CHS Community Health Systems

Information Technology Security Procedure Outline

Revision 1.0
9/5/2008

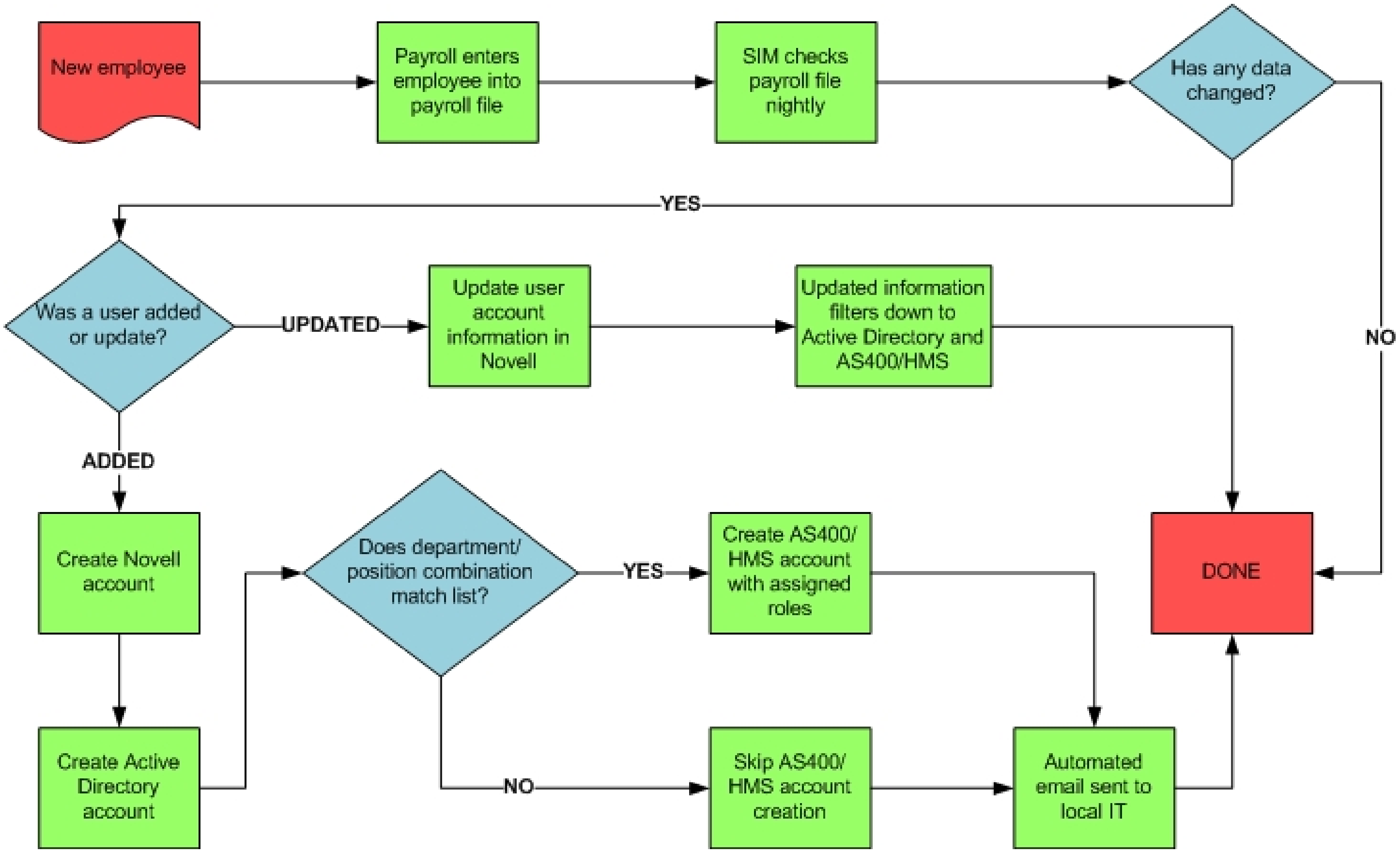
Table of Contents

SIM Overview

SIM (Security Identity Management) is a process that provisions new accounts, modifies existing accounts, and disables accounts based on changes in Payroll. After a facility is live on Payroll, the information from Payroll is processed nightly and any necessary changes are made with regard to user accounts.

For example, if a new hire is entered into Payroll, the following night SIM will provision a new account for that user. The access in HMS will be dependent on the Position and Department code entered for the user. If an existing user changes positions and/or departments, then their access may also change in a similar manner.

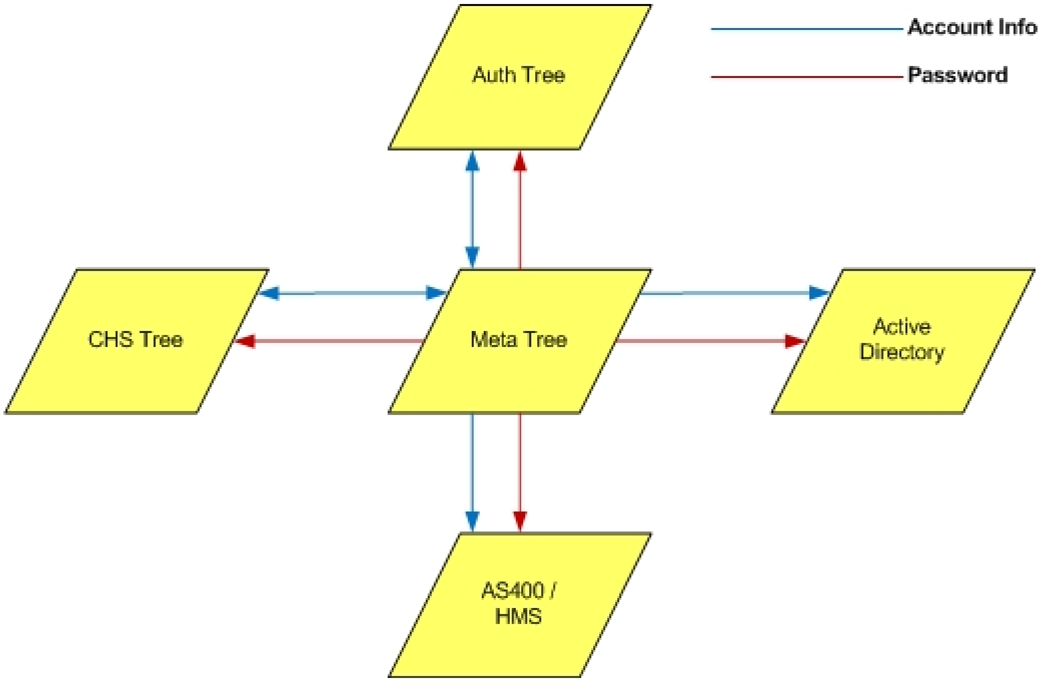
It is important to note that HMS access is granted based on the position and department combination. It is vital that this information be correct in the payroll file.


New employee
Payroll enters employee into payroll file
SIM checks payroll file nightly
Has any data changed?
YES
NO
Was a user added or update?
UPDATED
Update user account information in Novell
Updated information filters down to Active Directory and AS400/HMS
ADDED
Create Novell account
Create Active Directory account
Does department/ position combination match list?
YES
Create AS400/ HMS account with assigned roles
NO
Skip AS400/ HMS account creation
Automated email sent to local IT
DONE

CHS User ID Structure

In order to better understand how a User ID is affected, you must understand the structure that surrounds a User ID.

The first graph below shows the relationship between the different trees. As you'll notice, the **Meta Tree** is the control. Whether SIM or the Contractor's DB generates the User ID, the control account is found in the **Meta Tree**. All other accounts should be created and linked to the Meta account.



The second graph below indicates which Tree interfaces with what system.

Authentication Control List

Auth Tree	CHS Tree	Meta Tree	Active Directory	AS400 / HMS
• VPN Access	• Novell account	• Auth Tree • CHS Tree (does not control manually created accounts) • Active Directory • AS400 / HMS	• Citrix	• iMed • ProMed

Go-Live

Go-Live is a term that indicates a hospital is transitioning from their current financial or clinical system to CHS' financial or clinical system.

During a Financial Go-Live, unique User IDs are generated based on information provided by the onsite Analysts. About 2-3 weeks after a hospitals Go-Live date, a report is generated that compares the information in the hospital's Payroll file and the information in Meta. This report is then emailed to the local IT Director(s) and the Project Manager. In the body of the email, there are details for each comparison column.

Remedy

Remedy uses the sequence of ITIL recommended Standards. ITIL stands for Information Technology Infrastructure Library. BMC Remedy combines incident management, service request management, configuration management, and change management into one cohesive application suite. This integration allows modules to "talk" with each other and share information.

Currently we use the following:

- Incident Management
    - The Incident Management Console is a centralized location for the Support Staff to view assigned Incidents, important Broadcasts, and navigate within the ITSM application. It gives the user a quick view of the Incidents in the system by showing details in the bottom section of the console from the selected record in the Assigned Work table.
- Change Management
    - The BMC Remedy Change Management application provides a system of planning, scheduling, implementing, and tracking changes that need to be completed within your organization.
- Service Request Console (Under Construction)
    - Will be available for you to push out to your end users.
    - Purpose
        - Alleviate the amount of non-critical calls received to the service desk at your facility.

When an end-user creates a service request it will automatically create an incident which your department will receive.

Requesting Access

- During Go-Live, the local IS Director can submit a list of users to the facility's assigned Security resource that will need Help Desk access in Remedy. Help Desk access allows…
- After Go-Live, the local IS Director can request Help Desk access by entering a Remedy ticket through the Service Desk
- After Go-Live, all Remedy tickets regarding user access changes or new user access **must have an accompanying request form**.

Accessing Remedy

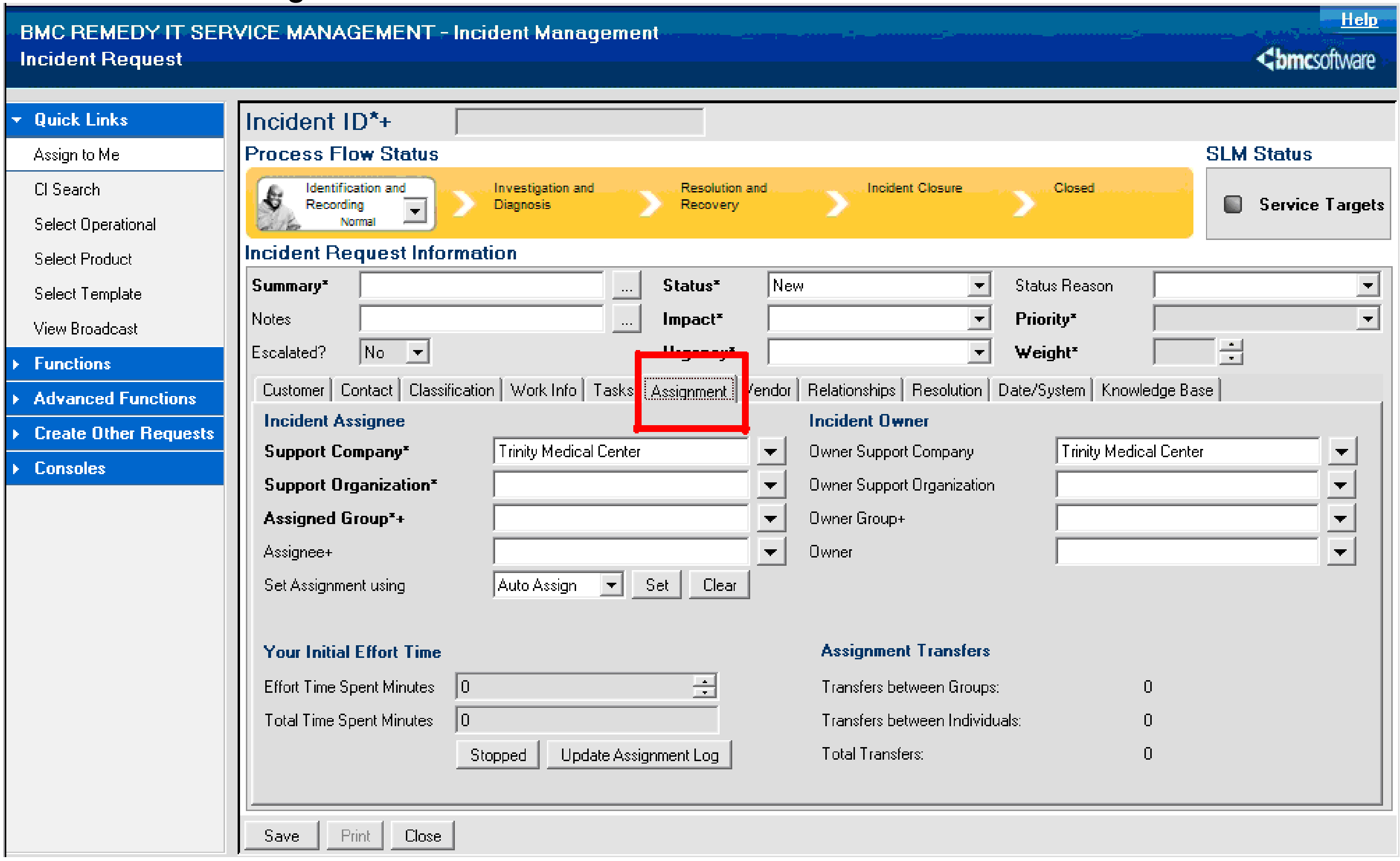
Remedy is recognized as being a service-desk application that is easily accessible by using the following URL: **Servicedesk.chs.net**

For information regarding training and/or access to the Remedy Application, please contact the service desk at (615)465-3100
Or you can open an incident ticket and assign it to the Service Desk at Corporate

Assigning a Remedy ticket to Corporate

To submit a ticket to corporate from facility, please follow these steps.

