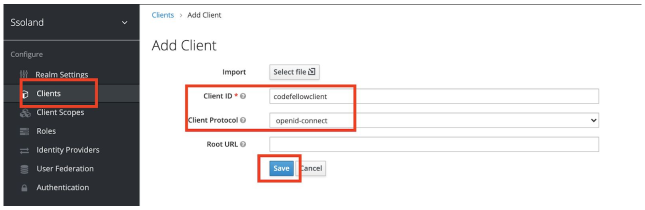
Enabled: ON

User-Managed Access: OFF

Endpoints: OpenID Endpoint Configuration; SAML 2.0 Identity Provider Metadata

### Create user





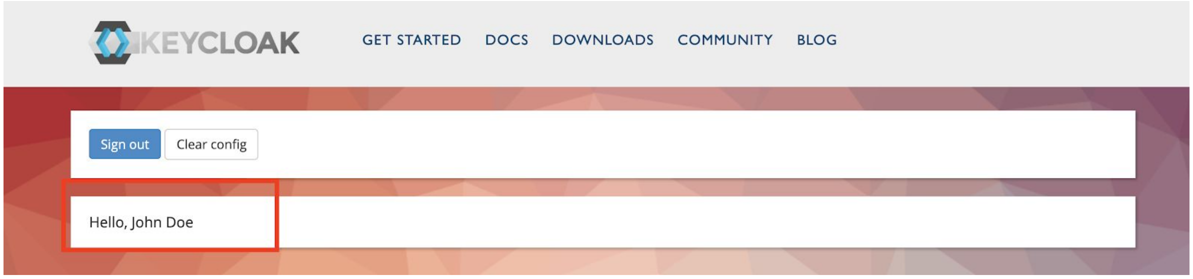
Import:

Client ID *: codefellowclient

Client Protocol: openid-connect

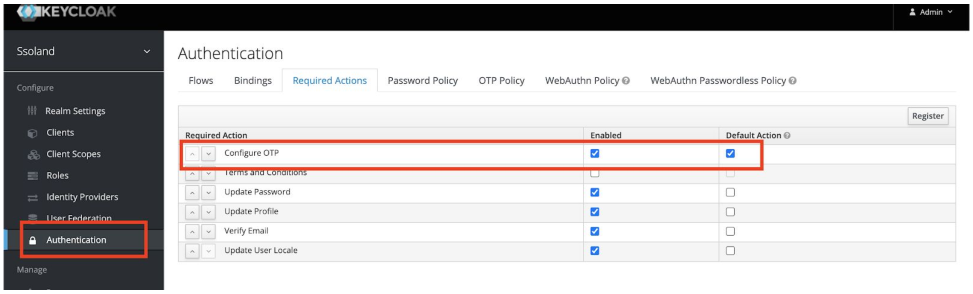
Root URL:

