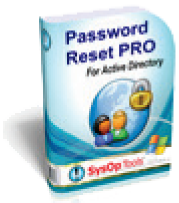
Password Reset PRO Version 3 Operational Summary and Screenshots



This guide covers screenshots relating to iPhone / mobile device self service access, Profile Enrollment Mode access and Active Directory Data Mode access.

Applies to software version 3.x.x

Below are screenshots and overview of the Password Reset PRO v3 self service portal web pages. You can completely brand all of the pages with your logo, you can change the text and wording on the pages, and you can change the images for enrollment. You can make the product look like something you built vs bought, while maintaining a highly secure and highly usable self service system.

- The "**PART1**" example outlines the "**Profile Enrollment**" access mode (user pre-enrollment required)
- The "**PART 2**" example outlines the "**Active Directory Data**" access mode (no user pre-enrollment required)
- The "**PART 3**" example outlines the "**Domain Basic Authentication**" access mode (fast, basic access mode)
- The "**PART 4**" example shows screenshots of mobile device access from iPhone. Screens are similar on Android, WM, BB. No app installations are required.

- Benefit - Deploy our software in either access mode
- Benefit - Deploy several self service web portals running in different access modes at the same time
- Benefit - The public facing web portal does not run with any domain credentials or contain any mechanisms that would pose a perimeter security risk
- Benefit - No separate databases required, highly redundant and fault tolerant architecture, fast to deploy
- Benefit – Run multiple installations within same domain, no added cost for multiple installs
- Benefit – Licensing is only required for your enabled, password expiring user account objects

Screenshots begin on next page..

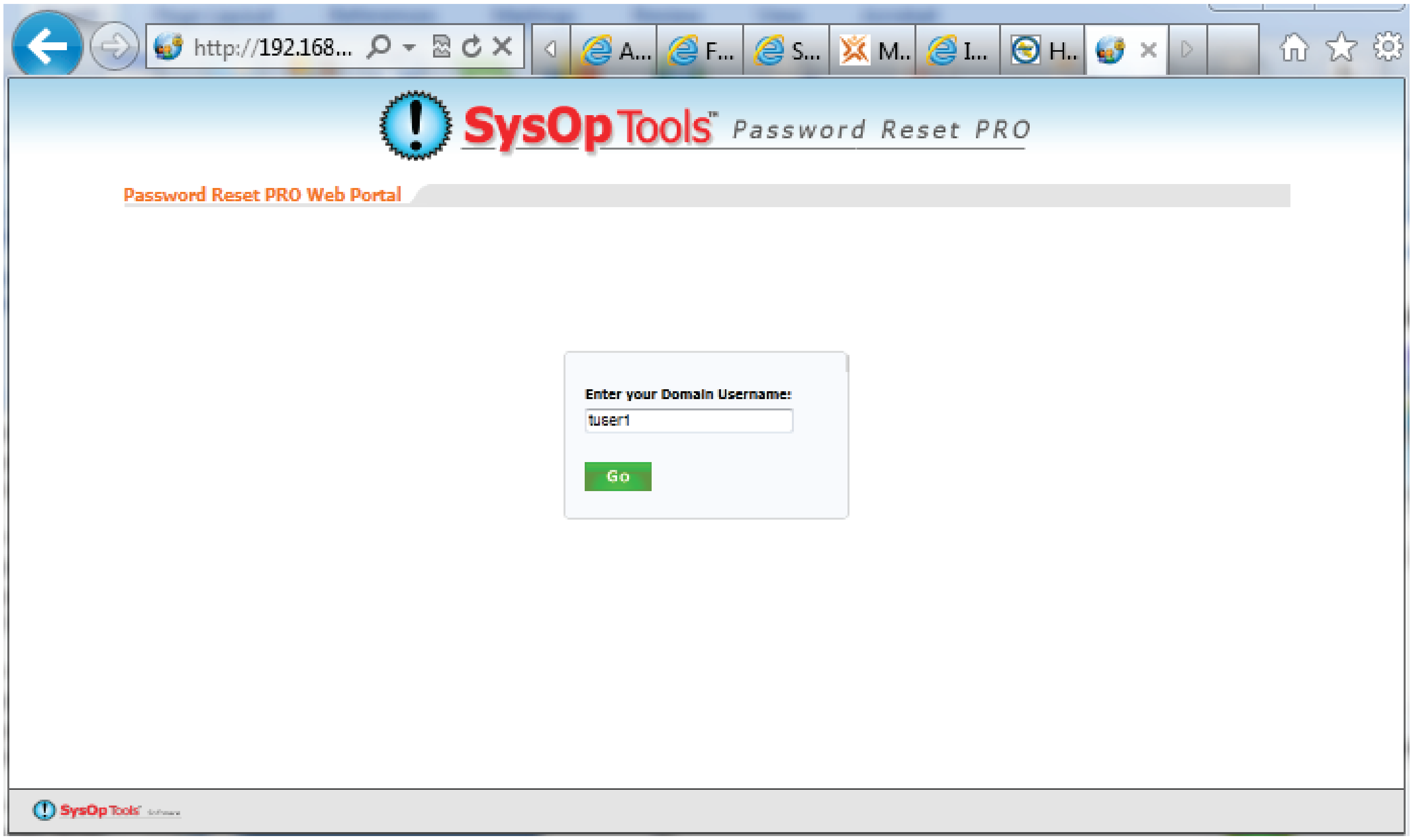
PART 1 – PROFILE ENROLLENT MODE WEB PORTAL. PRE-ENROLLMENT REQUIRED – New User can Enroll in all Situations Except for a Locked Account or Forgotten Password. User Must Enroll to Self Service Locked Account or Forgotten Password. Easy Administrative Setup / Deployment.

The main self service landing page is shown below and is easily branded to suit your environment. We allow full editing of the actual CSS and .aspx web pages, as well as images, link buttons, global banner, footer, etc.

User simply types in their domain username or domain email address to begin enrollment. The enrollment is a simple two step process, the method is highly memorable, and can be re-worded to better suit your user community.

Only your enabled, password expiring users accounts can use the self service portal and require software licenses. Your disabled user accounts, system AD accounts and users set with “password never expires” are automatically excluded from web portal access and do not require licenses.

1. **Profile Enrollment of a New User - Main landing page – All aspects are customizable**
   User enters nt account name (juser) or UPN (juser@domain.com) or domain\user (ntdomain\juser)

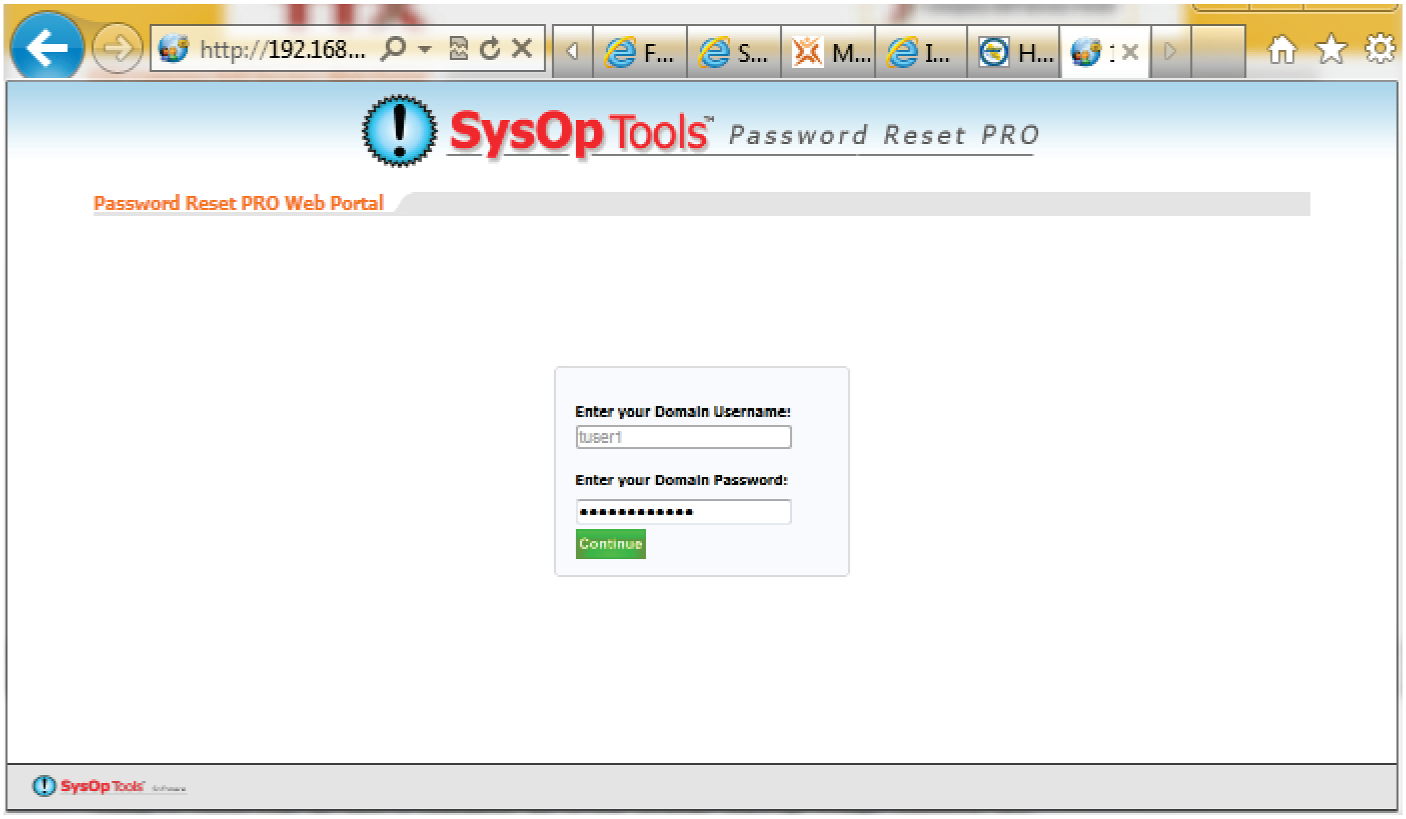


Enter your Domain Username: tuser1

Continued on next page…

2. **Profile Enrollment mode, initial authentication and enrollment of a new user:**

User must “authenticate” the very first time by entering their domain username (or email address) and domain password. The user can enroll even if their current domain password is expired, or they have been given a temporary / must change on next logon password. The only time a new user cannot enroll with this mode is if their domain account is locked out.


http://192.168...
F...
S...
M...
I...
H...
SysOp Tools™ Password Reset PRO
Password Reset PRO Web Portal