1. Have user fill out a ticket
2. Click on the **Assignment** tab



BMC REMEDY IT SERVICE MANAGEMENT - Incident Management
Incident Request

Incident ID*+

Process Flow Status: Identification and Recording (Normal) > Investigation and Diagnosis > Resolution and Recovery > Incident Closure > Closed

SLM Status: Service Targets

Incident Request Information

Summary*		Status*	New	Status Reason	
Notes		Impact*		Priority*	
Escalated?	No	Urgency*		Weight*	

Incident Assignee

Support Company*	Trinity Medical Center
Support Organization*	
Assigned Group*+	
Assignee+	
Set Assignment using	Auto Assign

Incident Owner

Owner Support Company	Trinity Medical Center
Owner Support Organization	
Owner Group+	
Owner	

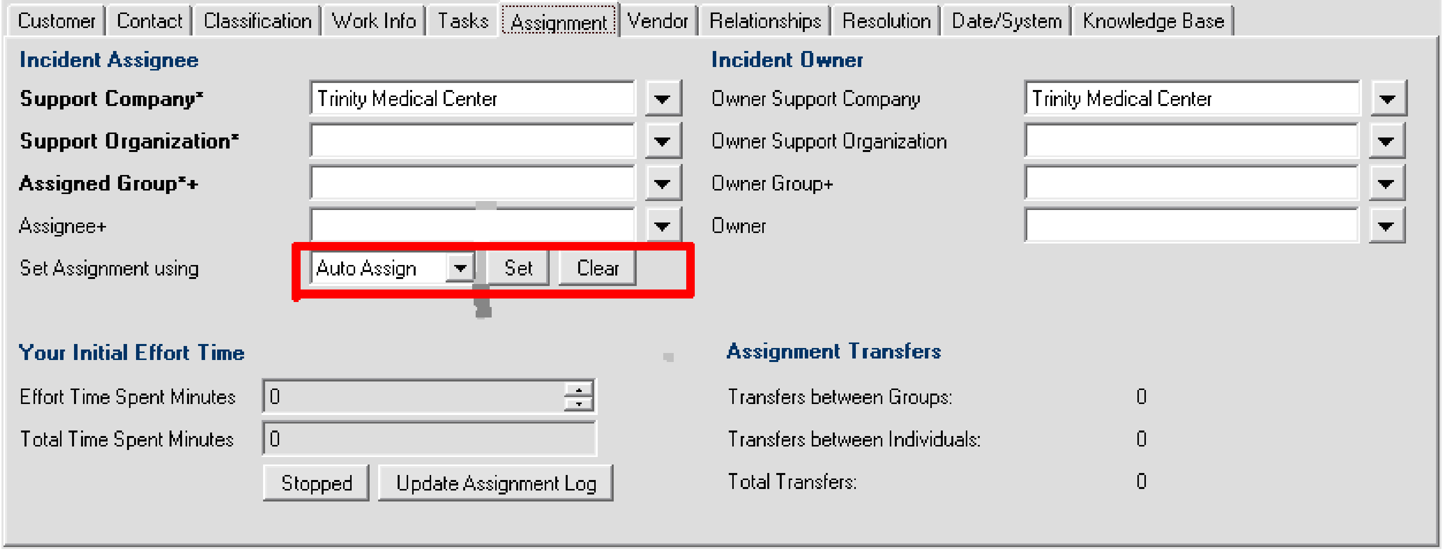
Your Initial Effort Time

Effort Time Spent Minutes	0
Total Time Spent Minutes	0

Assignment Transfers

Transfers between Groups:	0
Transfers between Individuals:	0
Total Transfers:	0

3. Click on the drop-down list highlighted below and select **Auto Assign**



Incident Assignee

Support Company*	Trinity Medical Center
Support Organization*	
Assigned Group*+	
Assignee+	
Set Assignment using	Auto Assign

Incident Owner

Owner Support Company	Trinity Medical Center
Owner Support Organization	
Owner Group+	
Owner	

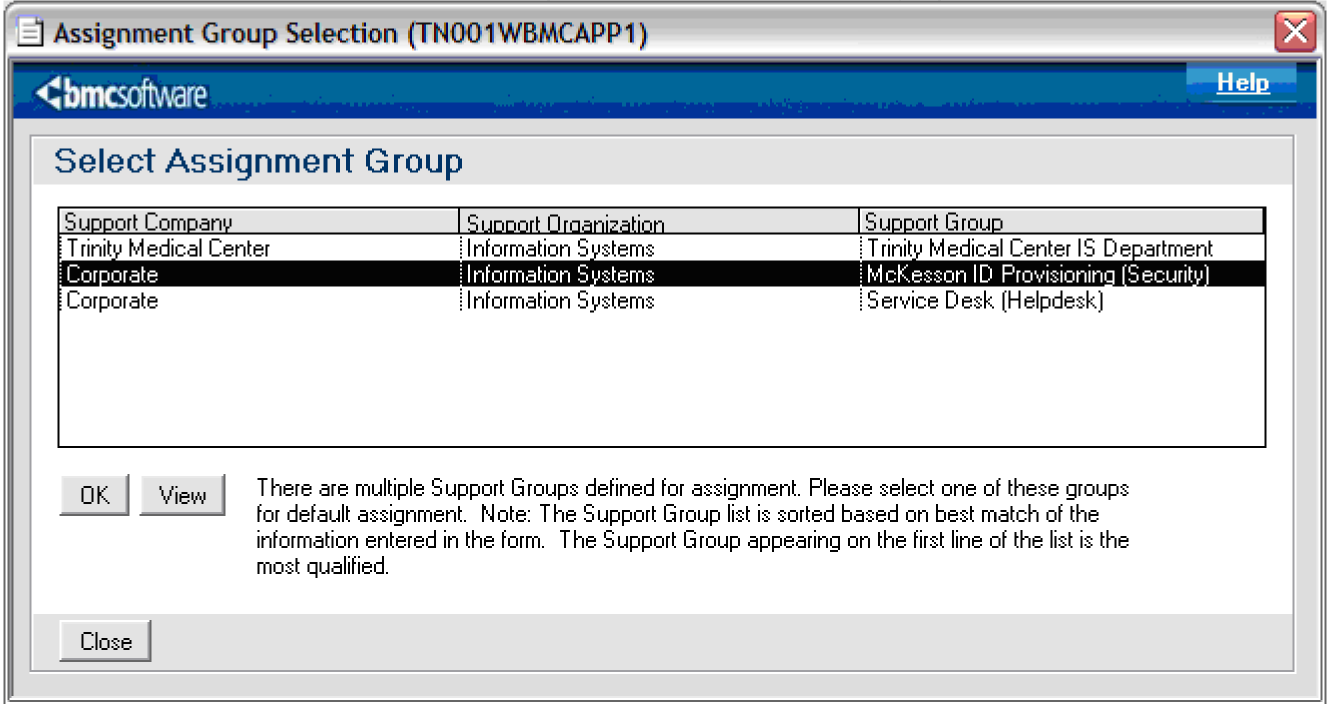
Your Initial Effort Time

Effort Time Spent Minutes	0
Total Time Spent Minutes	0

Assignment Transfers

Transfers between Groups:	0
Transfers between Individuals:	0
Total Transfers:	0

4. Click the **Set** button next to the drop-down list. This will bring up the box below



Select Assignment Group

Support Company	Support Organization	Support Group
Trinity Medical Center	Information Systems	Trinity Medical Center IS Department
Corporate	Information Systems	McKesson ID Provisioning (Security)
Corporate	Information Systems	Service Desk (Helpdesk)

There are multiple Support Groups defined for assignment. Please select one of these groups for default assignment. Note: The Support Group list is sorted based on best match of the information entered in the form. The Support Group appearing on the first line of the list is the most qualified.

5. At this point, the user can select one of the available corporate groups or their own local Help Desk

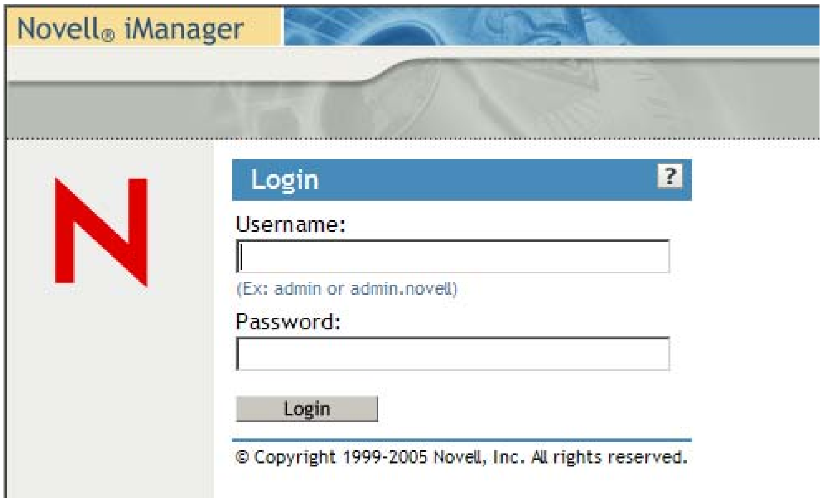
Only tickets for McKesson/HMS user provisioning may be assigned directly to Security System Administrators. McKesson user password resets can be handled by the Service Desk. Novell/HMS user password resets can be handled by Local IS through Novell.

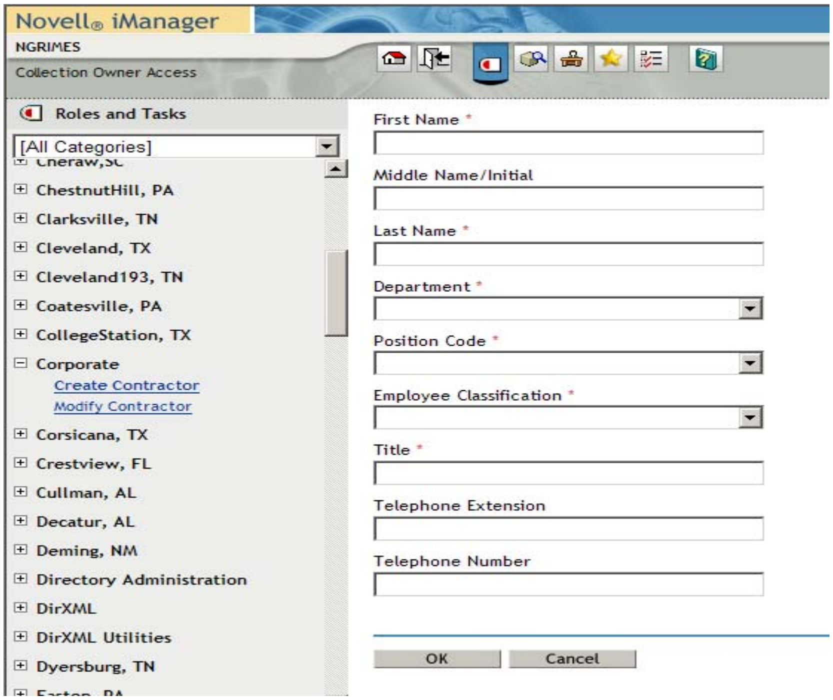
Contractors Database

The Contractors Database can be used by local IT to create IDs for physicians and contractors at your facility. The database can be accessed via the web at http://contractors.chs.net. Once logged in, you will be given the option to Create or Modify Contractors in your container. Enter information in each of the required fields and click OK to create the account.

If you do not have access to the Contractor's Database, please submit a Remedy ticket to Service Desk.

****ONLY USE FOR NON-EMPLOYEE USERS****


Novell® iManager
Login
Username:
(Ex: admin or admin.novell)
Password:
Login
© Copyright 1999-2005 Novell, Inc. All rights reserved.