### Web app

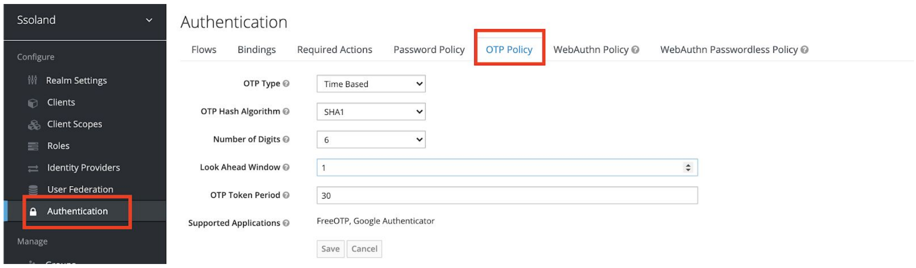


Hello, John Doe

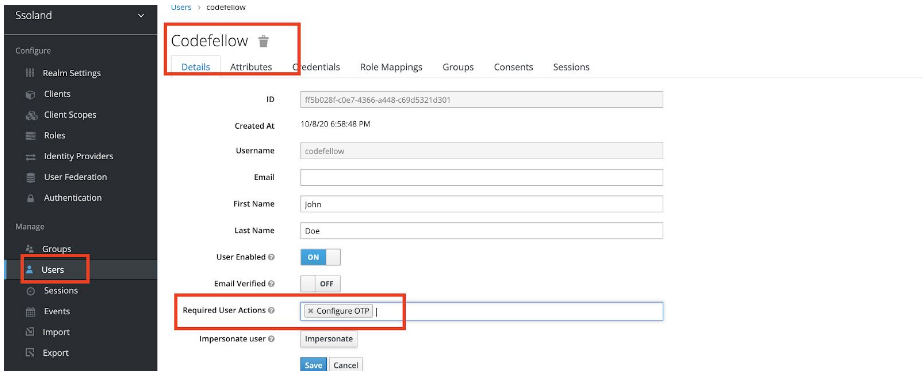
# OPT Policy / MFA



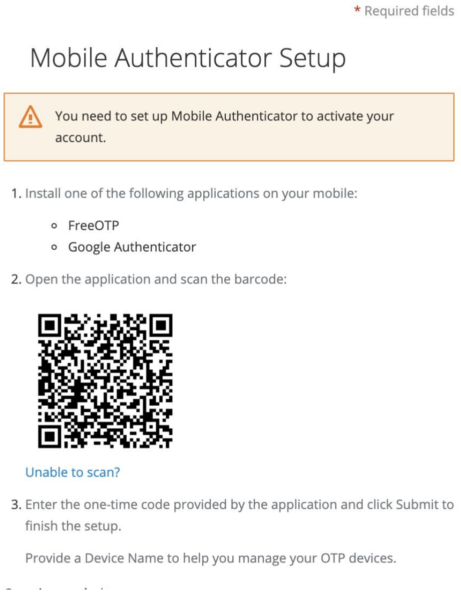
| Required Action | Enabled | Default Action |
|---|---|---|
| Configure OTP | ☑ | ☑ |
| Terms and Conditions | ☐ | ☐ |
| Update Password | ☑ | ☐ |
| Update Profile | ☑ | ☐ |
| Verify Email | ☑ | ☐ |
| Update User Locale | ☑ | ☐ |



| | |
|---|---|
| OTP Type | Time Based |
| OTP Hash Algorithm | SHA1 |
| Number of Digits | 6 |
| Look Ahead Window | 1 |
| OTP Token Period | 30 |
| Supported Applications | FreeOTP, Google Authenticator |



| | |
|---|---|
| ID | ff5b028f-c0e7-4366-a448-c69d5321d301 |
| Created At | 10/8/20 6:58:48 PM |
| Username | codefellow |
| Email | |
| First Name | John |
| Last Name | Doe |
| User Enabled | ON |
| Email Verified | OFF |
| Required User Actions | × Configure OTP |



* Required fields

## Mobile Authenticator Setup

You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:
   - FreeOTP
   - Google Authenticator
2. Open the application and scan the barcode:

   Unable to scan?
3. Enter the one-time code provided by the application and click Submit to finish the setup.

   Provide a Device Name to help you manage your OTP devices.

### Part 3: Reporting

- Compose an ITIL-compliant request for change (RFC)

# Client Solution Proposal Deliverable

Prepared for

HappyCorp

September 25, 2020

# Proposal Summary

## Proposal

The recent security breach that occurred at Happy Corp did to a lack of protocol and security policy in place for system and password security, we are proposing to implement a system using a containerized program that would host the internal system and using keycloak to create access management protocol for password protections and management of user privileges.

### Benefits to Fife School District

- Unified system for the entire organization
- Identity and access management of users
- Best practices for system security
- Password policy
- Preparation for possible audits

| | |
|---|---|
| Application ID: RFC80991 | Date: 10/08/2020 |

| | |
|---|---|
| Change Owner: | Initiator of the Request for Change: |
| Happy Corp Inc | Mike Jones, Superintendent |
| Priority: | Reference earlier proposal if applicable: |
| High | N/A |

Description of the requested change:

**Description of problem :**

employee failed to establish a secure password on the email account and reused the password across multiple web apps. The intruder was able to determine the password on the employee’s personal music player app, then reused the password to successfully access the employee’s company email account. The intruder used the hijacked account in order to spam the entire organization with phishing emails that appeared legitimate due to the authentic sender account, causing confusion and problems throughout the company.

Keycloak provides a way for your organization to protect its systems by providing access management services for your platform. It will allow us to create a database of users and set policies around how users can access and navigate within your eternal systems, this will assist I password policies and help ensure a more secure client platform.

| Consequence if not implemented: |
|---|
| ● System breaches<br>● Loss of customer<br>● Data loss<br>● Expensive recovery cost<br>● Non-compliance issues |