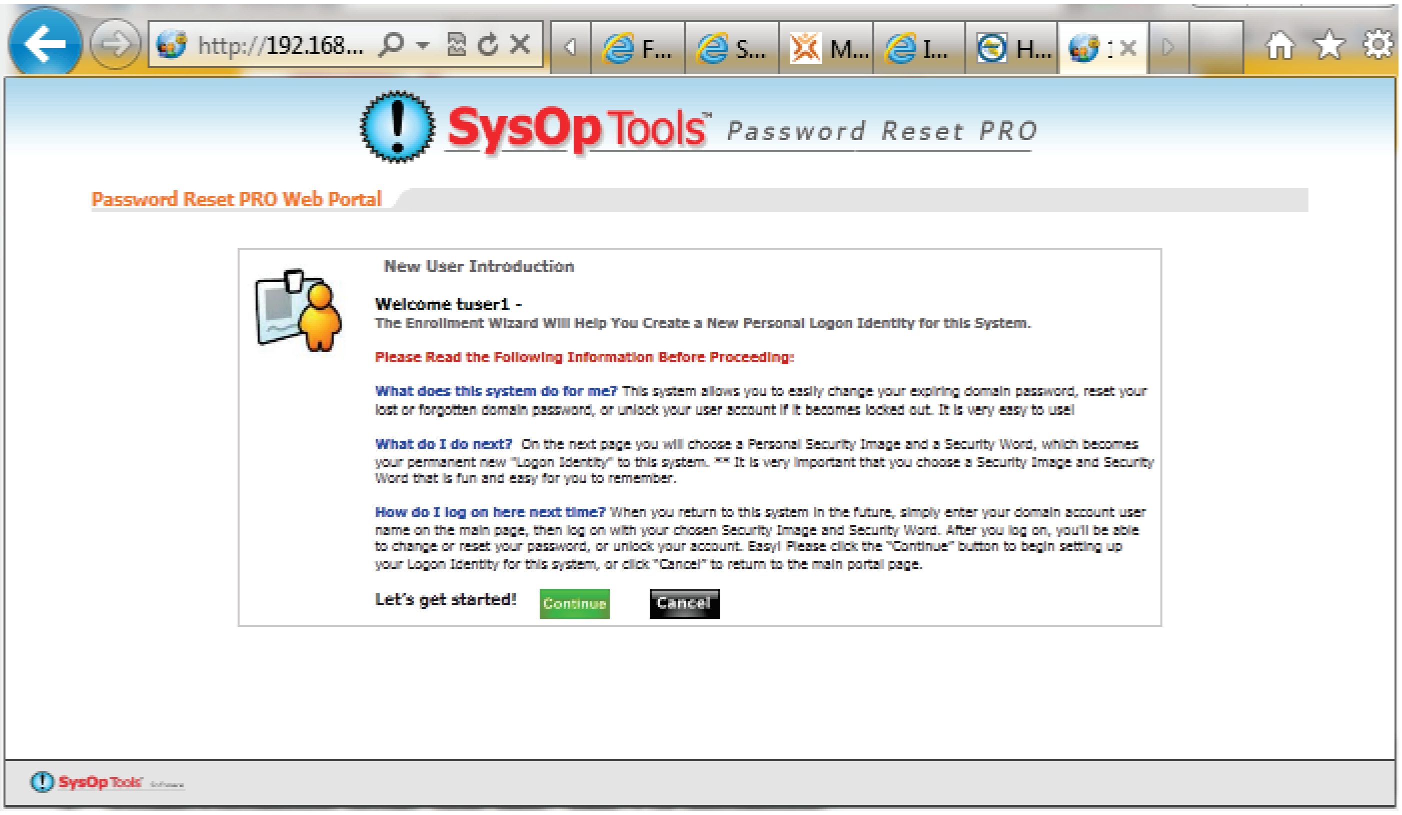
Enter your Domain Username:

tuser1

Enter your Domain Password:

•••••••••••••

3. **Profile Enrollment mode, next step, welcome page:**
   Keep in mind that all text is editable, as is the overall styling, image buttons, etc.


http://192.168...
F...
S...
M...
I...
H...
SysOp Tools™ Password Reset PRO
Password Reset PRO Web Portal

New User Introduction

Welcome tuser1 -

The Enrollment Wizard Will Help You Create a New Personal Logon Identity for this System.

Please Read the Following Information Before Proceeding:

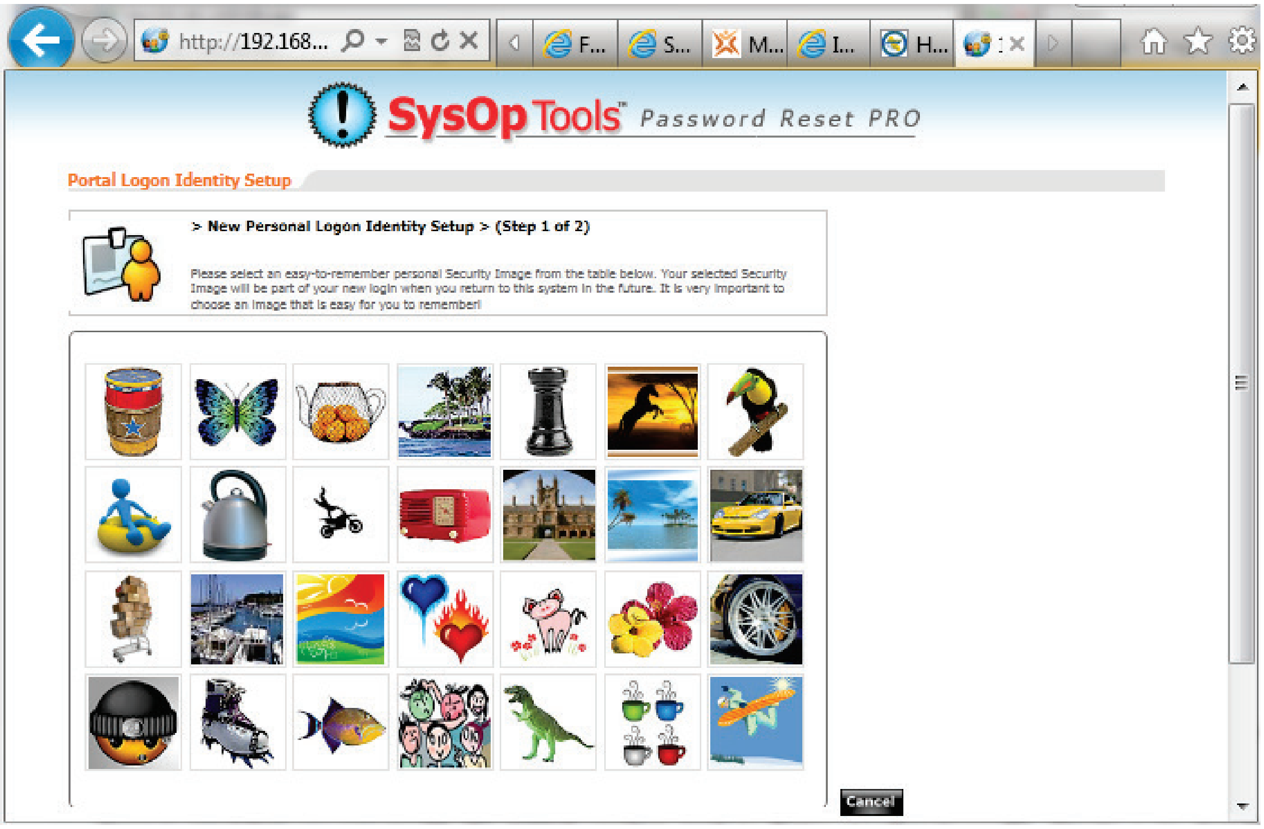
What does this system do for me? This system allows you to easily change your expiring domain password, reset your lost or forgotten domain password, or unlock your user account if it becomes locked out. It is very easy to use!

What do I do next? On the next page you will choose a Personal Security Image and a Security Word, which becomes your permenent new "Logon Identity" to this system. ** It is very important that you choose a Security Image and Security Word that is fun and easy for you to remember.

How do I log on here next time? When you return to this system in the future, simply enter your domain account user name on the main page, then log on with your chosen Security Image and Security Word. After you log on, you'll be able to change or reset your password, or unlock your account. Easy! Please click the "Continue" button to begin setting up your Logon Identity for this system, or click "Cancel" to return to the main portal page.

Let's get started!

4. **Profile Enrollment mode, next step, Step 1 of enrollment:**
   Keep in mind that all security images are editable / replaceable if you would prefer to use a different image set.

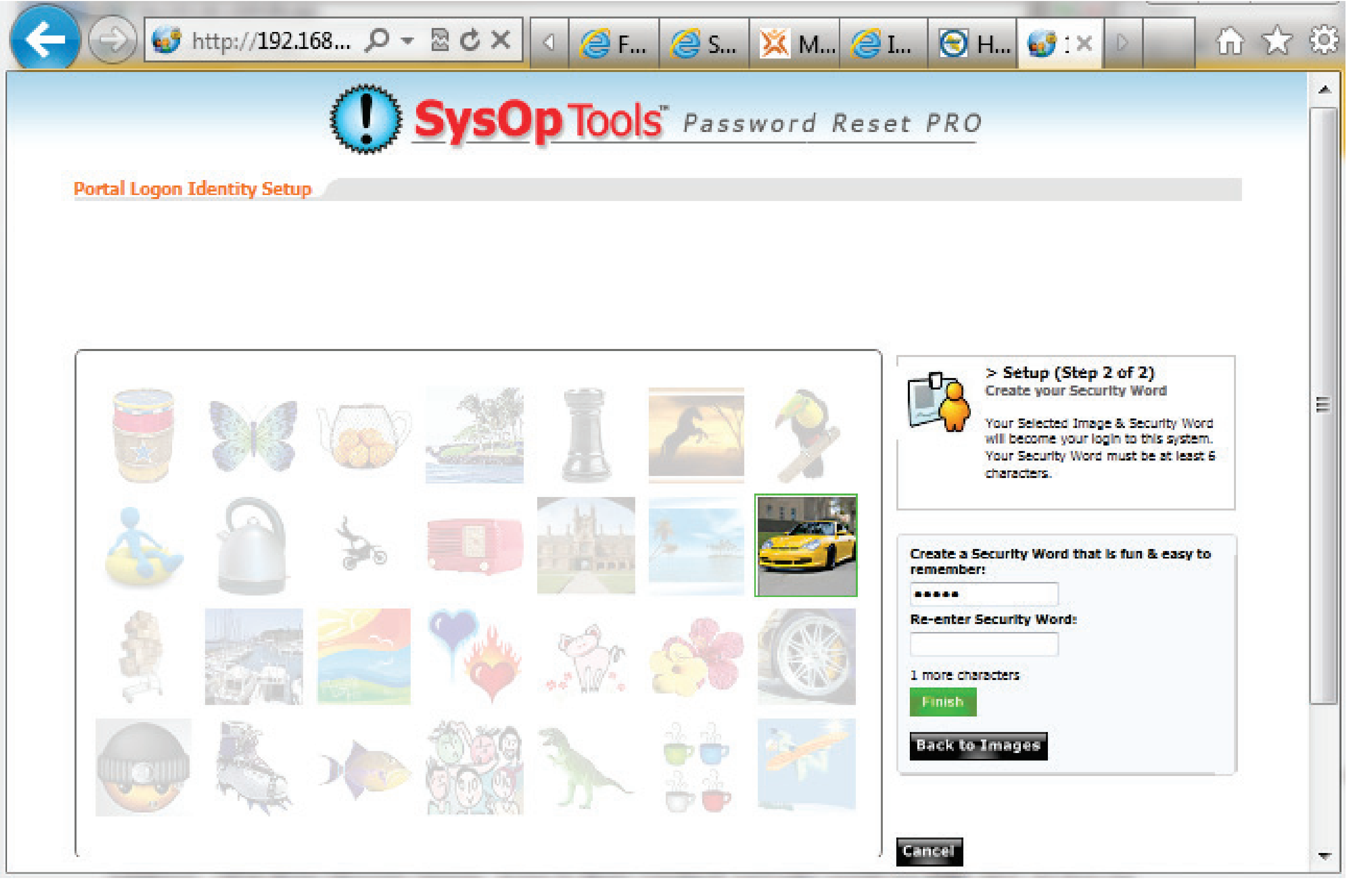


Portal Logon Identity Setup

> New Personal Logon Identity Setup > (Step 1 of 2)

Please select an easy-to-remember personal Security Image from the table below. Your selected Security Image will be part of your new login when you return to this system in the future. It is very important to choose an image that is easy for you to remember!

5. **Profile Enrollment mode, next step, Step 2 of enrollment:**
   Keep in mind that you can modify the default wording, such as ‘Enter your Employee ID’, ‘Create a six-digit PIN’, ‘Enter last four of your SSN’, etc.
   The goal is to ask your users to create something that is very easy to remember but still uniquely secure.