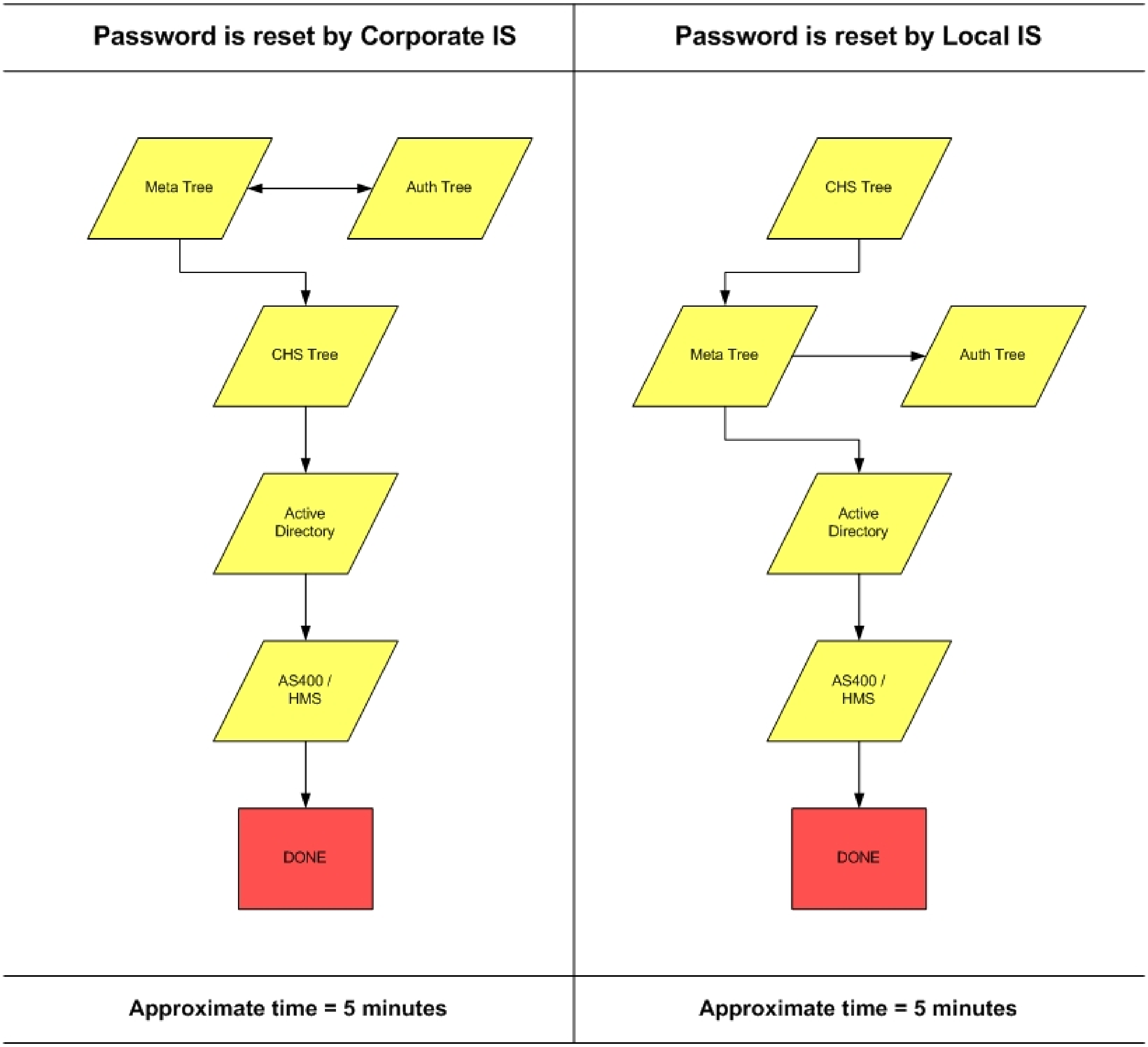


Password Self Service

CHS offers the ability for users to reset their passwords via the web at http://password.chs.net.

For new users, go to Initial Setup and Login

For existing users, go to Password Reset


Password is reset by Corporate IS
Meta Tree
Auth Tree
CHS Tree
Active Directory
AS400 / HMS
DONE
Approximate time = 5 minutes
Password is reset by Local IS
CHS Tree
Meta Tree
Auth Tree
Active Directory
AS400 / HMS
DONE
Approximate time = 5 minutes

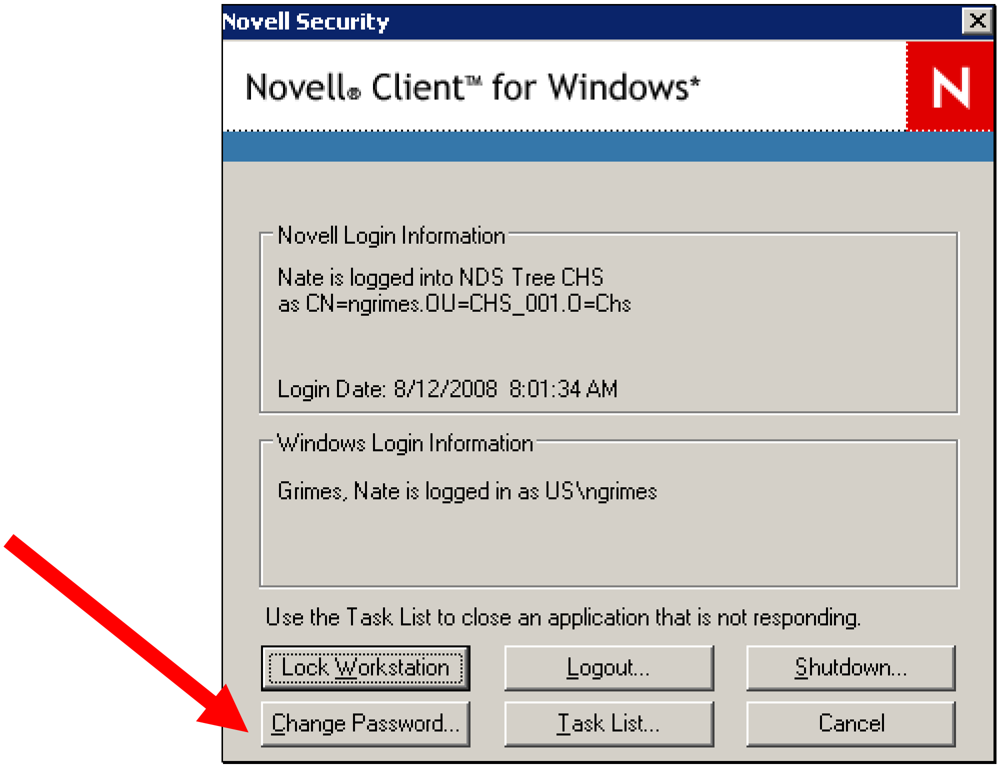
Local IT Level of Responsibility

Password Resets

Local IT will have access to reset Novell passwords, which will sync with AS400 and Active Directory accounts. The process may take up to 10 minutes to filter down to all systems. Once a user's password has been reset, the user must login to the AS400 with the new password before 11:59 PM of that day or the AS400 account will be disabled.

End users have the ability to change or reset their own passwords by using Password Self-Service at the website http://password.chs.net. **Users should be encouraged to login to Password Self-Service immediately upon their initial Novell login to establish their Challenge Responses. Users will not be able to use Password Self Service until they complete the Challenge Responses**.

Users may also change their passwords by selecting the Change Password option on the Novell Security window. Users may access the window by pressing Ctrl-Alt-Del.



Novell Login Information

Nate is logged into NDS Tree CHS
as CN=ngrimes.OU=CHS_001.O=Chs

Login Date: 8/12/2008 8:01:34 AM

Windows Login Information

Grimes, Nate is logged in as US\ngrimes

Use the Task List to close an application that is not responding.

Contractor account creation

Local IT can facilitate account creation for contractors by using the Contractors Database (http://contractors.chs.net). Please remember that the Contractors Database is only to be used for **non-employee users**. If the number of user accounts needed exceeds 25 users, Local IT may send a request to Corporate Security for bulk upload. Local IT will need to create a Remedy ticket to Service Desk and attach a spreadsheet listing the users needed. **During Go-Live, Local IT can submit the ticket directly to the Security System Administration group.**

The spreadsheet for contractor bulk upload should be in the following format:

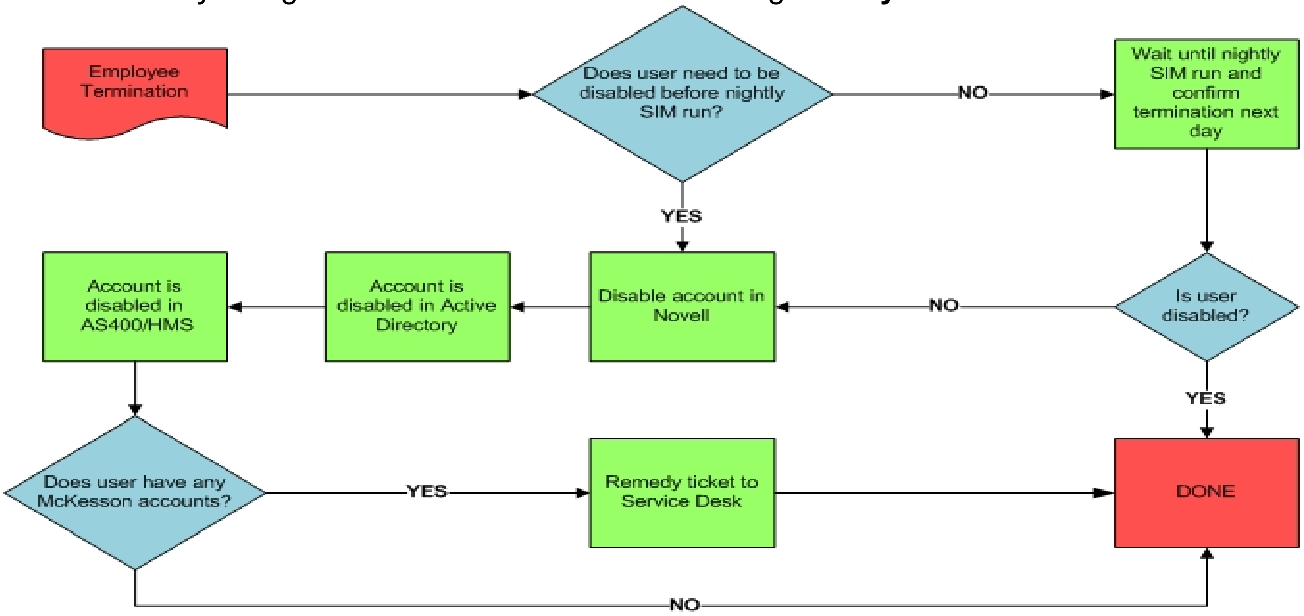
Last Name	First Name	Middle Name	Title	Phone Number	HMS Position #	HMS Dept #	Start Date	End Date

User Security Access Verification and Approval

Local IT will facilitate user access requests approval and Remedy ticket submissions to Service Desk with the completed access request forms attached (See Appendix: McKesson New User Access Form, HMS Role-Based Security Exception Form, Role-Based Security Exception Form). Local IT should verify that the requested access is appropriate for the user's job function and approved by their management. After Go-Live all additional access will require a McKesson New User Access form or McKesson Role-Based Security Exception Form. Please review process flow

Disabling accounts

Hospital user accounts will be disabled automatically by SIM when status is changed to **Terminated** in payroll. If an **Active** user account needs to be disabled, Local IT can disable the account in Novell which will also disable the appropriate Active Directory and AS400 account. If a McKesson account needs to be disabled, Local IT should submit a Remedy ticket to Service Desk. If a contractor account needs to be disabled, IT will also need to submit a Remedy ticket to Service Desk. Local IT can also disable accounts by using the Contractor's DB and choosing **Modify Contractor**.


Employee Termination
Does user need to be disabled before nightly SIM run?
NO
Wait until nightly SIM run and confirm termination next day
YES
Account is disabled in AS400/HMS
Account is disabled in Active Directory
Disable account in Novell
NO
Is user disabled?
YES
Does user have any McKesson accounts?
YES
Remedy ticket to Service Desk
DONE
NO

Corporate Security Level of Responsibility

Account Provisioning

1. If a new employee is entered into the payroll file and their **start date** is more than **<u>7 days</u>** in the future, SIM will **not** provision the account until 7 days before the **start date**
   (i.e. John Doe is entered into the payroll on 1/1, but his start date is 1/15. SIM will provision the account on 1/8)
2. If an existing employing is terminated in the payroll file, SIM will disable their accounts the day following their **termination date**
   (i.e. John Doe is terminated in the payroll file on 1/31. SIM will disable his accounts on 2/1)

Novell Provisioning

Corporate Security will be responsible for all user account provisioning. **Local IT should not create user accounts in Novell.** Upon completion of Go Live any new hospital users added to the payroll will be automatically created by SIM and granted access according to department and position combination. Corporate Security can create and assign new department/position combinations based on Remedy Request. SIM will create accounts in Novell, Active Directory/Citrix and AS400.

HMS/AS400 Provisioning

If a user needs access to HMS (AS400), Security will grant the access upon receiving a Service Desk ticket submitted by local IT. It will be the responsibility of local IT to determine the validity of the request from the user and include the necessary user information (i.e., User name, User ID, Position number, Department number, and Description of access needed) in the Remedy ticket. Position and department numbers can be verified by HR. Any Service Desk tickets for user access not submitted by IT will be rejected and the user will be advised to contact their IT staff.

McKesson/Citrix Provisioning

After the completion of Go Live, all McKesson access requests must be submitted by the user to local IT. The IT staff will approve the access by verifying that it is appropriate to job function and that it is approved by management. IT will attach a completed access request form to a Remedy ticket. Security will provision the McKesson access according to the approved request form. **No McKesson access can be given without a completed and approved access request form.** ***Please refer to the <u>CHS Hospital McKesson Access request Process Flow</u>***

The appropriate forms can be found on the CHS home page under the IT Service Desk tab. On the IT Service Desk page click the IT Security link on the right of the page under IT Links. On the right side of the IT Security page under the Security heading you will find links to the <u>CHS McKesson New User Access Form</u> and the <u>Role-Based Security Exceptions Form</u>.

The <u>CHS McKesson New User Access Form</u> is to be used for users with no prior McKesson access.

