

Benefits Summary of Changing to the Guest Account System for URMIC Guest Accounts:

- First step in replacing ADTools, aligning the Medical Center with current University guest account creation and management processes.
- Proactive, streamlined management of guest accounts.
- Elimination of manual account management processes and subsequent human error
- No need to print or request additional welcome letters
- Ability to quickly request bulk account creations
- Longer expiration dates
- No more terminations of accounts for lack of use
- Ability to manage multiple account passwords from a single site
- Guests will now have an identity within the University Identity Management System.

Changes for URMCA ADTool's Users:

Process	Current State with ADTools	New State Using the Guest Account System	Benefits of the Guest Account System
Create New Guest Accounts	The URMCA sponsor submits a request in ADTools. Identity Management processes the request after obtaining approvals and proof of antivirus and encryption.	The URMCA sponsor submits a request through the Guest Account System and agrees to the " Sponsor Agreement ".	
Expiration Date Maximum Length	Six months	Thirteen months	Sponsor maintenance of account expirations is reduced by over 50%.
URID Creation	<p>Once the account is created in ADTools, the new user ID has to be manually added to a URID generation table. The welcome letter sent by ADTools contains instructions on how to enter their Personal Identifying Information (PII) through the "URMCA Identity Matching/Generation" site.</p> <p>*Personal Identifying Information includes information such as name, date of birth, social security number, home address and phone, personal e-mail address, etc. Employers have limitations on use, posting, printing and communicating of PII. Sponsors NEVER see guest's PII.</p>	<p>The Guest Account System allows the guest to input their PII at the time the request is submitted if the guest is with the requestor at the time of submission.</p> <p>If the guest is not with the requestor at the time of submission, the guest receives an email with a link to self-enter their PII in the Guest Account System.</p> <p>Again, sponsors never see their Guest PII</p>	Sponsors will no longer need to direct their guest to the " URMCA Identity Matching/Generation " site.

Stale Account Terminations	Accounts that have not been logged into in over six months are terminated/disabled as "stale".	Accounts will never be terminated/disabled as stale.	As long as the sponsor extends the expiration date, your guests will never lose access and have to have an ISD Help Desk ticket created to have their account reactivated by Identity Management.
Account Approval Process for Non-employee Accounts	Approvals are required by either Identity Management or the Privacy and Security Officials. If the guest will be using a personal device, the guest is required to provide screenshots of a recent clean full system disk antivirus scan and full system disk encryption.	At the time of the request submission, the sponsor is required to attest to a " Sponsor Agreement ".	The "Sponsor Agreement" will do away with the email back and forth with IdM and also do away with the need to have your guests capture anti-virus and encryption screenshots greatly streamlining account creation.

Management of Accounts:

<ul style="list-style-type: none"> View Status of ALL Accounts 	Only possible through a ticket to the ISD Help Desk. Identity Management would then manually put together a list to send to the sponsor.	Sponsors will see all of their guest accounts in the Guest Account System, the current state of the accounts and the expiration dates as soon as they log into the system.	Sponsors can quickly see the status of all of their guests allowing proactive management.
<ul style="list-style-type: none"> Update Account Expirations 	An entirely manual process including: <ul style="list-style-type: none"> generating the list of upcoming expiring accounts multiple rounds of emails notifications are sent to hundreds of sponsors (none to guests) tracking of responses and updating accounts no feedback to sponsors 	Email notifications to sponsors AND guests are automated (30, 14 and 7 days before expiration) Sponsors extend accounts by logging into the Guest Account System with their NetID and extend the expiration date as needed.	Sponsors AND guests can proactively ensure that their vital guest accounts never expire and lose access. Sponsors and guests should never again be surprised to learn that an account has expired.

<ul style="list-style-type: none"> Termination of Accounts 	<p>A request is submitted through ADTools or by creating a ticket with the ISD Help Desk.</p> <p>Critical terminations are performed by contacting the ISD Help Desk and filling out the "Critical Termination Request Form".</p>	<p>Sponsors will be able to terminate guest relationships by logging into the Guest Account System and selecting the "End Sponsorship Now" option.</p> <p>There will be no change to critical terminations.</p>	<p>Sponsors can proactively terminate their accounts as needed and do not have to contact the ISD Help Desk.</p>
<ul style="list-style-type: none"> Reactivate Expired Accounts for the Same Role 	<p>A request is submitted through the ISD Help Desk for Identity Management to update the expiration date.</p>	<p>Sponsors will be able to reactivate accounts by logging into the Guest Account System and selecting the "Reactivate" button.</p>	<p>Sponsors can proactively extend their accounts as needed and do not have to contact the ISD Help Desk.</p>
<ul style="list-style-type: none"> Reactivate Expired Accounts for A Different Role 	<p>An ADTools transfer request is submitted and processed by Identity Management.</p>	<p>Sponsors will be able to reactivate accounts by logging into the Guest Account System and submitting a new guest account request.</p>	<p>Sponsors can proactively extend accounts as needed and do not have to contact the ISD Help Desk.</p>
<ul style="list-style-type: none"> Reactivate Terminated Accounts for Same Role 	<p>An account rollback to the same state as prior to the termination can be completed within the first six months of the termination by submitting an ISD Help Desk request. Identity Management then rolls the account back to its prior state.</p> <p>Anything greater than six months past the termination requires an ADTools transfer request to reactivate the account.</p>	<p>Sponsors will be able to reactivate accounts by logging into the Guest Account System and selecting the "Reactivate" button.</p>	<p>Sponsors can proactively reactivate accounts as needed and do not have to contact the ISD Help Desk.</p>
<ul style="list-style-type: none"> Reactivate Terminated Accounts for Different Role 	<p>An ADTools transfer request is submitted and processed by Identity Management.</p>	<p>Sponsors will be able to reactivate accounts by logging into the Guest Account System and submitting a new guest request.</p>	<p>Sponsors can proactively reactivate accounts as needed and do not have to wait for the ADTools request to be processed.</p>