Portal Logon Identity Setup

> Setup (Step 2 of 2)
Create your Security Word

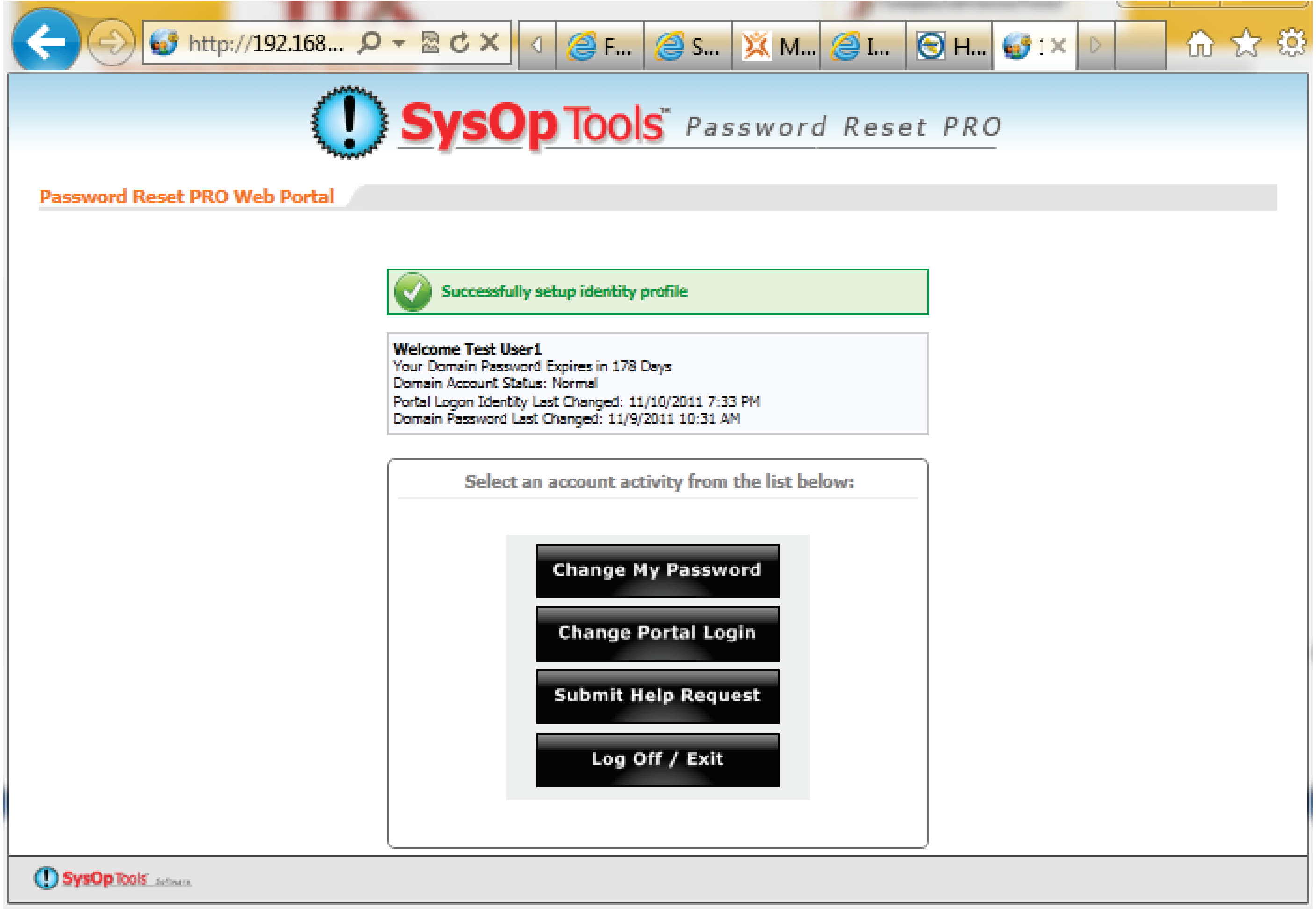
Your Selected Image & Security Word will become your login to this system. Your Security Word must be at least 6 characters.

Create a Security Word that is fun & easy to remember: •••••

Re-enter Security Word:

1 more characters

6. **Profile Enrollment mode, next step, enrollment complete:**
   On returning visit, user will access the self service portal by entering their NT username or domain email address, click their chosen image, type in their created security word (or PIN etc), to log on.
   User can log on if account is locked out or password expired, and self service these situations easily.



Password Reset PRO Web Portal

Successfully setup identity profile

Welcome Test User1
Your Domain Password Expires in 178 Days
Domain Account Status: Normal
Portal Logon Identity Last Changed: 11/10/2011 7:33 PM
Domain Password Last Changed: 11/9/2011 10:31 AM

Select an account activity from the list below:

The enrolled user can now change their password if desired. The change password process automatically enforces your domain password policies, including complexity / history / minimum age.

If a new enrolled user had enrolled with an *expired password* or *temporary password*, the new user would have been automatically taken to the "change my password page" instead of the above main page. Everthing is automated so the user does not have to "think".

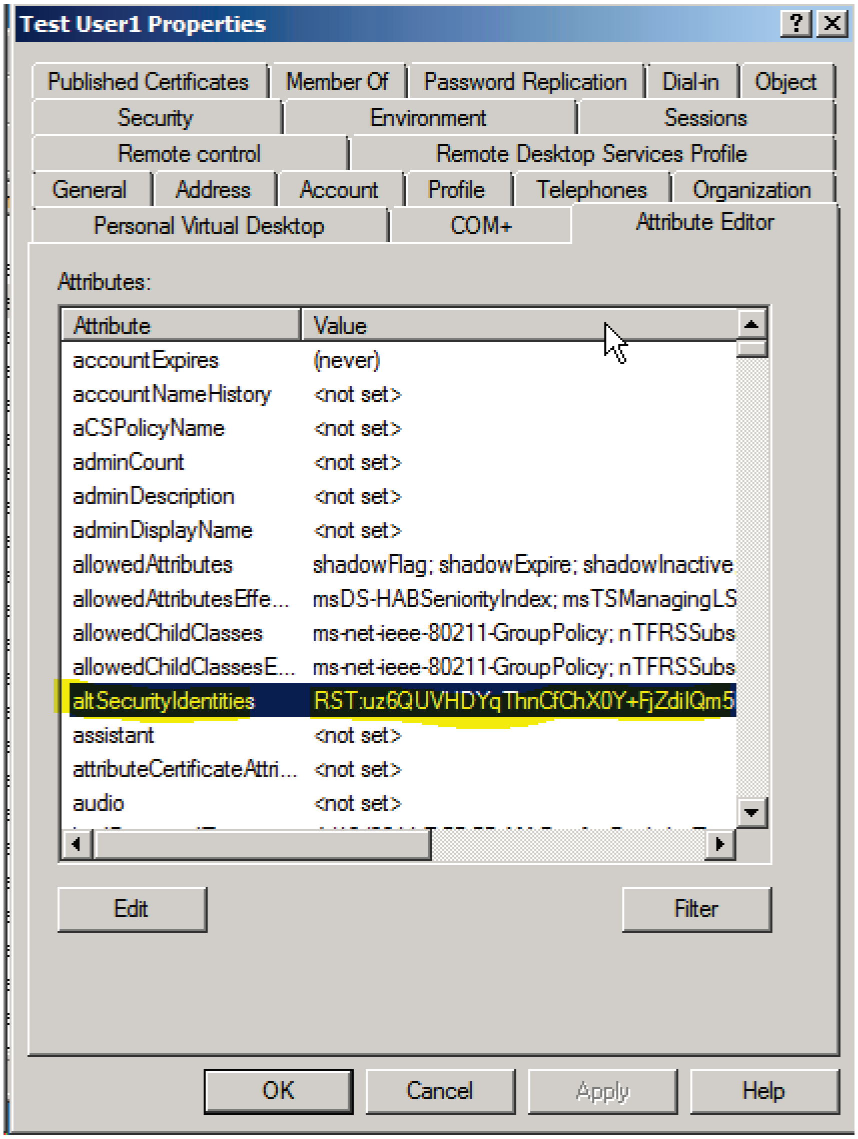
Where is this enrollment data stored for the user?
After the user selects their security image and creates a security word / PIN / etc, the internal "Master Service" portion of our software creates an encrypted token representing the user's enrollment selections and stores it directly in AD in the 'altSecurityIdentities' schema field of their AD account. The data is not accessible to be read or decrypted by anyone except for our software, so their enrolled data is always secure.

The encrypted token representing the image / security word chosen by user is stored securely in AD, so it is not possible to lose user enrollments. No external databases are required.

To un-enroll a user or reset a user's enrollment, it is as simple as deleting the "RST:" token. The user can then easily re-enroll, even if their domain password is expired.

See next page for screenshot of the AD property field and token..

Example of a user's enrolled identity token in Active Directory



Attributes:

Attribute	Value
accountExpires	(never)
accountNameHistory	<not set>
aCSPolicyName	<not set>
adminCount	<not set>
adminDescription	<not set>
adminDisplayName	<not set>
allowedAttributes	shadowFlag; shadowExpire; shadowInactive
allowedAttributesEffe...	msDS-HABSeniorityIndex; msTSManagingLS
allowedChildClasses	ms-net-ieee-80211-GroupPolicy; nTFRSSubs
allowedChildClassesE...	ms-net-ieee-80211-GroupPolicy; nTFRSSubs
altSecurityIdentities	RST:uz6QUVHDYqThnCfChX0Y+FjZdiIQm5
assistant	<not set>
attributeCertificateAttri...	<not set>
audio	<not set>

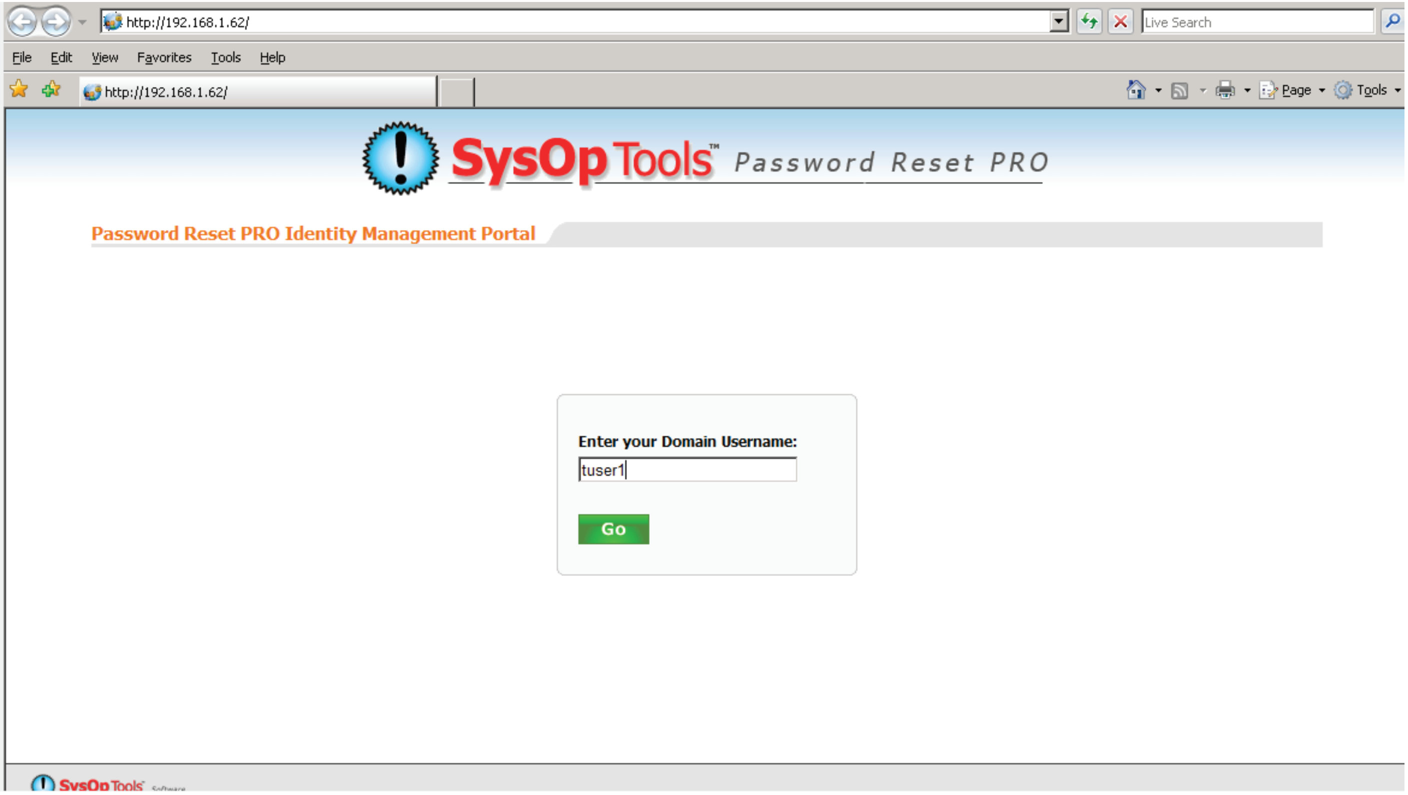
Since we are using an AD field and a unique property value, you can easily build logon scripts to help enforce user enrollment. Simply create a logon script that checks for "RST:*" present under altSecurityIdentities. If the property value is present, ignore. If the property value is not present, prompt the user to enroll.