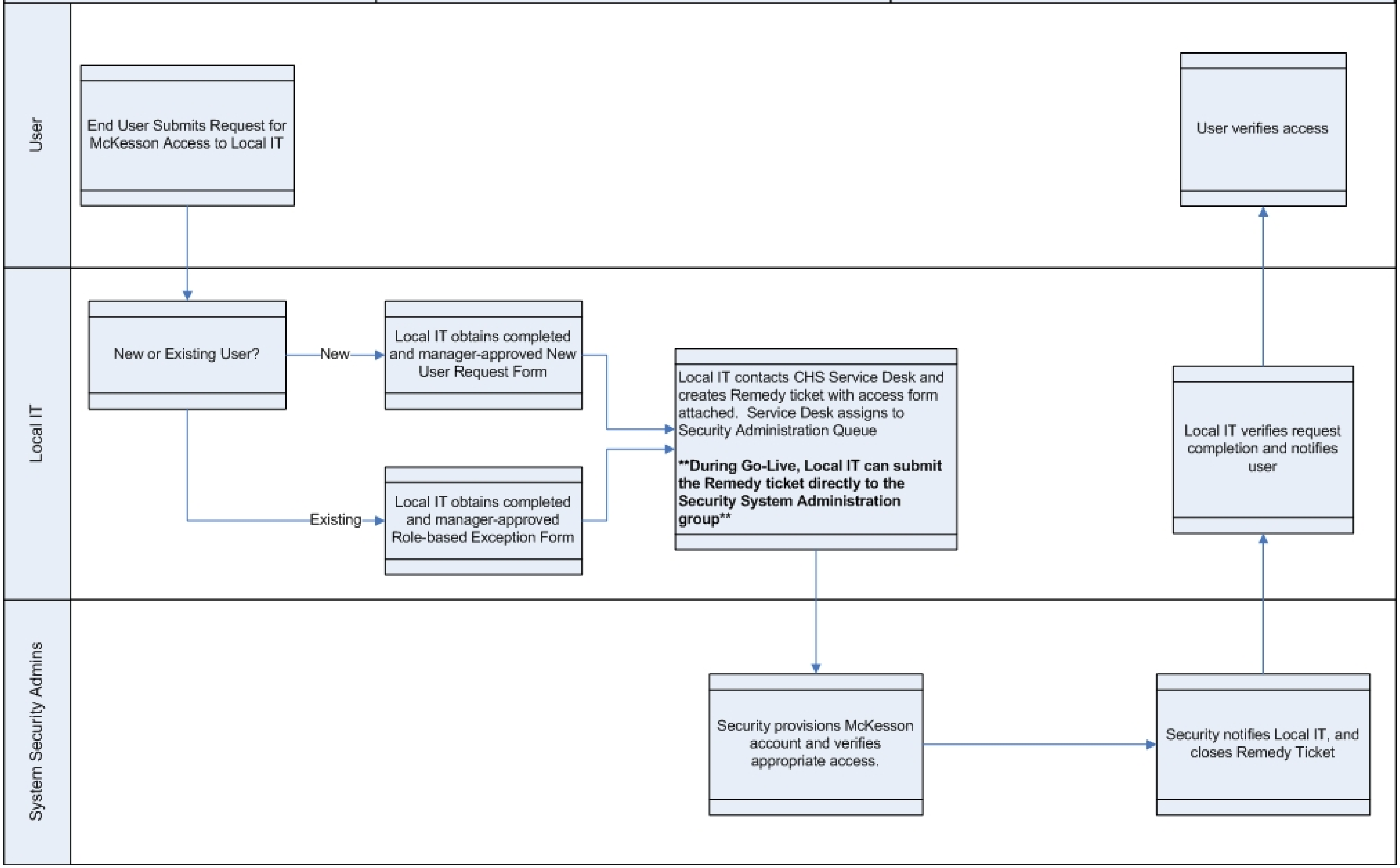
The <u>Role-Based Security Exceptions Form</u> should be used for existing McKesson users requesting access to additional McKesson applications.

CHS Community Health Systems

CHS Hospital McKesson Access Request Process Flow

Version 1.0

Updated: 8/11/08



User

End User Submits Request for McKesson Access to Local IT

User verifies access

Local IT

New or Existing User?

New

Local IT obtains completed and manager-approved New User Request Form

Existing

Local IT obtains completed and manager-approved Role-based Exception Form

Local IT contacts CHS Service Desk and creates Remedy ticket with access form attached. Service Desk assigns to Security Administration Queue

****During Go-Live, Local IT can submit the Remedy ticket directly to the Security System Administration group****

Local IT verifies request completion and notifies user

System Security Admins

Security provisions McKesson account and verifies appropriate access.

Security notifies Local IT, and closes Remedy Ticket

Service Desk Information

Local IT is the point of contact for end users. Excluding password resets, all requests for user access to the Service Desk should be filtered through local IT. Trouble tickets to the Service Desk that do not come from IT staff will be forwarded back to the local IT queue in Remedy creating a delay in resolution of the incident. Local IT will confirm that end users are requesting the correct access for their job function and that they have completed any necessary access request forms.

Hours of Operation: 24x7 including Holidays
Phone: 615-465-3100
Email: itservicedesk@chs.net

Clinical Desktop

Overview

The CHS Clinical Workstation/Desktop consists of standard deployment hardware running the minimal software set required for clinicians to perform tasks on the hospital floor. To deploy CHS Clinical Desktop, the following requirements are listed;

Windows XP – Standard CHS tier-(x) image

Secure Sign On (SSO / NSL)

Citrix Password Manager when applications are being published via Citrix

The tools deployed on the desktop to ease the burden of login / logoff and application launching are as follows;

Novell Secure Login

Provides single point login capabilities for;

a. Imed
b. EasyID
c. Notes
d. As400
e. Blueware
f. Citrix

Automatic Logoff

Tunable auto logoff time out to secure the desktop for HIPAA compliance. The application object, 'clinical workstation screen saver' controls the registry entries that control the notification timeout and the logoff timeout. This is the Microsoft Logoff Screen Saver available in the resource kit for most recent versions of Windows.

Hardened Workstation

Prevents access to questionable websites and Windows apps and utilities that the end user has no need to access or use. Also helps to prevent access to the machine by viri and browser hijacks. This package utilizes Windows Group Policies that are delivered by Zen for Desktops. The group policy controls access to the local drives, Windows Explorer, Internet Explorer control panel and approved websites. The installation documentation covers adding sites to the list.

Application Launcher Desktop Interface

Provides the end user with a single interface to launch applications, allowing the local IS department to limit the applications that are available. The Zen for Desktops application is used to replace

Windows Explorer further removing cumbersome interfaces and providing single point application launching and workstation logoff.

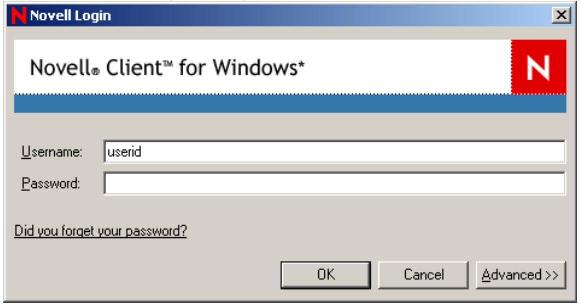
Installing Prerequisites for Clinical Desktop

Please refer to **future link**

User Login Experience

Novell – First time login

1. You will be prompted to enter your username and password (Figure 25)

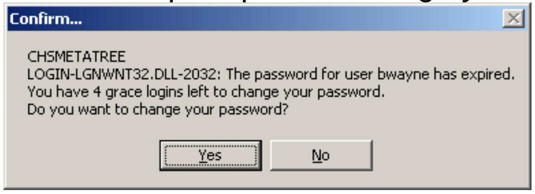


Username: userid

Password:

2. Enter your Novell userid and password

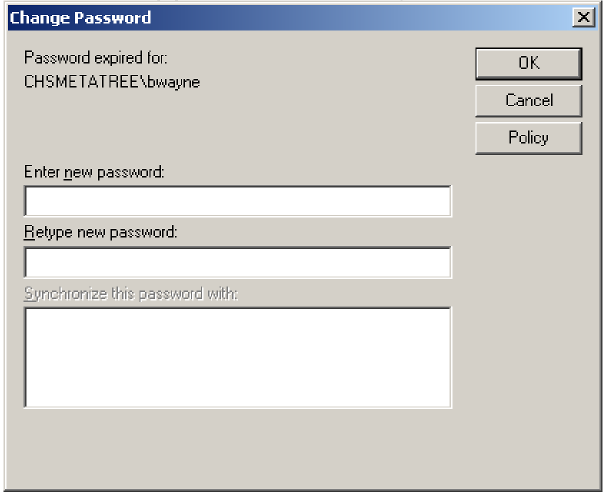
3. You will be prompted to change your password (Figure 26)



CHSMETATREE
LOGIN-LGNWNT32.DLL-2032: The password for user bwayne has expired.
You have 4 grace logins left to change your password.
Do you want to change your password?

4. Click Yes

5. New box appears and asks you to enter a new password (Figure 27)



Password expired for:
CHSMETATREE\bwayne

6. New passwords must follow the below rules
   a. Password must be unique within past 5 passwords used
   b. Minimum characters: 5
   c. Maximum characters: 10
   d. Numeric as first character: Not allowed
   e. Non-alphanumeric characters: Not allowed
   f. Longest repetition of a character: 3

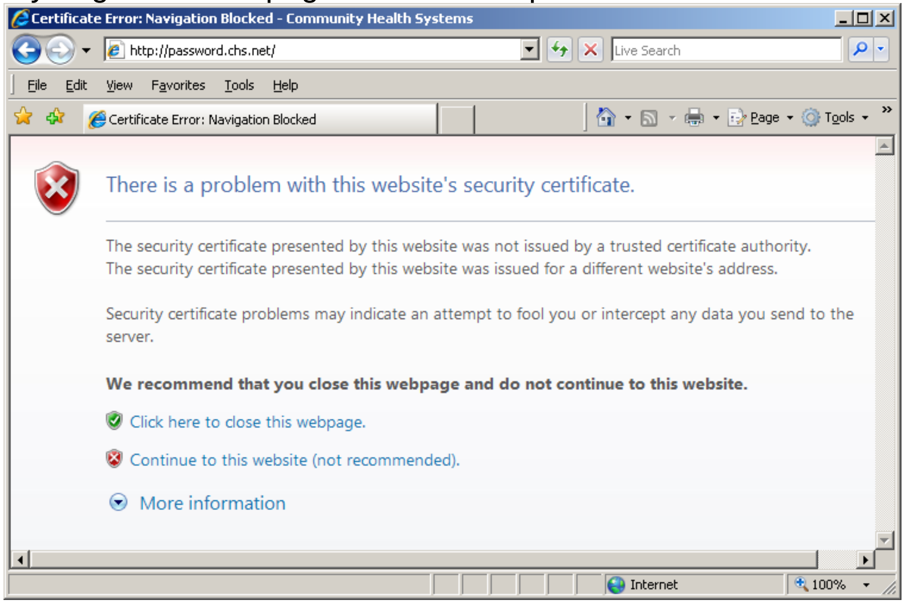
7. Click OK

Password Self Service

Initial Login and Setup

1. Go to the website: http://password.chs.net/

2. If you get an error page choose the option “Continue to this website (not recommended).”


Certificate Error: Navigation Blocked - Community Health Systems
http://password.chs.net/
Live Search
File
Edit
View
Favorites
Tools
Help
Certificate Error: Navigation Blocked
Page
Tools
Internet
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

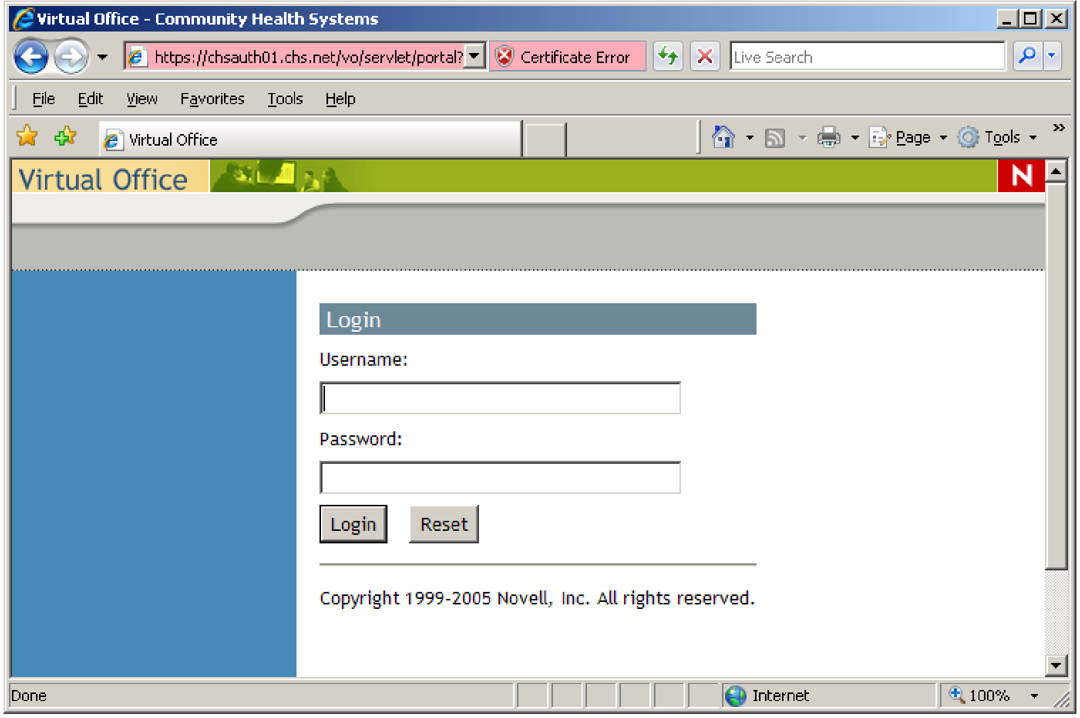
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

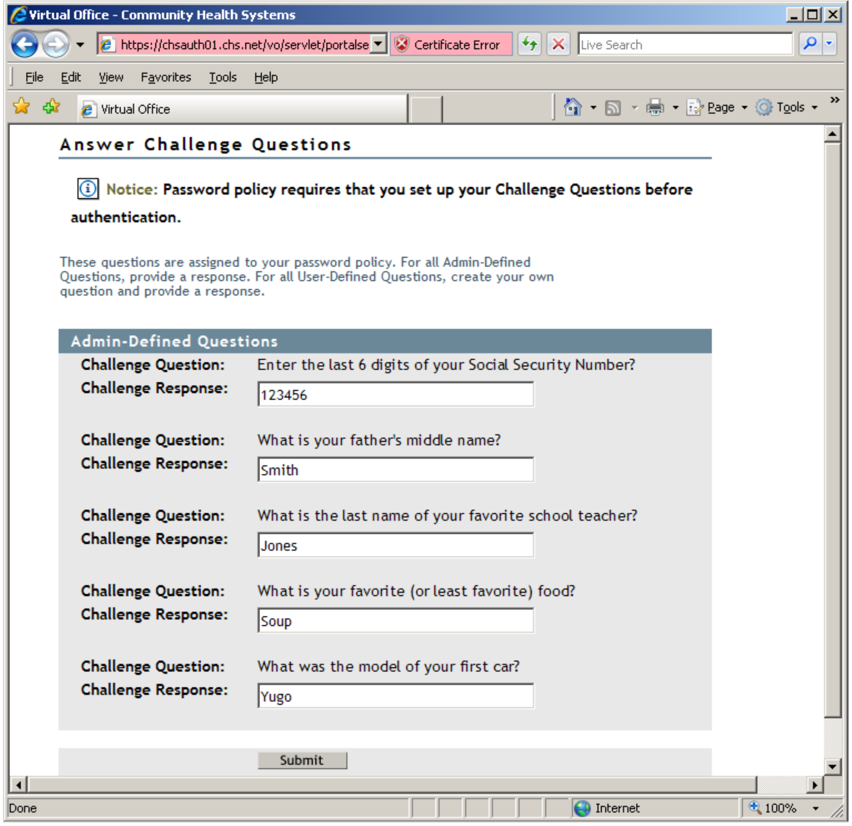
More information

3. Enter your Username and Password to login



Copyright 1999-2005 Novell, Inc. All rights reserved.