<ul style="list-style-type: none"> Account Initialization 	<p>Your manager or ADTools requestor gives the end user their username and temporary password on a piece of paper.</p>	<p>Guests go to https://myidentity.rochester.edu/newuser, identify themselves with their DOB and URID, and provide what they want their initial password to be set to.</p> <p>Tutorial: https://tech.rochester.edu/tutorials/account-initialization-workflow/</p>	<p>Initial passwords are not generated and transferred. They're set by the guest.</p>
<ul style="list-style-type: none"> Password Change (User knows current password) 	<p>Users can reset their password through ADTools Account Self Service "Reset Password".</p>	<p>Users can reset their password through myIdentity Self Service.</p>	<p>Users have the ability to reset and manage all university related passwords through myIdentity Self Service.</p>
<ul style="list-style-type: none"> Forgot Password (User doesn't know their current password) 	<p>If security questions were setup in ADTools, users can use the "Forgot Password" option or contact the ISD Help Desk and have their identity verified through a third-party tool before the guest can reset their password.</p>	<p>If security questions were setup in myIdentity, users can use the "Forgot your password?" option or contact the ISD Help Desk and have their identity verified through a third-party tool before the guest can reset their password.</p>	<p>Users are prompted and encouraged to setup their security questions as part of the onboarding process with the Guest Account System and myIdentity Account Initialization.</p>
<ul style="list-style-type: none"> Requesting Additional Permissions 	<p>ADTools has check boxes to add the following permissions and a free form box to request any other permissions not included in the ADTools template.</p> <ul style="list-style-type: none"> eRecord icon collect credit card data Pyxis 	<p>Sponsors will need to reach out the ISD Help Desk or the end user will be able to use the Self Service Portal to request permissions not included in the selected guest template.</p>	
<ul style="list-style-type: none"> Name Changes 	<p>End users call the ISD Help Desk and have their identity verified through a third-party site. The Help Desk agent processes the name changes and sends tickets for applications with local access credentials. If the NetID needs updated, the ISD Help Desk warm transfers the end user to the University Help Desk.</p>	<p>No changes.</p>	

<ul style="list-style-type: none"> • NetID Creation 	<p>Guests are not required to obtain NetIDs.</p>	<p>All guests are provisioned with a NetID as well as a UR or URM domain account.</p>	<p>Users have the ability to reset and manage all university related passwords through myIdentity Self Service. Provisioning a NetID aids in uninterrupted access to applications as applications transition from NetID authentication to AD authentication in the future.</p>
<ul style="list-style-type: none"> • Voluntary Faculty Onboarding 	<p>A non-employee request is submitted through ADTools. Departmental chair approvals are required and proof of antivirus and encryption are requested for non-URMC managed devices. Accounts are provisioned with expiration dates up to six months into the future.</p>	<p>An employee request is submitted through ADTools. The request will be processed as a normal employee request and no expiration date will be placed on the account.</p>	<p>Users no longer have to get approvals and accounts no longer have to be renewed every six months.</p>
<ul style="list-style-type: none"> • Welcome Letters for New Accounts 	<p>The requestor of the ADTools template receives a welcome letter with instructions on how to initialize their account using the MyIdentity New User site or reset their password with their username and temporary password.</p>	<p>The requestor and the end user will receive an email with their URID instructing them to initialize their accounts through MyIdentity New User</p>	<p>Users have the ability to reset and manage all university related passwords through myIdentity Self Service.</p>
<ul style="list-style-type: none"> • Phone and Office Locations for New Accounts 	<p>Phone and office location information for the Outlook Global Address List (GAL) was populated by the ADTools requestor inputting the information into the ADTools requests.</p>	<p>Phone and office location information for the Outlook Global Address List (GAL) will be requested by contacting the ISD Help Desk.</p>	