END OF PART 1

Continued on next page…

PART 2 - ACTIVE DIECTORY DATA MODE – NO PRE-ENROLLMENT REQUIRED – NEW USER CAN SELF SERVICE UNDER ALL SITUATIONS (LOCKED ACCOUNT, EXPIRED PASSWORD ETC)

1. **Active Directory Data mode, main landing page:**
   User enters nt account name (juser), UPN (juser@domain.com) or domain\user (domain\juser)

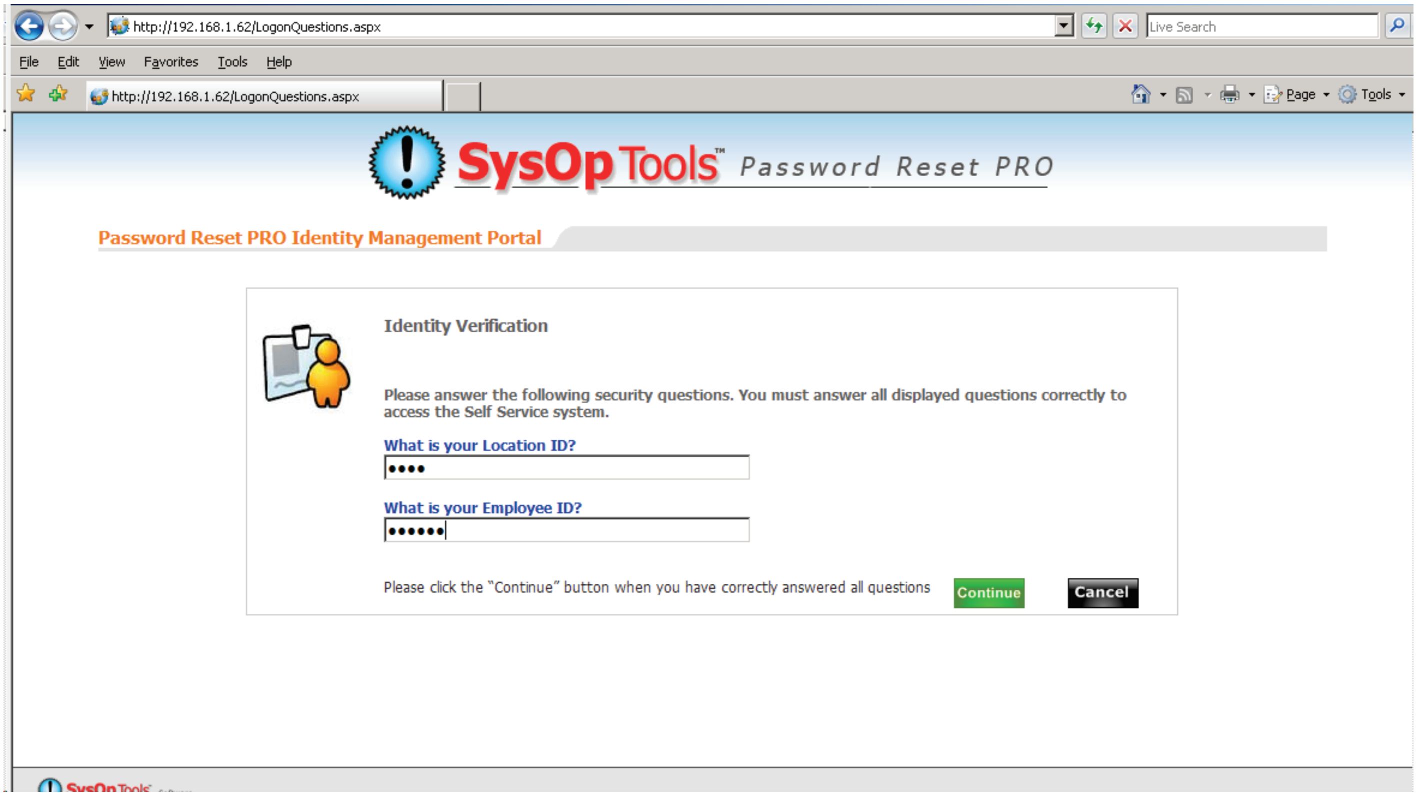


Password Reset PRO Identity Management Portal

Enter your Domain Username:

tuser1

2. **Active Directory Data mode, next step, user answers pre-defined security questions:**
   These questions are set up by the administrator, and the user must enter answers to each question that matches the answer data stored in AD. *See screenshots farther down for clarification.*


http://192.168.1.62/LogonQuestions.aspx
Live Search
File
Edit
View
Favorites
Tools
Help
Page
Tools
SysOp Tools™ Password Reset PRO
SysOp Tools

Password Reset PRO Identity Management Portal

Identity Verification

Please answer the following security questions. You must answer all displayed questions correctly to access the Self Service system.

What is your Location ID?

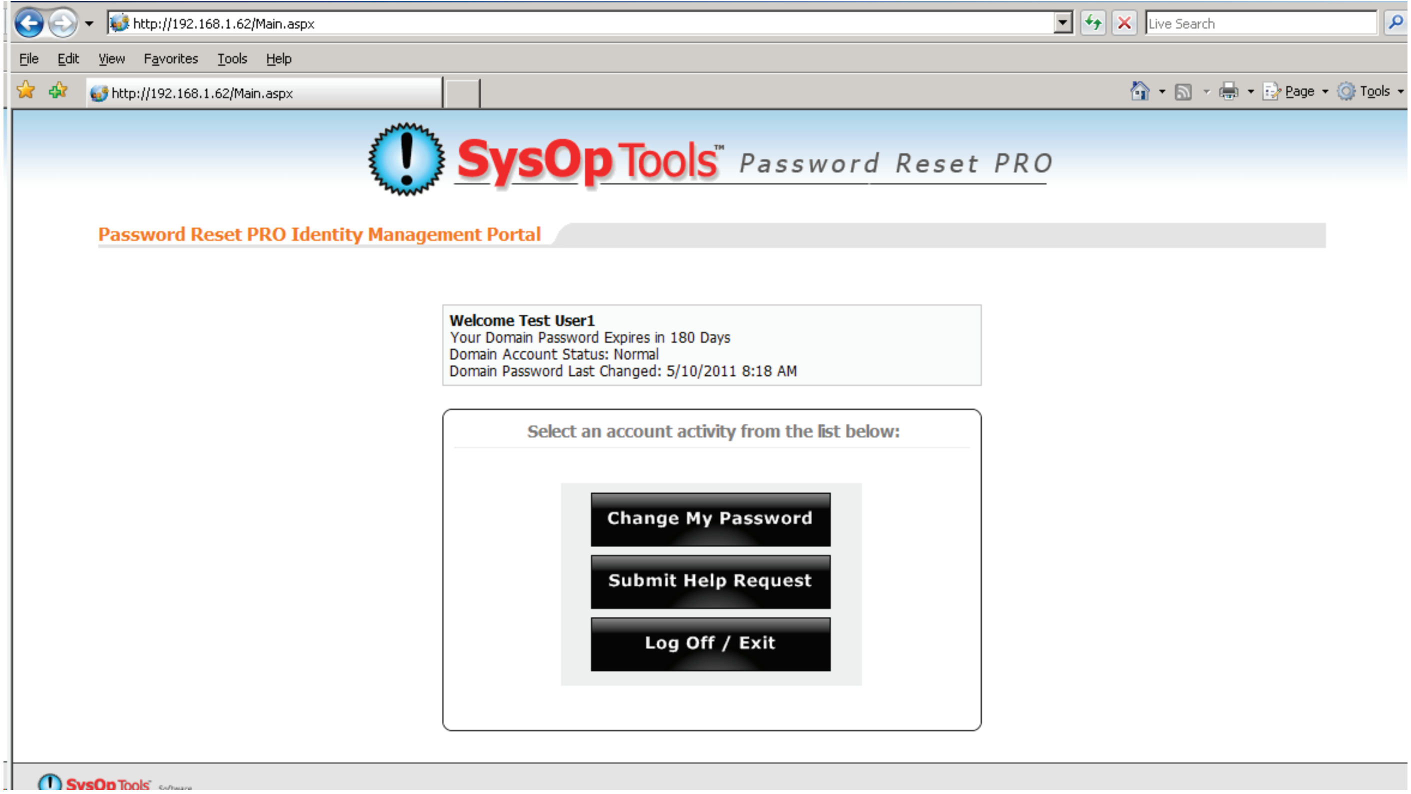
••••

What is your Employee ID?

••••••

Please click the "Continue" button when you have correctly answered all questions

3. **Active Directory Data mode, next step, user successfully answers security questions and is authenticated to self service portal main activity area:**
   Once authenticated, the user can now unlock account, reset password, or change password.



Welcome Test User1
Your Domain Password Expires in 180 Days
Domain Account Status: Normal
Domain Password Last Changed: 5/10/2011 8:18 AM

Select an account activity from the list below:

How are these questions set up for your users?
Question text that appears in the web portal, and the AD field mappings which already contain the answers to the questions are set up in the Master Service portion of software. The user is not asked to choose questions or create answers. The questions will be created by the administrator, from 1 question to as many as you would like. Each question is “mapped” to a field in AD that contains data. The user is simply answering the question with data that should match what is already in AD.

Software Settings in the Master Service for establishing Questions:
In the example screenhots below, we have created two questions to ask users visiting the web self service portal:

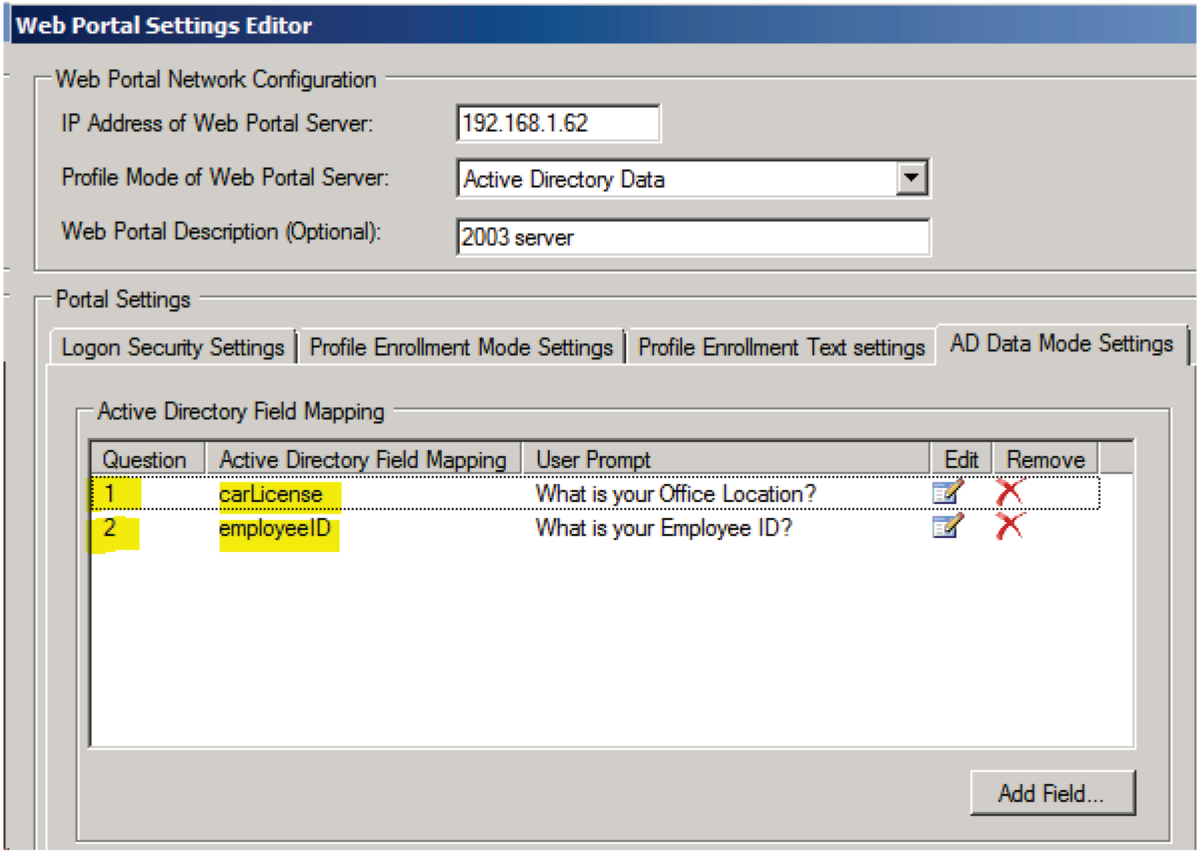
1. “What is your office location?” – this question is mapped to the AD data field, “carLicense”, which contains the answer data “rome”.