4. Answer the Challenge Questions and click the Submit button



Answer Challenge Questions

Notice: Password policy requires that you set up your Challenge Questions before authentication.

These questions are assigned to your password policy. For all Admin-Defined Questions, provide a response. For all User-Defined Questions, create your own question and provide a response.

Admin-Defined Questions

Challenge Question: Enter the last 6 digits of your Social Security Number?
Challenge Response: 123456

Challenge Question: What is your father's middle name?
Challenge Response: Smith

Challenge Question: What is the last name of your favorite school teacher?
Challenge Response: Jones

Challenge Question: What is your favorite (or least favorite) food?
Challenge Response: Soup

Challenge Question: What was the model of your first car?
Challenge Response: Yugo

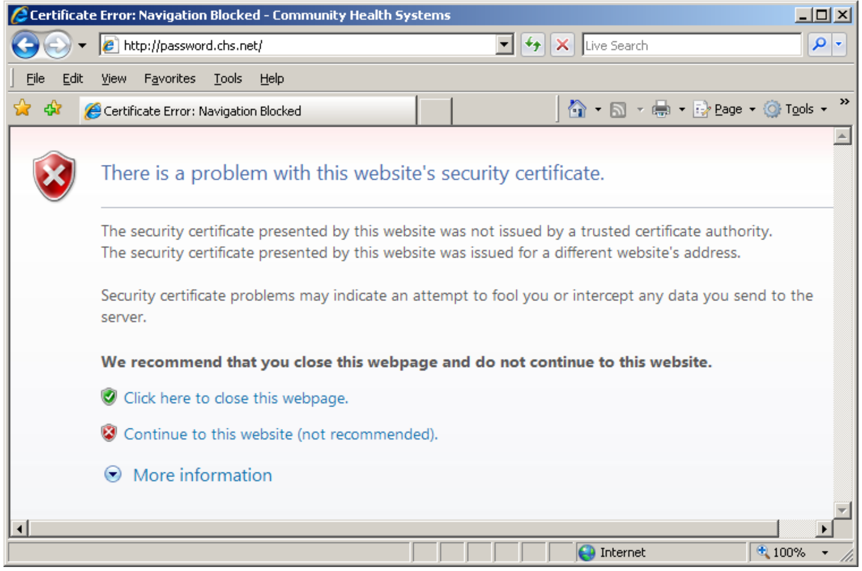
Submit

5. You can now change or reset your password with Password Self Service

Password Reset

1. Go to the website: http://password.chs.net/

2. If you get an error page choose the option “Continue to this website (not recommended).”



Certificate Error: Navigation Blocked - Community Health Systems
http://password.chs.net/
Live Search
File
Edit
View
Favorites
Tools
Help
Certificate Error: Navigation Blocked
Page
Tools
Internet
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

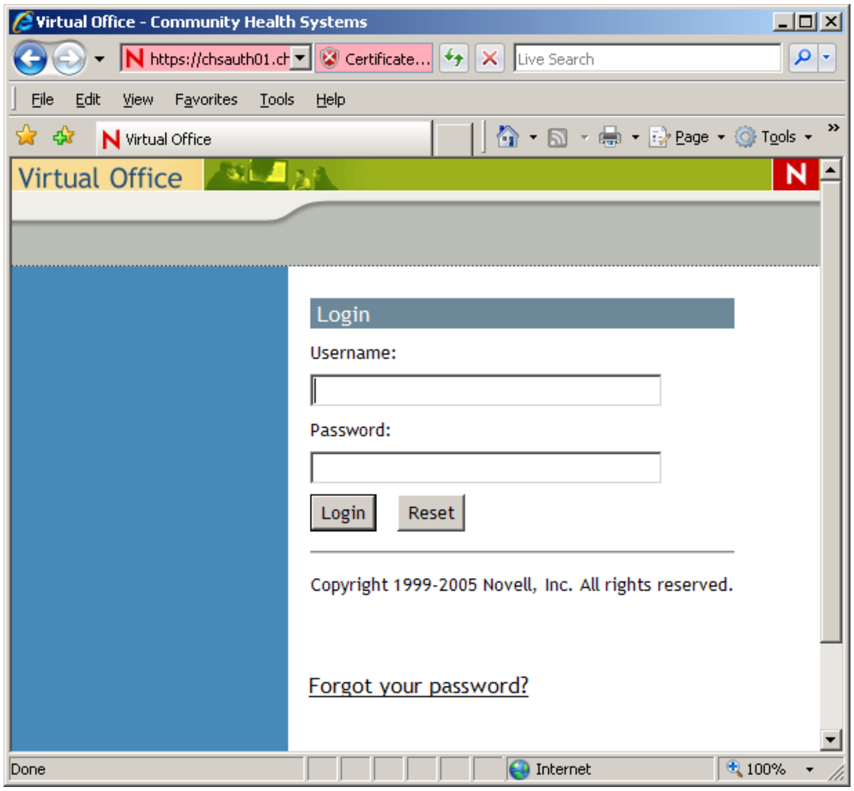
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

3. To change a known password enter your Username and Password and click the Login button. The Reset button clears all fields.



Login

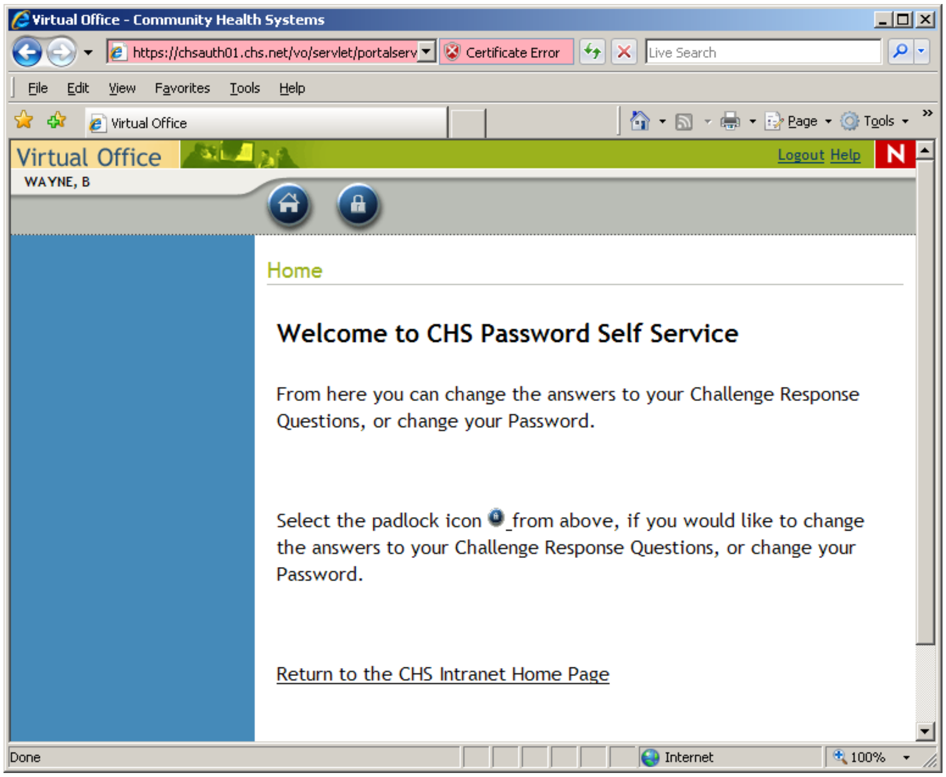
Username:

Password:

Copyright 1999-2005 Novell, Inc. All rights reserved.

Forgot your password?

4. Follow the instructions on the screen to change your password or your Challenge Response answers.


Virtual Office - Community Health Systems
https://chsauth01.chs.net/vo/servlet/portalserv
Certificate Error
Live Search
File Edit View Favorites Tools Help
Virtual Office
Page Tools
Virtual Office
Logout Help
WAYNE, B
Done
Internet
100%

Home

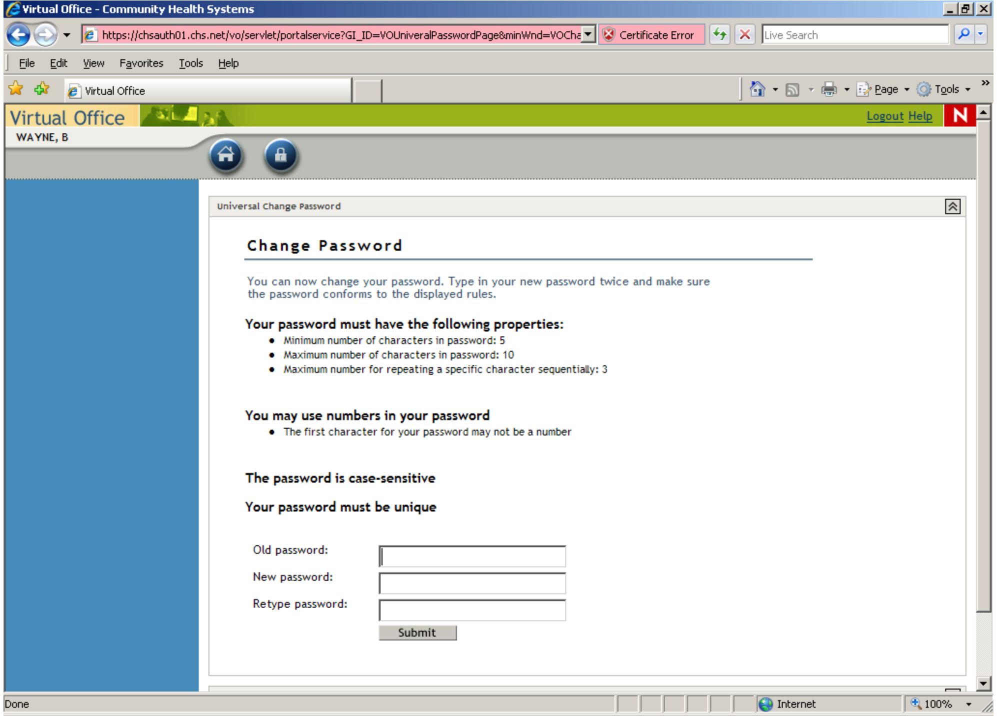
Welcome to CHS Password Self Service

From here you can change the answers to your Challenge Response Questions, or change your Password.

Select the padlock icon from above, if you would like to change the answers to your Challenge Response Questions, or change your Password.

Return to the CHS Intranet Home Page

5. If you don't know your password and you have previously answered the Challenge questions then click the "Forgot your password?" link.


Virtual Office - Community Health Systems
https://chsauth01.chs.net/vo/servlet/portalservice?GI_ID=VOUniveralPasswordPage&minWnd=VOCha
Certificate Error
Live Search
File Edit View Favorites Tools Help
Virtual Office
Page Tools
Virtual Office
Logout Help
WAYNE, B
Universal Change Password
Submit
Done
Internet
100%

Change Password

You can now change your password. Type in your new password twice and make sure the password conforms to the displayed rules.