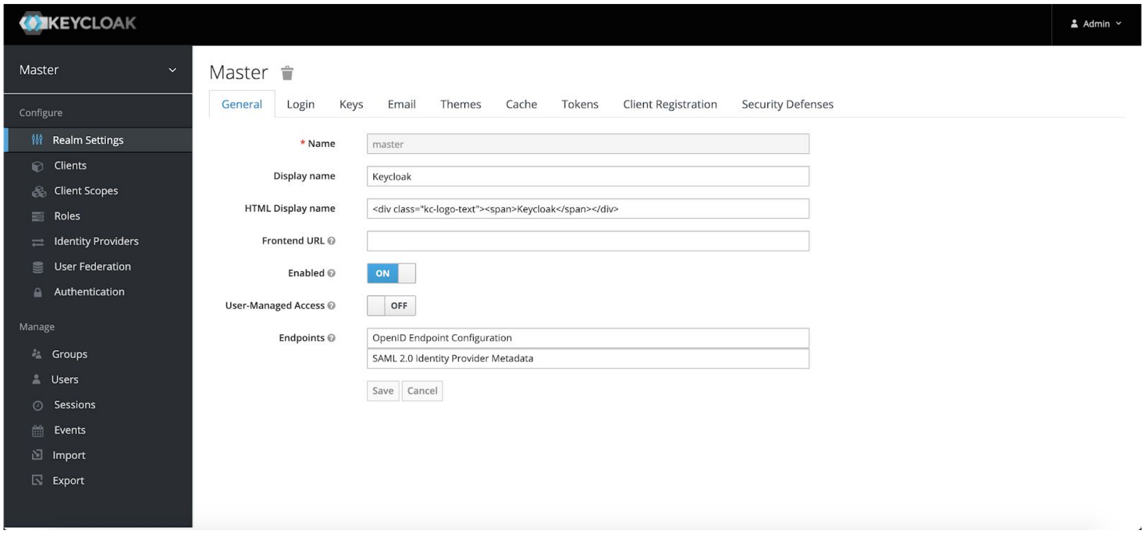
| Services affected by the change: |
|---|
| ● All district departments which depend on the use of the IT infrastructure (itemized below) |

| IT infrastructure components affected by the change: |
|---|
| ● Web app<br>● Operating system |

| New technology being implemented: |
|---|
| ● Docker<br>● Windows 10 pro or enterprise<br>● KeyCloak |

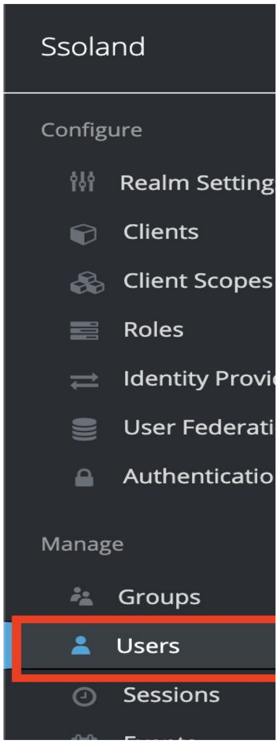
| Risks during the implementation of change: |
|---|
| ● Training users on a new protocol<br>● Upgrading software<br>● Security |

## Real Creation:



| | |
|---|---|
| * Name | master |
| Display name | Keycloak |
| HTML Display name | <div class="kc-logo-text"><span>Keycloak</span></div> |
| Frontend URL | |
| Enabled | ON |
| User-Managed Access | OFF |
| Endpoints | OpenID Endpoint Configuration<br>SAML 2.0 Identity Provider Metadata |

## User Creation:



| Task to perform | Suggested start date: | Suggested date of completion: |
|---|---|---|
| System evaluation | October 10, 2020 | October 12, 2020 |
| Analyze the Scope of Work | October 13, 2020 | October 14, 2020 |
| Migrate system to Keycloak | October 15, 2020 | October 20, 2020 |

**Software:**

| Item: | Cost: |
|---|---|
| Docker | Average Annual Cost: $ 750.00 |
| Windows 10 Pro | Average Annual Cost: $ 309.00 |

| Personnel resources: | Estimated man hours: | Cost estimate: |
|---|---|---|
| 1 IT Professionals | 64 | $3840 |

| | |
|---|---|
| Projected migration budget: | N/A |

| | |
|---|---|
| Projected monthly budget: | N/A |

Is the budget already cleared by the Change Advisory Board? **Yes___** **No___**

Attach any additional supporting document if applicable:

---

Is the request (please circle): **Approved** **Rejected**

| The priority assigned by Change Management (please circle): | | | |
|---|---|---|---|
| **Standard** | **Normal** | **Major** | **Emergency** |

Reason for rejecting (if applicable):

If approved, are there any restrictions?

Authorized signature of the Change Manager:

____________________________________ Date:_____________

Change reviewers:

1. ______________________________
2. ______________________________
3. ______________________________