2. “What is your employee ID?” – this question is mapped to the AD data field, “employeeID”, which contains the answer data “123456”, and is the employee’s unique ID number.

As long as the user can answer these questions correctly (their typed in answer matches the data field in AD), they are authenticated. You can use any AD field for question mapping, your options are limitless with leveraging data in your Active Directory as a means of authenticating users.

Screenshots continue on next page…

Master Service settings in Password Reset PRO for building the pre-defined questions:



Web Portal Settings Editor

Web Portal Network Configuration

IP Address of Web Portal Server: 192.168.1.62

Profile Mode of Web Portal Server: Active Directory Data

Web Portal Description (Optional): 2003 server

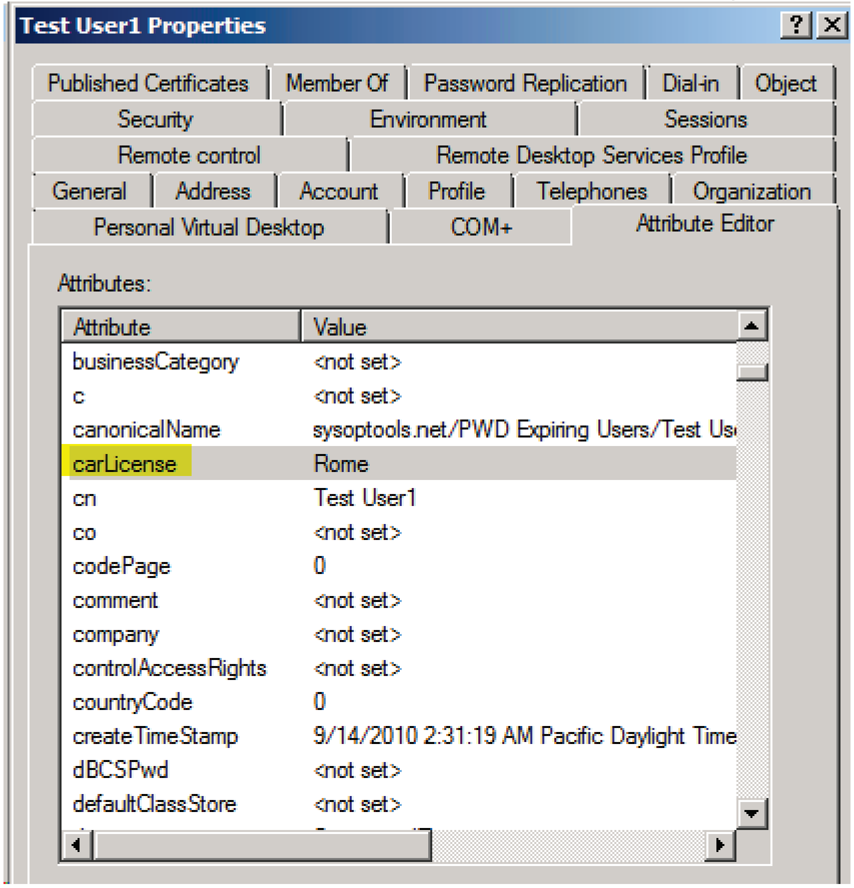
Portal Settings

Logon Security Settings
Profile Enrollment Mode Settings
Profile Enrollment Text settings
AD Data Mode Settings

Active Directory Field Mapping

Question	Active Directory Field Mapping	User Prompt	Edit	Remove
1	carLicense	What is your Office Location?	✎	✗
2	employeeID	What is your Employee ID?	✎	✗

Active Directory field data must pre-exist for questions displayed to user in the web portal – ADUC:
Question1 "What is your Office Location?" is mapped to the "carLicense" answer field in ADUC, and the AD field contains the answer "Rome". The user must answer "rome" in the web portal, because it matches AD:

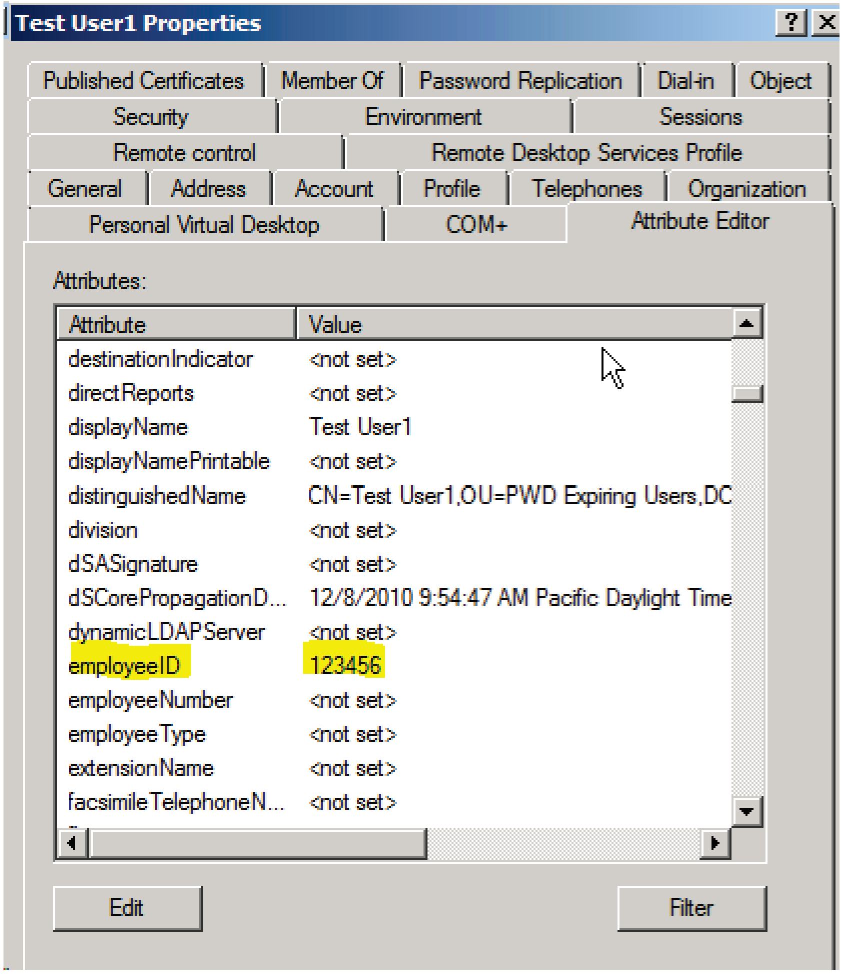


Test User1 Properties

Attributes:

Attribute	Value
businessCategory	<not set>
c	<not set>
canonicalName	sysoptools.net/PWD Expiring Users/Test Us
carLicense	Rome
cn	Test User1
co	<not set>
codePage	0
comment	<not set>
company	<not set>
controlAccessRights	<not set>
countryCode	0
createTimeStamp	9/14/2010 2:31:19 AM Pacific Daylight Time
dBCSPwd	<not set>
defaultClassStore	<not set>

Question2 – “What is your Employee ID?” is mapped to answer field “employeeID” in AD:



Attribute	Value
destinationIndicator	<not set>
directReports	<not set>
displayName	Test User1
displayNamePrintable	<not set>
distinguishedName	CN=Test User1,OU=PWD Expiring Users,DC
division	<not set>
dSASignature	<not set>
dSCorePropagationD...	12/8/2010 9:54:47 AM Pacific Daylight Time
dynamicLDAPServer	<not set>
employeeID	123456
employeeNumber	<not set>
employeeType	<not set>
extensionName	<not set>
facsimileTelephoneN...	<not set>

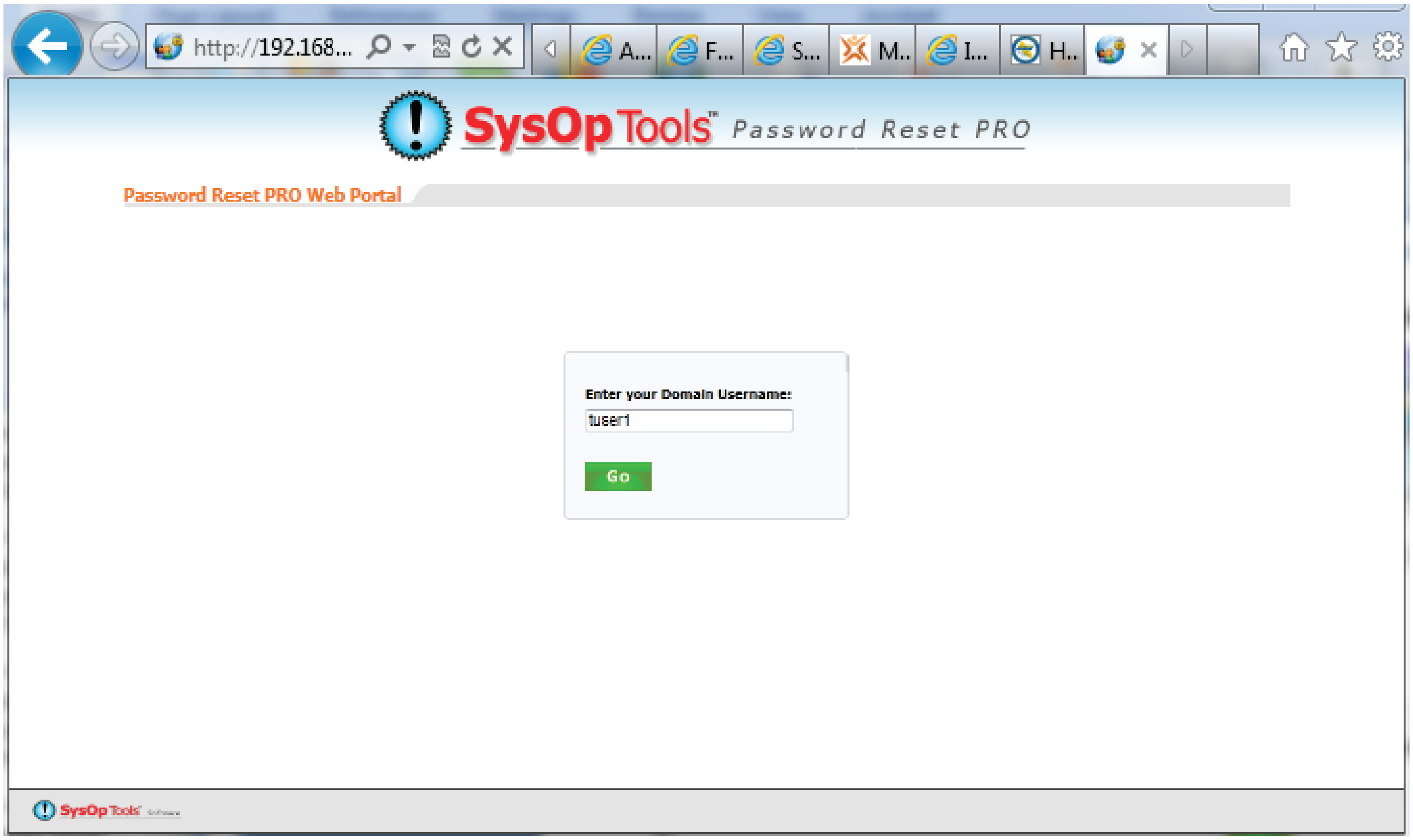
You can set up as many questions as needed, the only requirement is that you have the answer data already populated in AD for each question’s mapped field. The user is not asked to set up their own questions or set up their own data.

END OF PART 2

PART 3 – DOMAIN BASIC AUTHENTICATION MODE WEB PORTAL – NO ENROLLMENT REQUIRED. USER CAN CHANGE CURRENT PASSWORD, EXPIRED PASSWORD AND TEMPORARY PASSWORD, BUT CANNOT UNLOCK A LOCKED ACCOUNT.