Your password must have the following properties:

- Minimum number of characters in password: 5
- Maximum number of characters in password: 10
- Maximum number for repeating a specific character sequentially: 3

You may use numbers in your password

- The first character for your password may not be a number

The password is case-sensitive

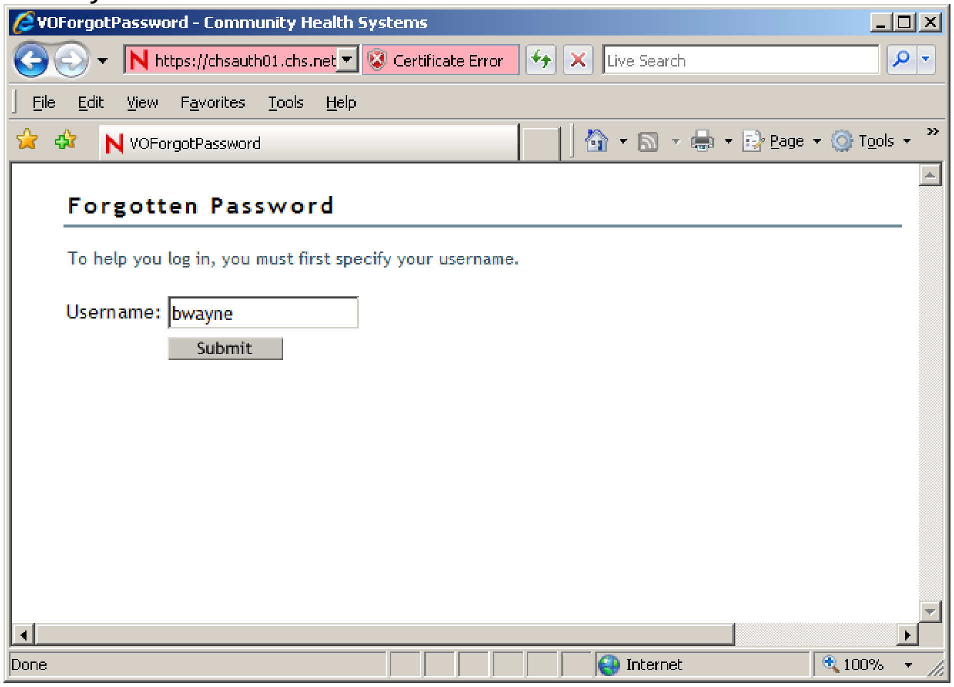
Your password must be unique

Old password:

New password:

Retype password:

6. Enter your Username and click Submit.

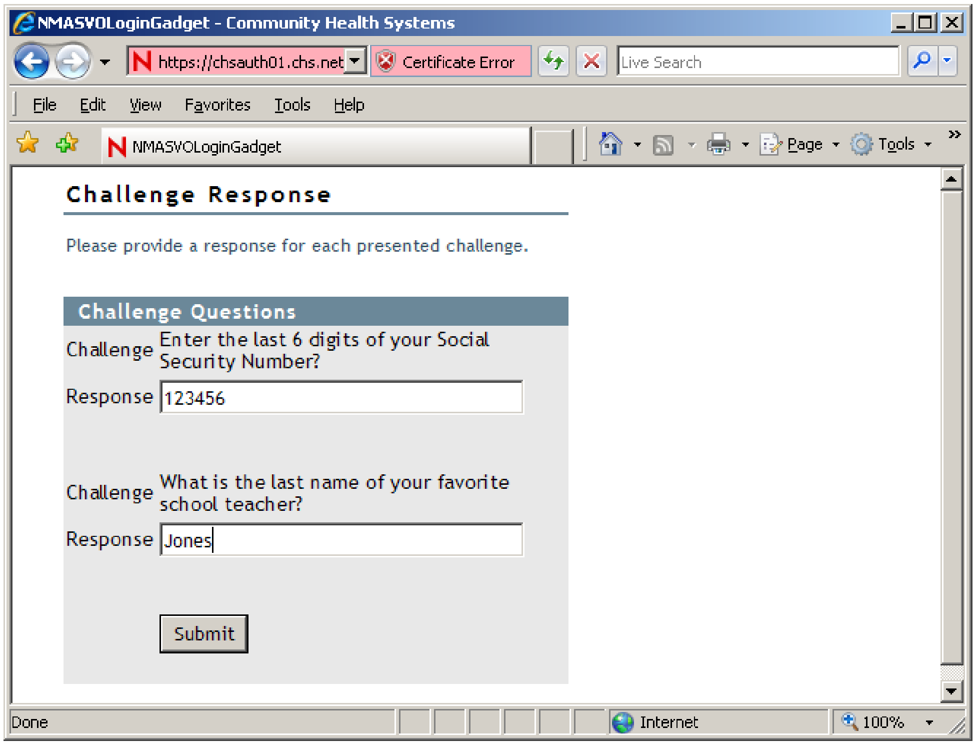

VOForgotPassword - Community Health Systems
https://chsauth01.chs.net
Certificate Error
Live Search
File Edit View Favorites Tools Help
VOForgotPassword
Page
Tools
Done
Internet
100%

Forgotten Password

To help you log in, you must first specify your username.

Username: bwayne

7. You will be prompted to answer two of your Challenge Response questions. Enter your answers and click the Submit button.


NMASVOLoginGadget - Community Health Systems
https://chsauth01.chs.net
Certificate Error
Live Search
File Edit View Favorites Tools Help
NMASVOLoginGadget
Page
Tools
Done
Internet
100%

Challenge Response

Please provide a response for each presented challenge.

Challenge Questions

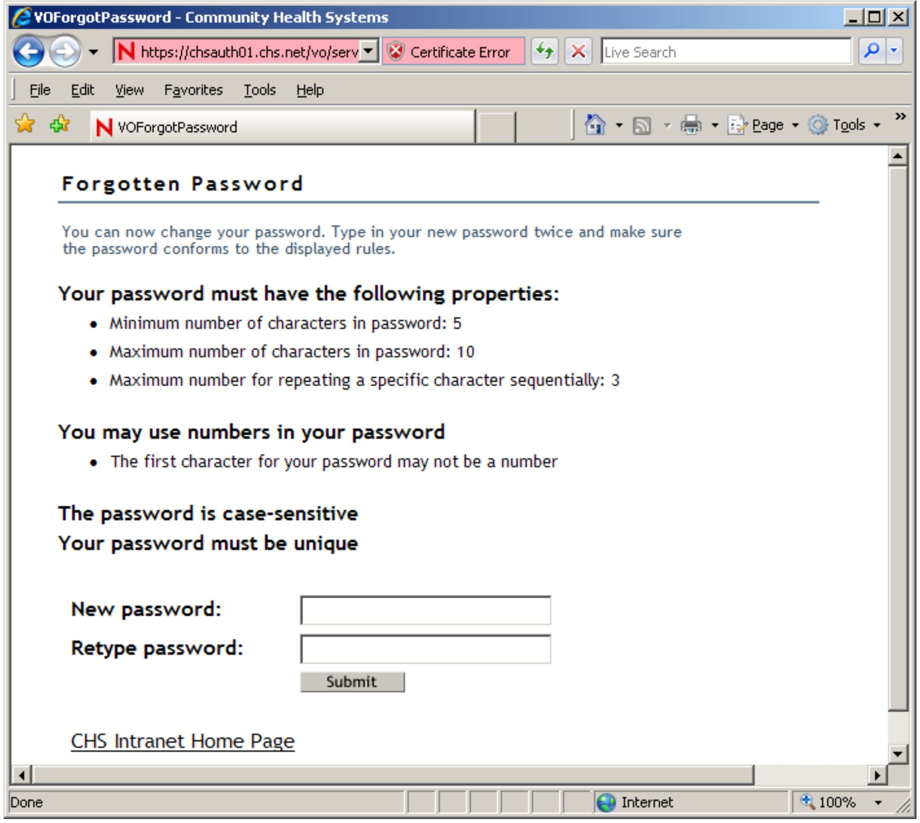
Challenge Enter the last 6 digits of your Social Security Number?

Response 123456

Challenge What is the last name of your favorite school teacher?

Response Jones

8. You can now select a new password. Follow the on screen directions to select a valid password and click the Submit button.



Forgotten Password

You can now change your password. Type in your new password twice and make sure the password conforms to the displayed rules.

Your password must have the following properties:

- Minimum number of characters in password: 5
- Maximum number of characters in password: 10
- Maximum number for repeating a specific character sequentially: 3

You may use numbers in your password

- The first character for your password may not be a number

The password is case-sensitive

Your password must be unique

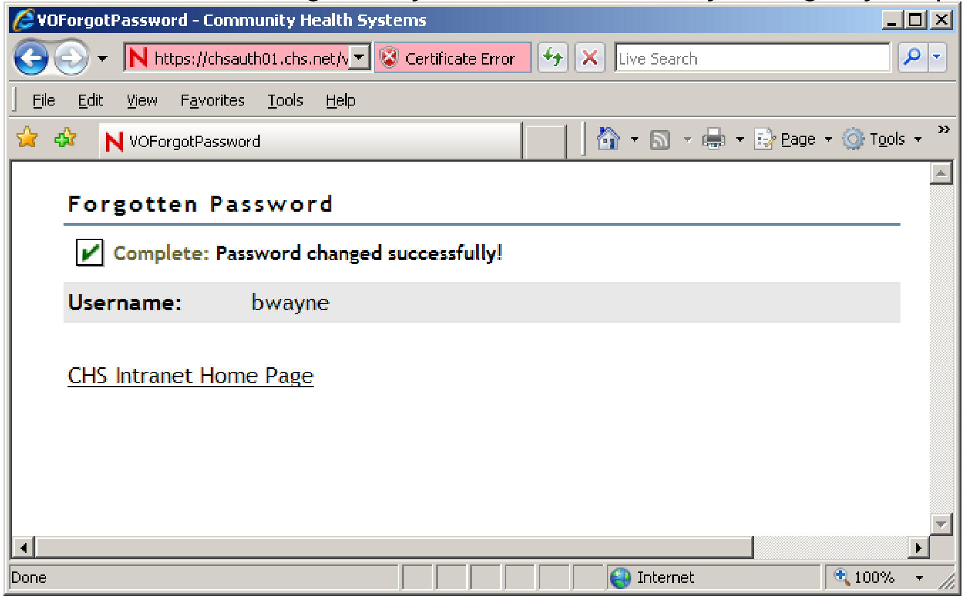
New password:

Retype password:

Submit

CHS Intranet Home Page

9. You will see a message that you have successfully changed your password.



Forgotten Password

☑ Complete: **Password changed successfully!**

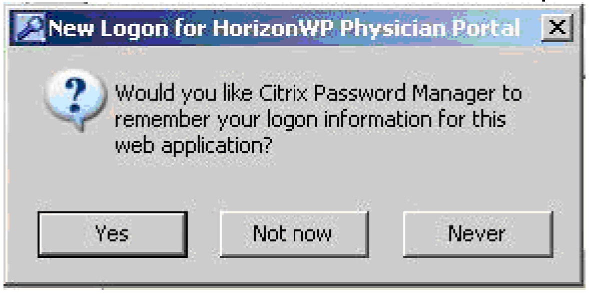
Username: bwayne

CHS Intranet Home Page

Citrix Password Manager

Setting Up Initial User Login Credentials

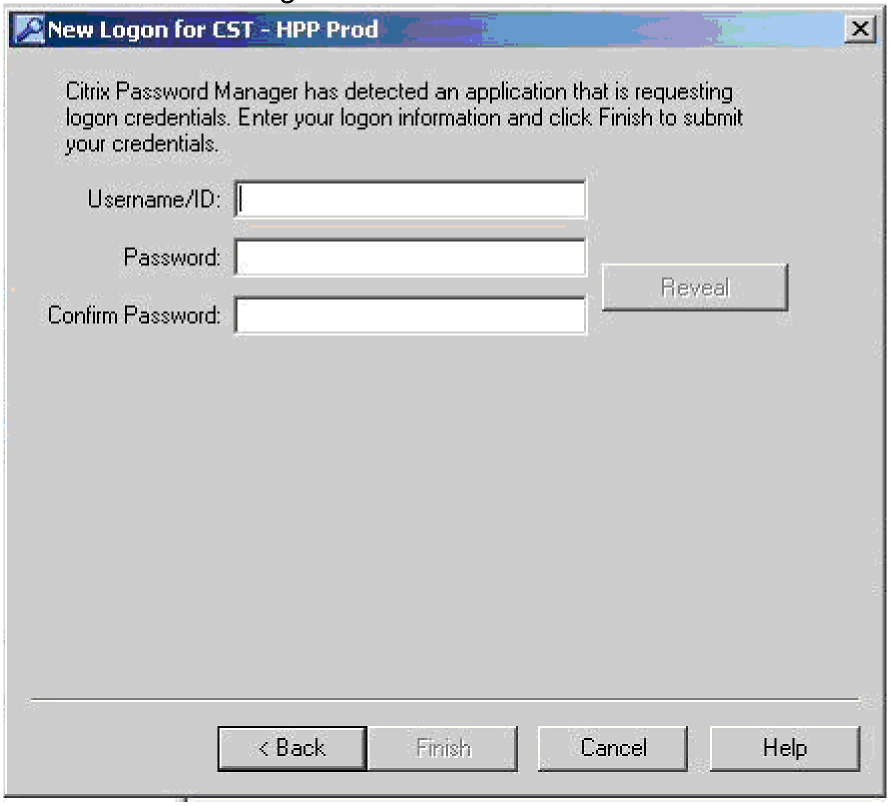
1. When the application is first launched, *Password Manager* will determine the application launched and compare that with the list of configured applications. If a match is found, *Password Manager* will then prompt the user whether or not to save the login credentials by selecting **YES**, **NOT NOW** or **NEVER**.
   a. **YES**: save credentials in the database.
   b. **NOT NOW**: Will not save during this instance, but will ask again at next login.
   c. **NEVER**: Will not save and will not prompt again.



New Logon for HorizonWP Physician Portal

Would you like Citrix Password Manager to remember your logon information for this web application?

2. If **YES** is selected, the user will be prompted to enter their username and password into *Password Manager*.



New Logon for CST - HPP Prod

Citrix Password Manager has detected an application that is requesting logon credentials. Enter your logon information and click Finish to submit your credentials.