1. **Domain Basic Authentication Mode, User First Time Access, Main landing page – All aspects are customizable**
   User enters nt account name (juser) or UPN (juser@domain.com) or domain\user (ntdomain\juser)

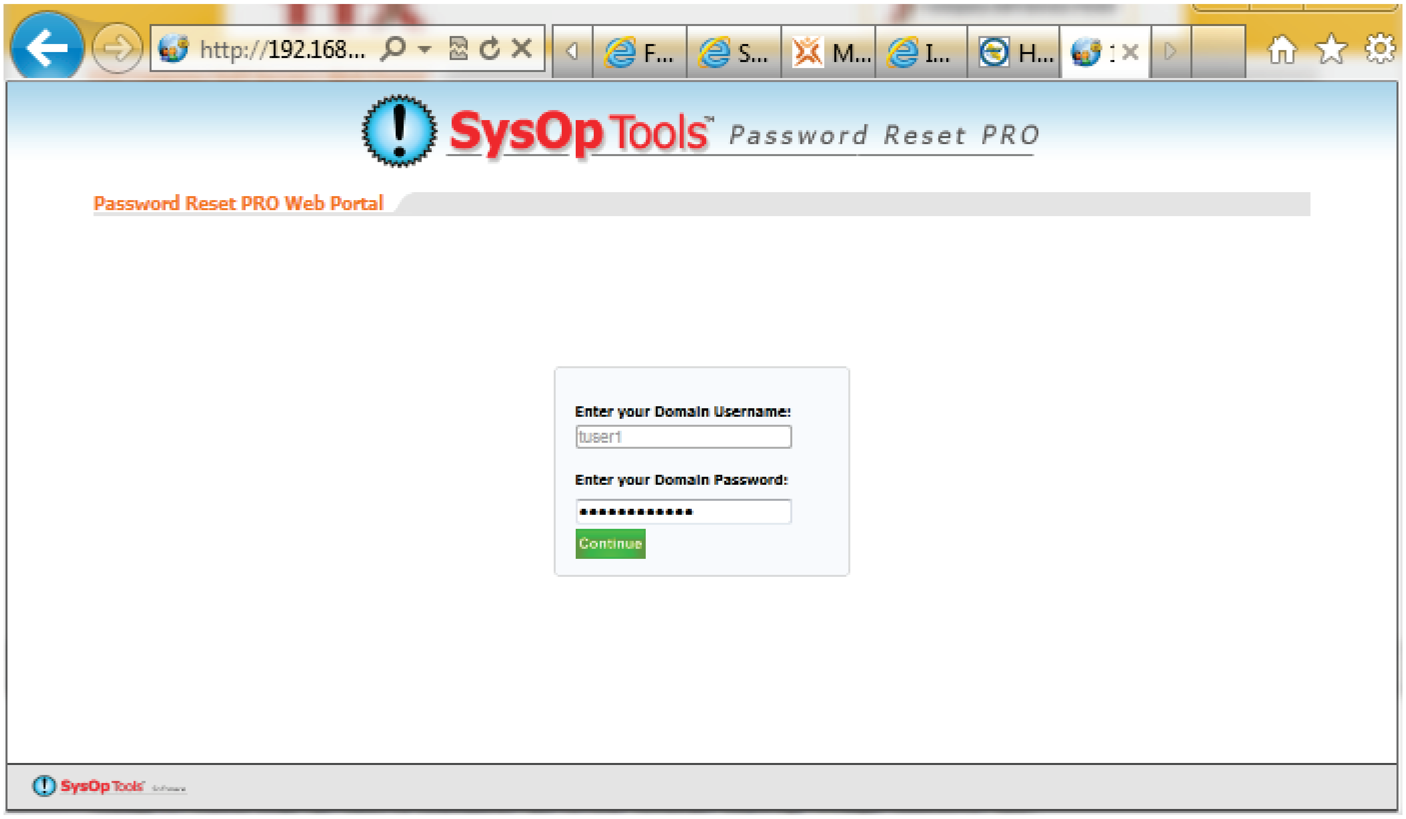
   Screenshots continued on next page…



Enter your Domain Username: tuser1

2. **Domain Basic Authentication Mode, initial authentication of a user:**

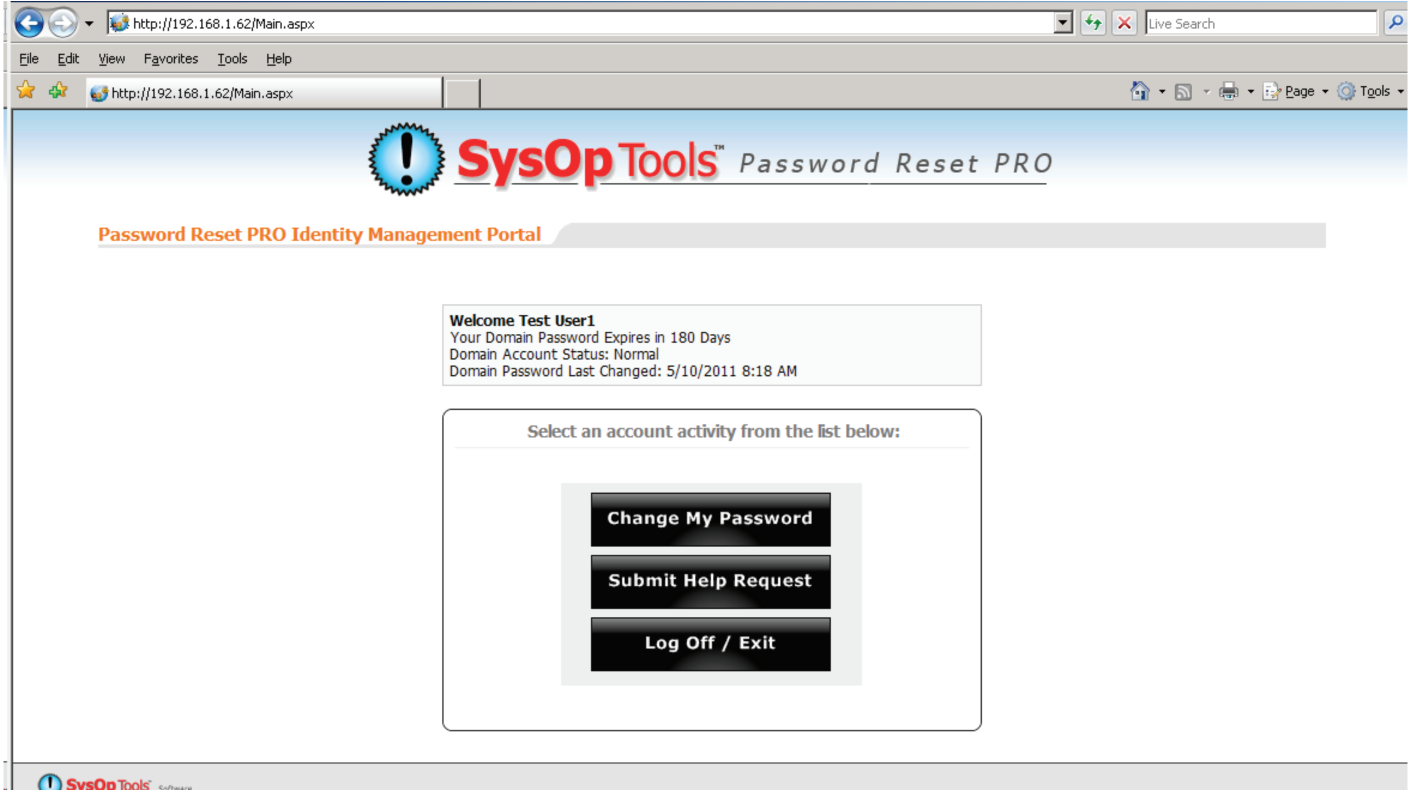
User must “authenticate” by entering their domain username (or email address) and domain password. The user can access this mode if their domain password is currently active, expired, or they have been given a temporary / must change on next logon password. The only time a new user cannot acces this mode is if their domain account is locked out. This mode is extremely handy for use inside the LAN (Mac users etc), and in newhire orientations where users must change their issued temporary domain password.



Enter your Domain Username: tuser1

Enter your Domain Password: •••••••••••••

3. **Domain Basic Authentication mode, next step, user is authenticated to self service portal main activity area:**
   Once authenticated, the user can now change their password or reset their password.



Welcome Test User1
Your Domain Password Expires in 180 Days
Domain Account Status: Normal
Domain Password Last Changed: 5/10/2011 8:18 AM

Select an account activity from the list below:

http://192.168.1.62/Main.aspx
Live Search
File Edit View Favorites Tools Help
Page Tools
SysOp Tools™ Password Reset PRO
Password Reset PRO Identity Management Portal
Change My Password
Submit Help Request
Log Off / Exit
SysOp Tools Software

We do not recommend deploying this mode publically to the internet since there is no 3rd factor of user authentication, which is provided by the other two Web Portal modes. Plus, users will not be able to unlock a locked out account with this mode.

END OF PART 3

PART 4 – ACCESSING THE SELF SERVICE WEB PORTAL FROM MOBILE DEVICES

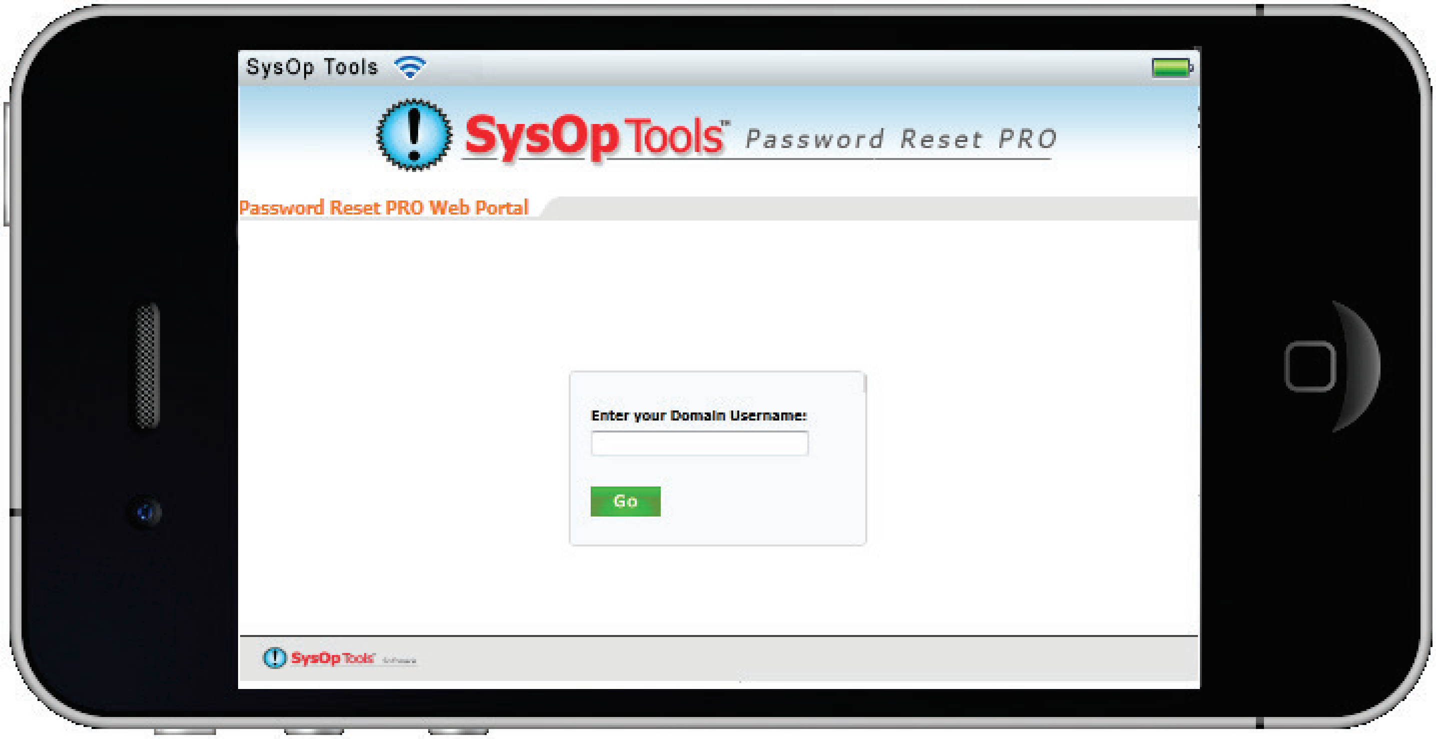
Mobile Device Access:
All web portal pages will render on web enabled mobile devices such as iPhone, iPad, Android, WM, BB. This offers the ultimate level of convenince for your end users. No app installations are required.

Continued on next page…

A. Profile Enrollment Mode Web Portal

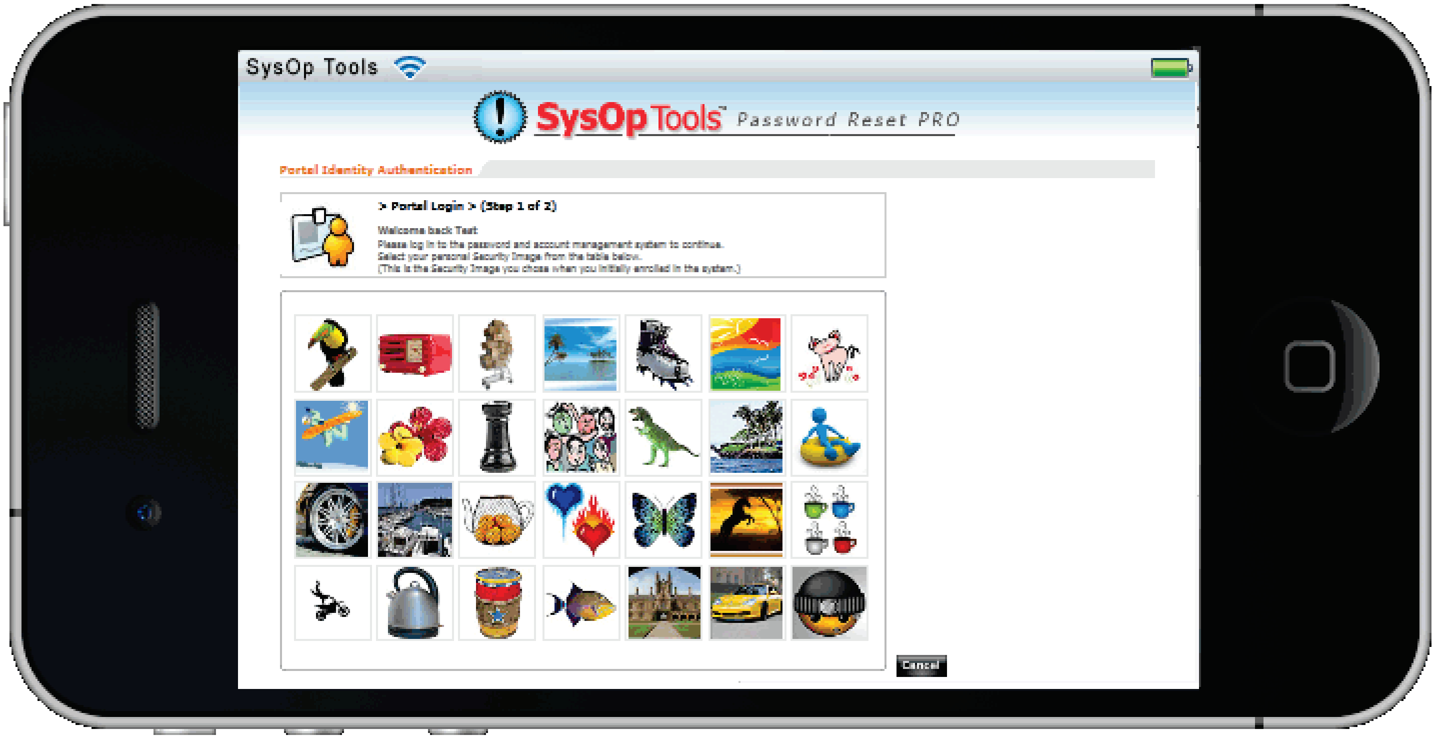
The Following Screenshots Show Example of and Enrolled User Logging on to the Profile Enrollment Mode Web Portal. This mode renders very fast on web enabled mobile devices, but may require some pinch zooming on the image thumbnails, depending on the screen size of the mobile device.

1. **Enter the enrolled user's domain username, touch "Go"**



Enter your Domain Username:

2. **User must select the security image chosen at time of enrollment by touching a thumb tile**

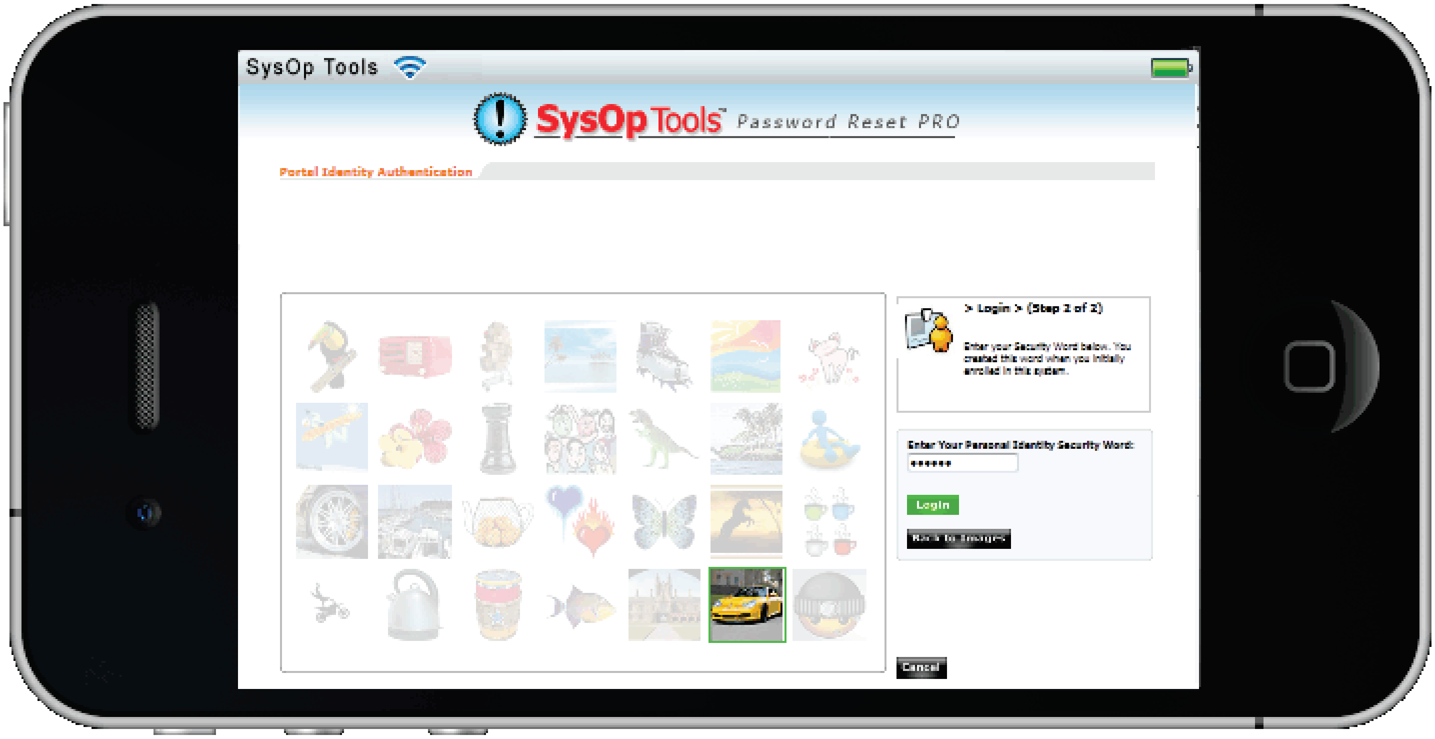


SysOp Tools
SysOp Tools Password Reset PRO
Portal Identity Authentication

> Portal Login > (Step 1 of 2)

Welcome back Test
Please log in to the password and account management system to continue.
Select your personal Security Image from the table below.
(This is the Security Image you chose when you initially enrolled in the system.)

3. User must enter their security word (or PIN, etc) that was created at time of enrollment, then touch “Login”

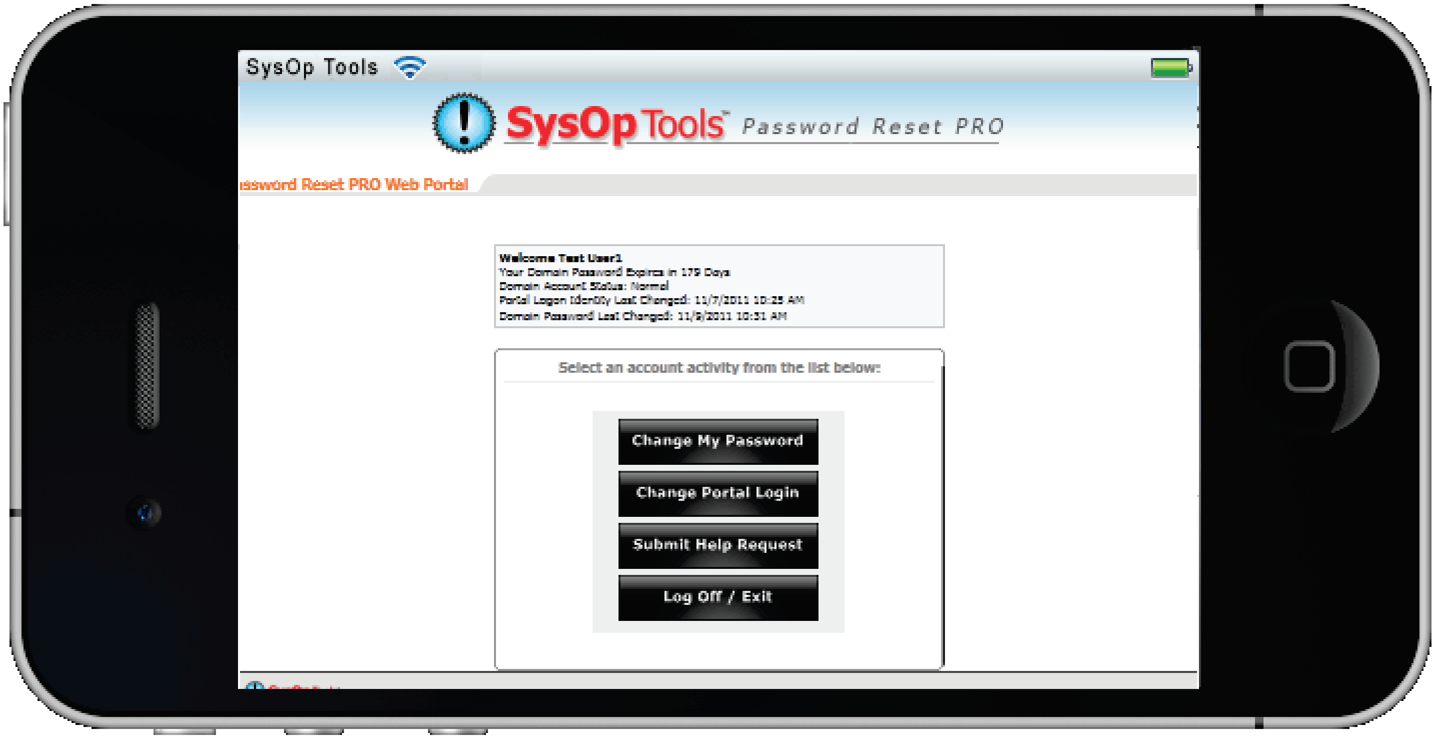

SysOp Tools
SysOp Tools Password Reset PRO
Portal Identity Authentication
> Login > (Step 2 of 2)

Enter your Security Word below. You created this word when you initially enrolled in this system.