Username/ID:

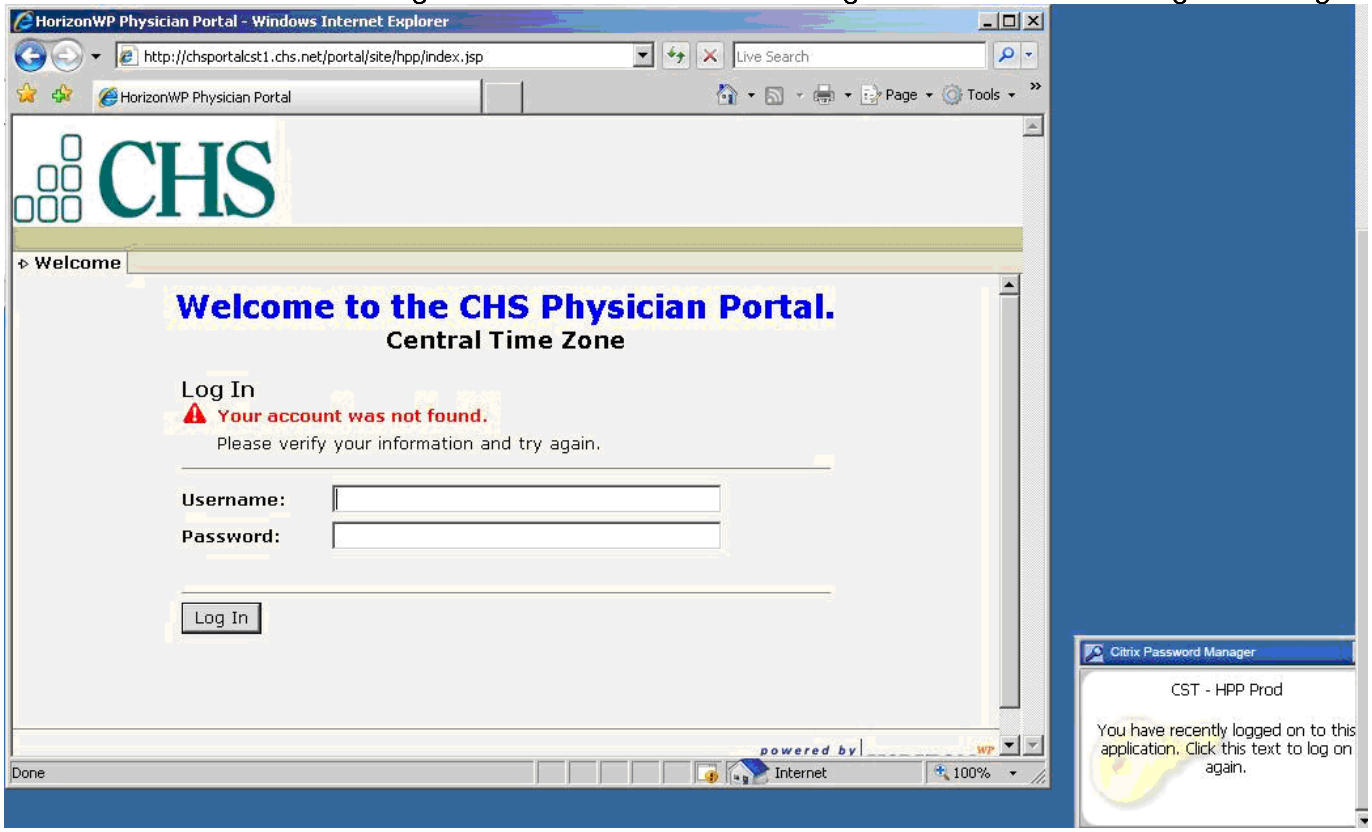
Password:

Confirm Password:

Password Expiration

If the password expires inside the application, then the password stored inside *Password Manager* and the password inside the application will become out of sync. When this happens, *Password Manager* will continue to pass the incorrect credentials until the stored password is changed. To accomplish this, follow these steps.

1. Click the *Password Manager* notification in the bottom right of the screen for Logon Manager.



HorizonWP Physician Portal - Windows Internet Explorer
http://chsportalcst1.chs.net/portal/site/hpp/index.jsp
Live Search
HorizonWP Physician Portal
Page
Tools
CHS
Welcome
Done
Internet
100%
Citrix Password Manager

Welcome to the CHS Physician Portal.
Central Time Zone

Log In
Your account was not found.
Please verify your information and try again.

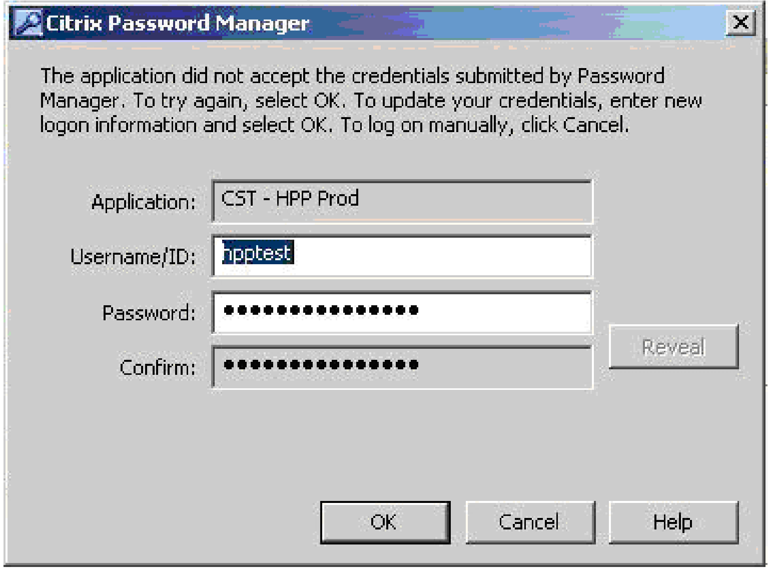
Username:
Password:

Log In

CST - HPP Prod

You have recently logged on to this application. Click this text to log on again.

2. The Citrix Password Manager Login window will appear. Enter your new password and confirm your new password. Select *"OK"* to save your new password.



The application did not accept the credentials submitted by Password Manager. To try again, select OK. To update your credentials, enter new logon information and select OK. To log on manually, click Cancel.

Application: CST - HPP Prod

Username/ID: hpptest

Password: ••••••••••••••••

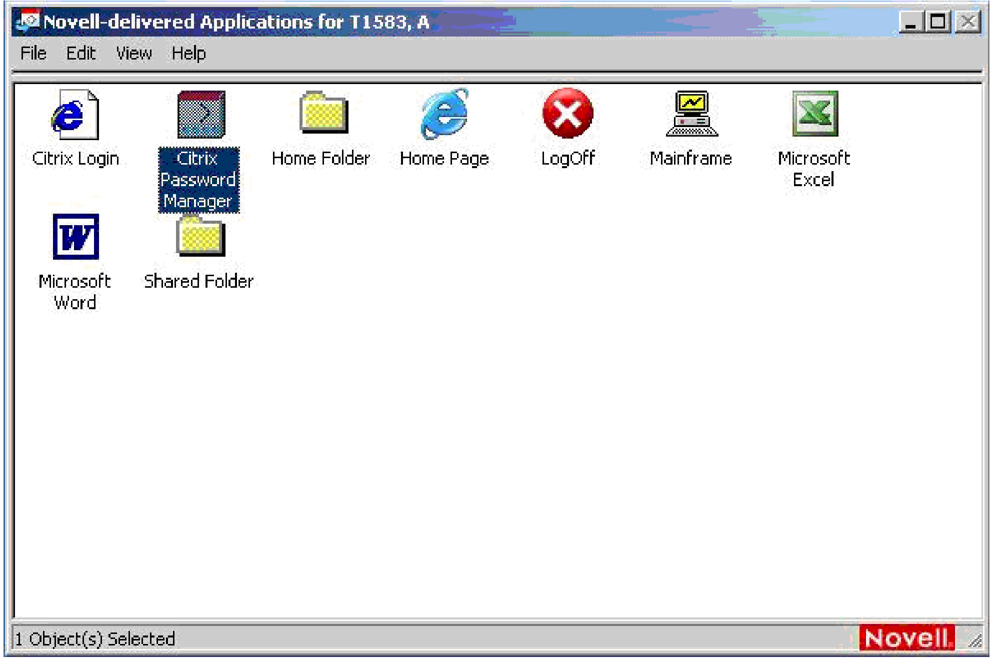
Confirm: ••••••••••••••••

3. When that is completed, the passwords will now be synchronized and *Password Manager* will start logging in with the newly set password.

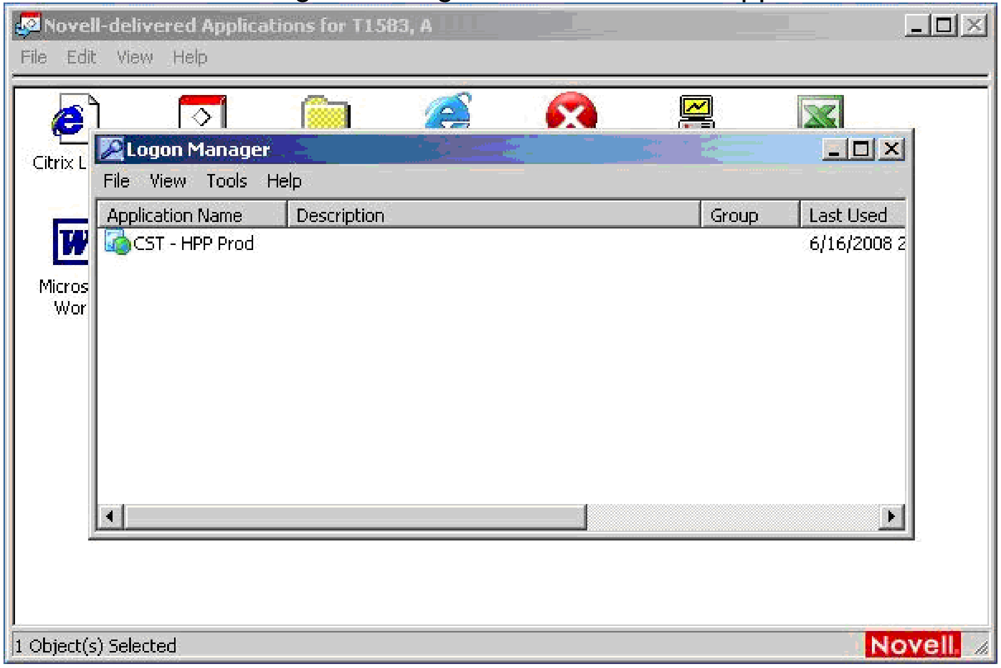
Manually Changing Password

If you decide to change your password within the McKesson application and Citrix Password Manager Change window is not launched, your password is out of sync with the Citrix Password Manager database. You can manually change your password in Citrix to sync your password with the McKesson application. To accomplish this, please follow these steps.

1. Click on the *"Citrix Password Manager"* Icon on the desktop.

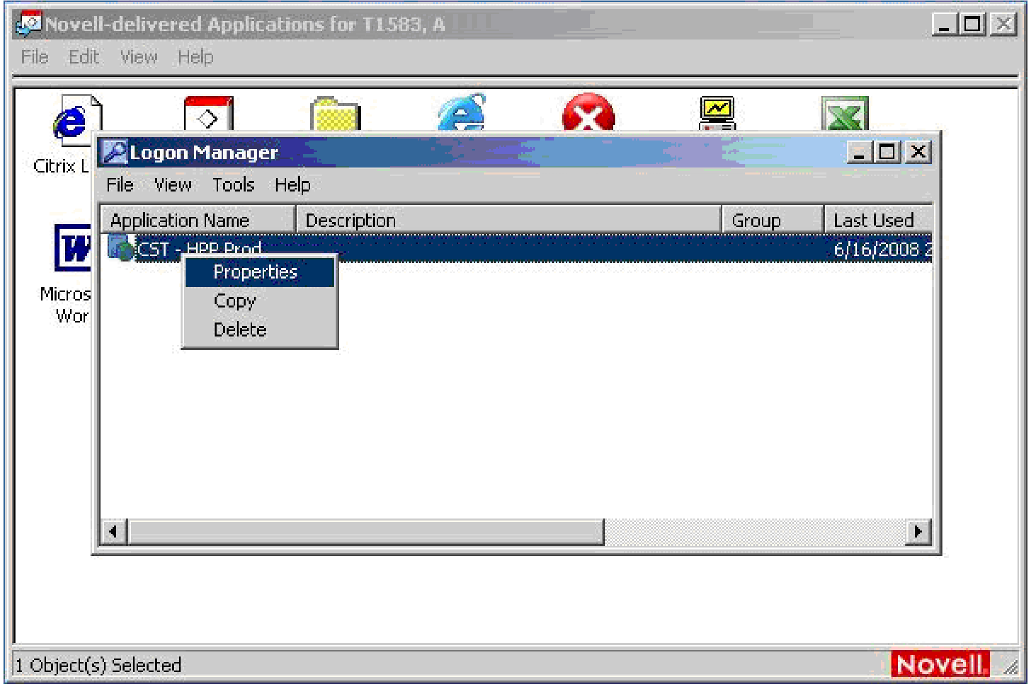


2. You will see a Logon Manager window that will appear.



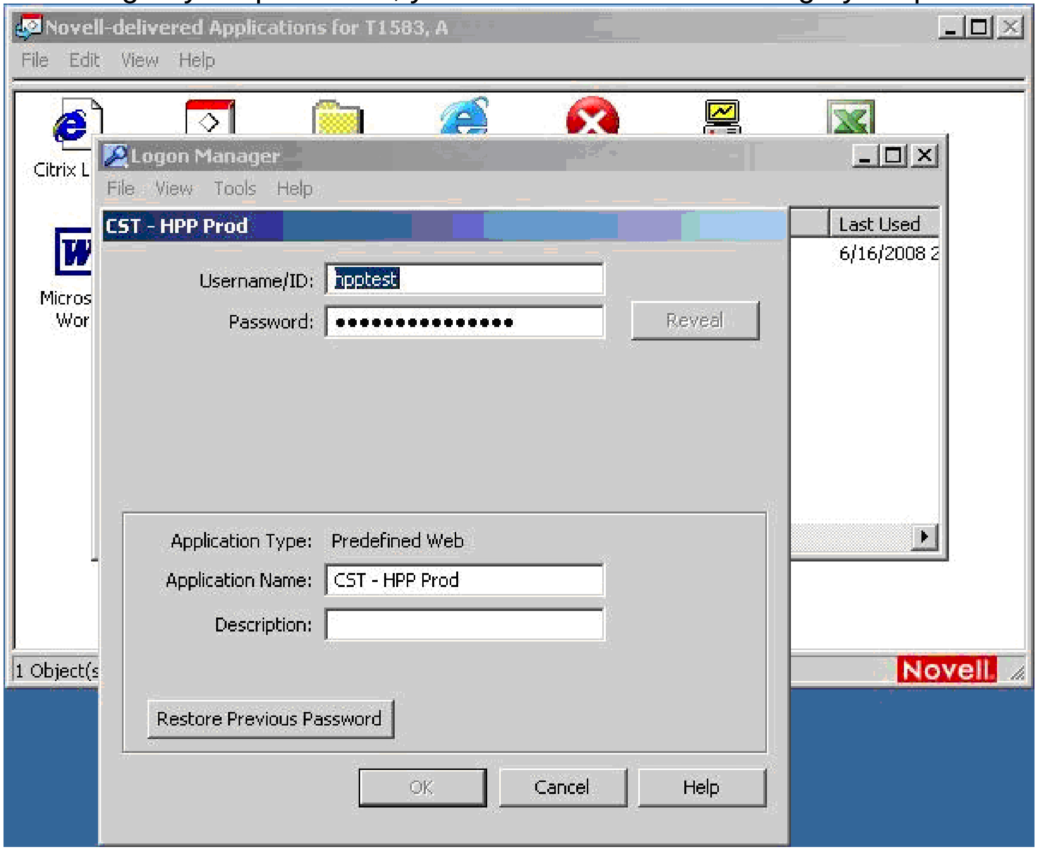
Application Name	Description	Group	Last Used
CST - HPP Prod			6/16/2008 2

3. Right-click on the Icon in the window. A dialogue box will appear and click on *"Properties"* to change your password.



Application Name	Description	Group	Last Used
CST - HPP Prod			6/16/2008 2

4. Enter your username and new password in the required fields. Please validate that the *"Application Name"* is the application that you are attempting to change. Once you have changed your password, you will select *"OK"* to change your password.



Username/ID: hpptest

Password: ●●●●●●●●●●●●●●●●

Application Type: Predefined Web

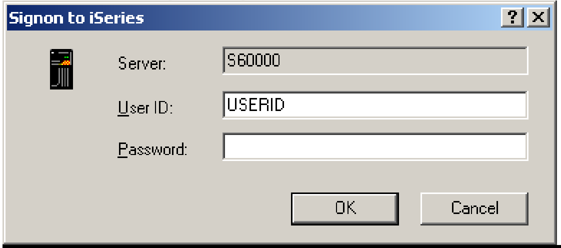
Application Name: CST - HPP Prod

Description:

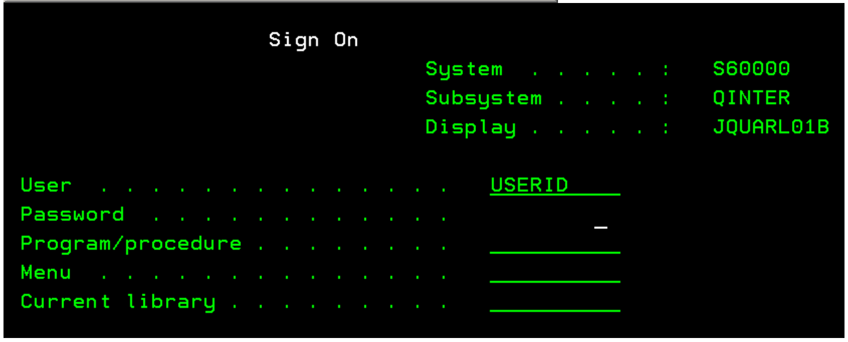
AS400/HMS

1. Open AS400/HMS

2. You will be prompted to enter username and password (Figure 1)



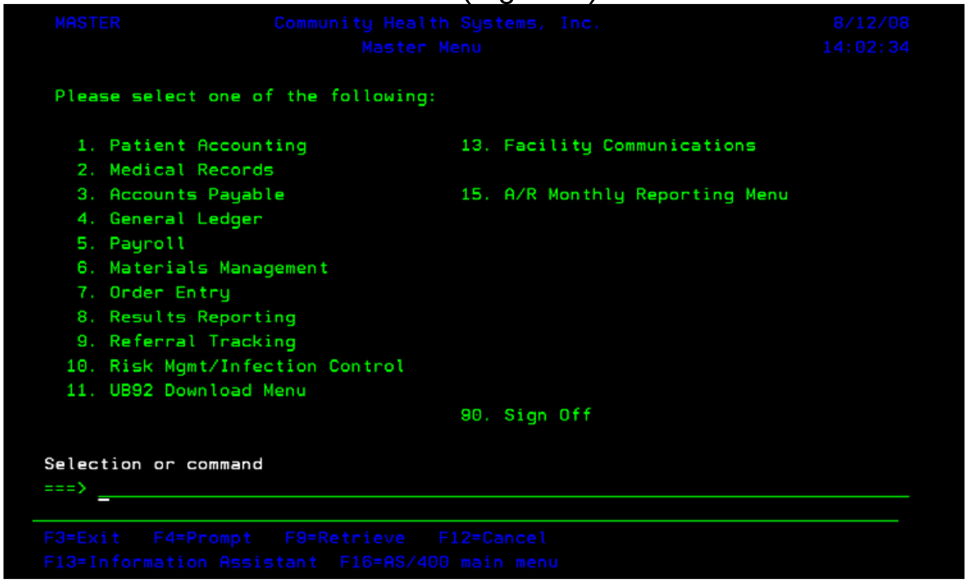
```
Server:     S60000
User ID:    USERID
Password:
```



```
                      Sign On
                                System  . . . . . :   S60000
                                Subsystem . . . . :   QINTER
                                Display . . . . . :   JQUARL01B

User  . . . . . . . . . . . . . .     USERID
Password  . . . . . . . . . . . .
Program/procedure . . . . . . . .
Menu  . . . . . . . . . . . . . .
Current library . . . . . . . . .
```

3. Enter AS400/HMS userid and password

4. You will be taken to initial menu (Figure 2)



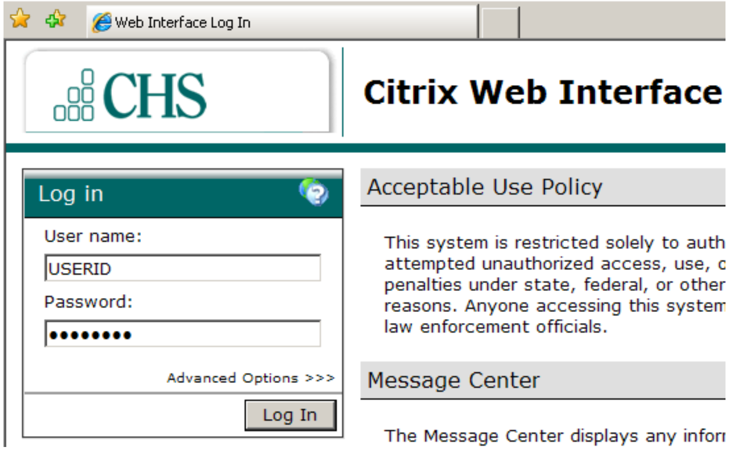
```
 MASTER              Community Health Systems, Inc.                  8/12/08
                                  Master Menu                           14:02:34

 Please select one of the following:

    1. Patient Accounting                  13. Facility Communications
    2. Medical Records
    3. Accounts Payable                    15. A/R Monthly Reporting Menu
    4. General Ledger
    5. Payroll
    6. Materials Management
    7. Order Entry
    8. Results Reporting
    9. Referral Tracking
   10. Risk Mgmt/Infection Control
   11. UB92 Download Menu
                                           90. Sign Off

Selection or command
===> _

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant   F16=AS/400 main menu
```

Citrix/McKesson

1. Open Internet Explorer

2. In the address bar enter http://mck.chs.net

3. You will be prompted to enter username and password (Figure 3)



Web Interface Log In

CHS

Citrix Web Interface

Log in

User name:

USERID

Password:

••••••••

Advanced Options >>>

Log In

Acceptable Use Policy

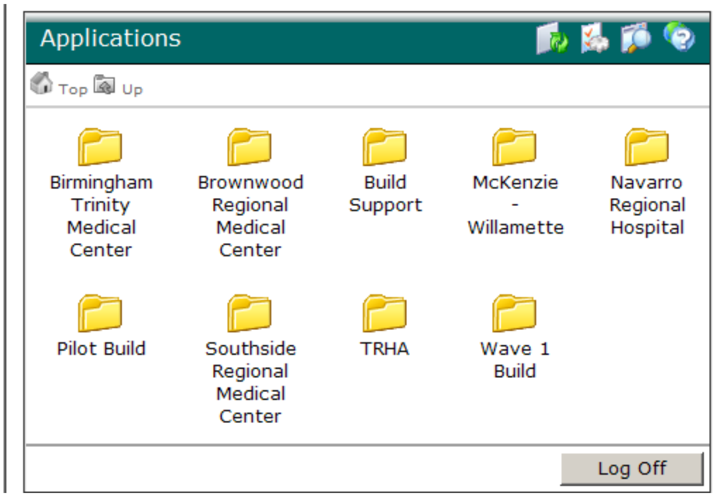
This system is restricted solely to auth
attempted unauthorized access, use, c
penalties under state, federal, or other
reasons. Anyone accessing this system
law enforcement officials.

Message Center

The Message Center displays any infor

4. Enter Novell userid and password

5. You will be taken to the next screen that shows your hospital name or 4 letter designation (Figure 4)



Applications

Top Up

Birmingham Trinity Medical Center

Brownwood Regional Medical Center

Build Support

McKenzie - Willamette

Navarro Regional Hospital

Pilot Build

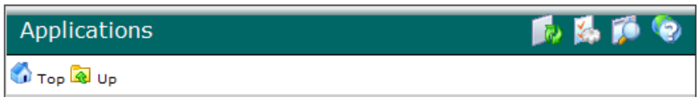
Southside Regional Medical Center

TRHA

Wave 1 Build

Log Off

6. If you have access to multiple hospitals, click on the Top button to be taken to the screen that shows all the folders. The Top button is located below the word "Applications" (Figure 5)

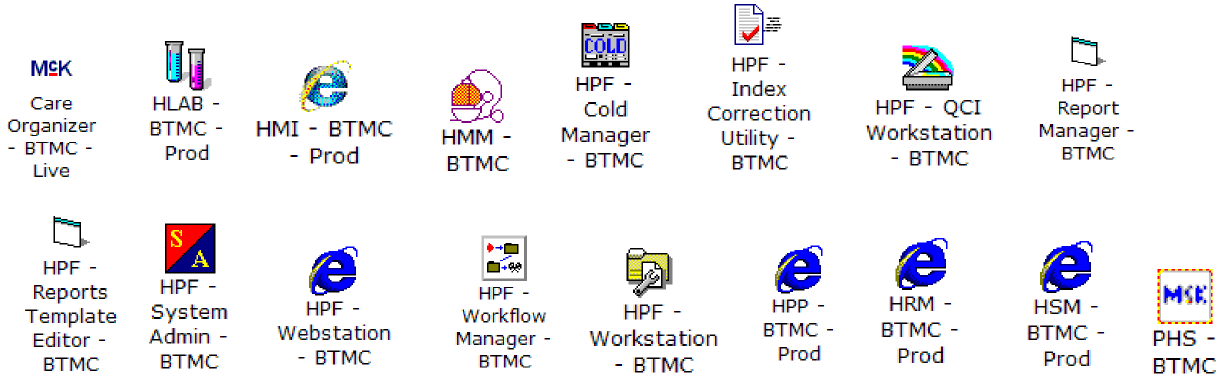


Applications

Top Up

7. Click on your folder and you will be taken to the next screen with the McKesson icons

8. Depending on the access given to your account, you will see 1 or more of the following icons for McKesson applications (Figures 6 - 23)


Care Organizer - BTMC - Live
HLAB - BTMC - Prod
HMI - BTMC - Prod
HMM - BTMC
HPF - Cold Manager - BTMC
HPF - Index Correction Utility - BTMC
HPF - QCI Workstation - BTMC
HPF - Report Manager - BTMC
HPF - Reports Template Editor - BTMC
HPF - System Admin - BTMC
HPF - Webstation - BTMC
HPF - Workflow Manager - BTMC
HPF - Workstation - BTMC
HPP - BTMC - Prod
HRM - BTMC - Prod
HSM - BTMC - Prod
PHS - BTMC

9. To logoff, click the **Log Off** button towards the bottom (Figure 24)