Enter Your Personal Identity Security Word: ******

Login
Back to Images
Cancel

4. Access granted to the enrolled user. Enrolled user may now unlock account, reset password, or change password.



Welcome Test User1
Your Domain Password Expires in 179 Days
Domain Account Status: Normal
Portal Logon Identity Last Changed: 11/7/2011 10:25 AM
Domain Password Last Changed: 11/9/2011 10:31 AM

Select an account activity from the list below:

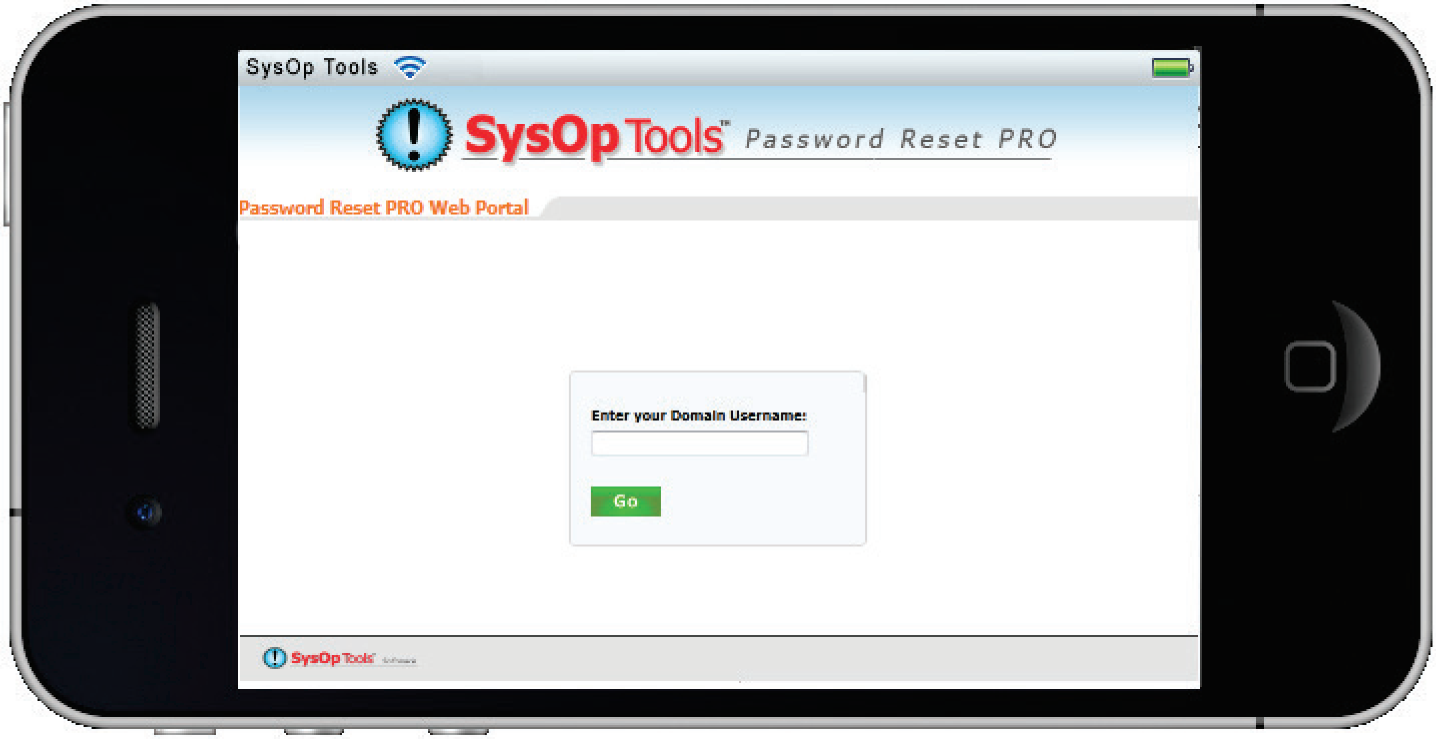
End of Profile Enrollment Mode Web Portal screenshots

Continued on next page…

B. Active Directory Data Mode

Next set of screenshots shows example of logging on to the Active Directory Data Mode Web Portal. No previous enrollment is required and this is the fastest access method for mobile device users:

1. User enters domain username, or email address, or domain\username and touches "Go"



SysOp Tools

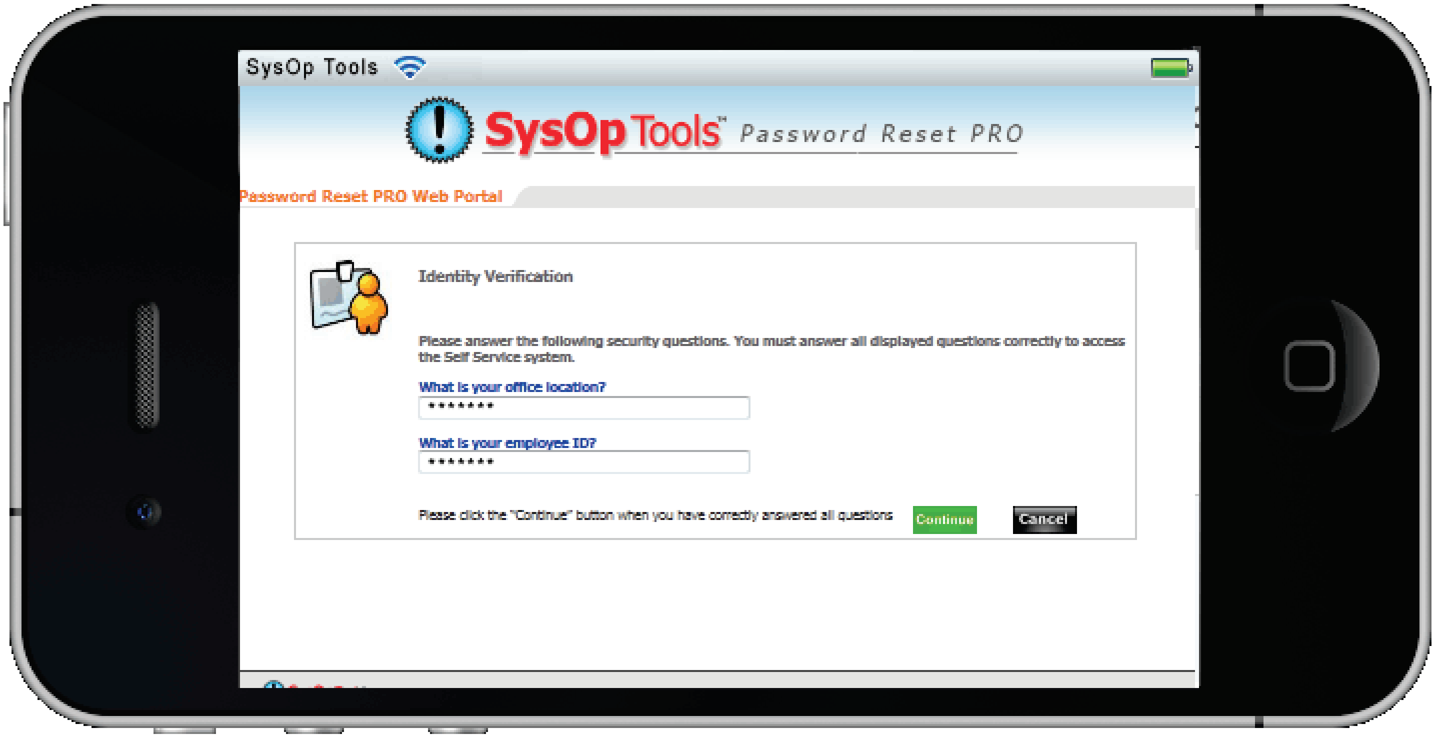
SysOp Tools Password Reset PRO

Password Reset PRO Web Portal

Enter your Domain Username:

Go

2. User correctly answers the presented security questions established by the IT administrator, then touches "Continue"



SysOp Tools

SysOp Tools Password Reset PRO

Password Reset PRO Web Portal

Identity Verification

Please answer the following security questions. You must answer all displayed questions correctly to access the Self Service system.

What is your office location?

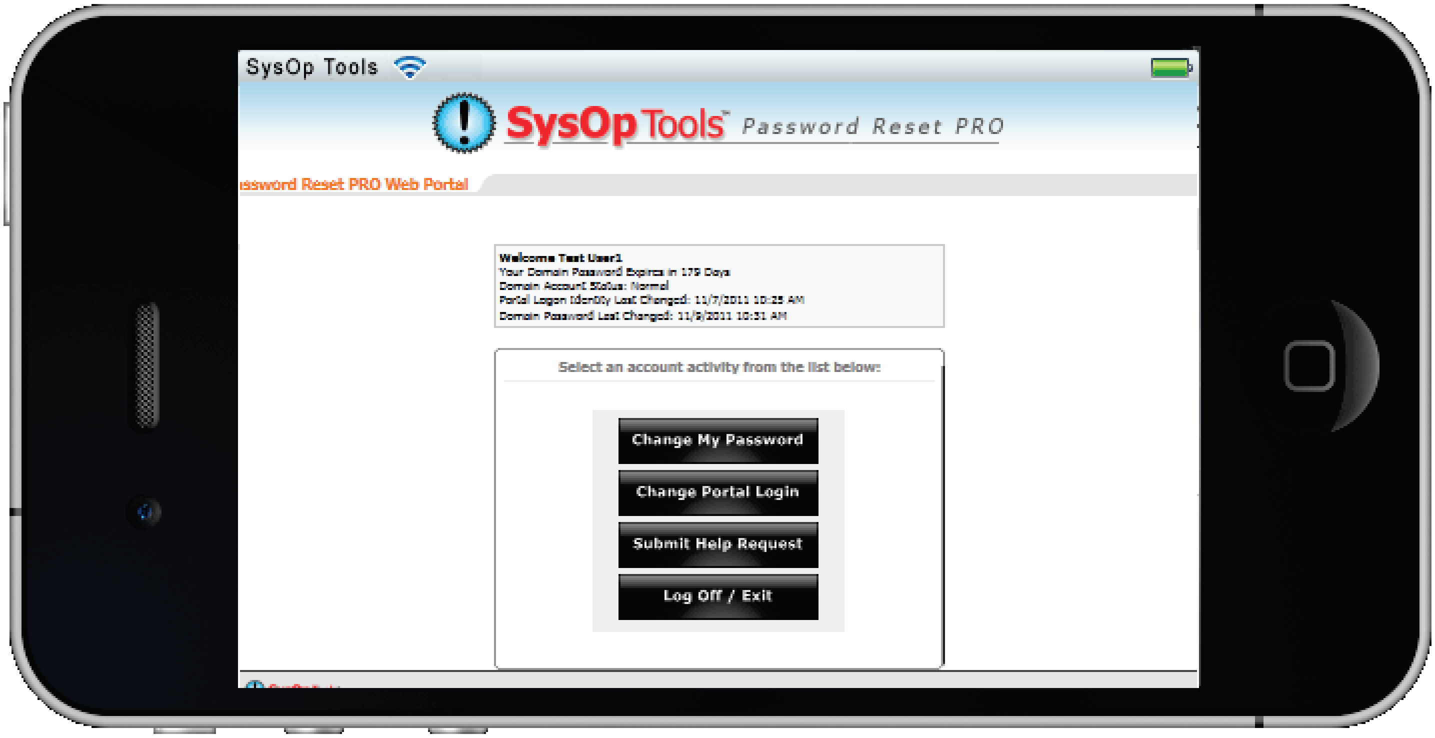
****

What is your employee ID?

****

Please click the "Continue" button when you have correctly answered all questions

3. **Access granted to user after correctly answering security questions. User may now unlock account, reset password, or change password.**


SysOp Tools
SysOp Tools Password Reset PRO
assword Reset PRO Web Portal
Select an account activity from the list below:
Change My Password
Change Portal Login
Submit Help Request
Log Off / Exit

Welcome Test User1
Your Domain Password Expires in 179 Days
Domain Account Status: Normal
Portal Logon Identity Last Changed: 11/7/2011 10:25 AM
Domain Password Last Changed: 11/9/2011 10:31 AM

End of Active Directory Data Mode Web Portal screenshots

The same process for mobile device access also applies to the "Domain Basic Authentication" mode web portal.

END OF GUIDE

--

Enterprise Support Team
SysOp Tools, Inc.
877-SYSOPTOOLS
Direct / Fax 213-995-5060
www.sysoptools.com