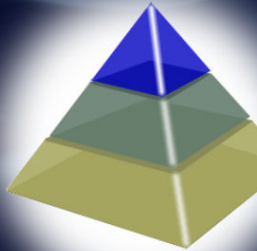


NC Identity Management (NCID)



Identity Management,
Authentication,
Authorization

NCID Program is directed by the Technology Planning Group (TPG)

TPG is a board of CIO's that advise George Bakolia and Bill Willis

TPG has authorized a TPG-Steering Committee made up of agency representatives to set direction for the service offering.



Agenda

- *What is NCID - Glenn*
- *Why NCID - Glenn*
- *Delineation of Responsibilities - Brent*
- *Delegated Administration - Brent*
- *High Priority Issues - Brent*
- *Changes Completed and Planned - Brent*
- *BEACON Portal Troubleshooting Guide - Terry*
- *Information - Terry*
- *Questions*

We have been asked to put together a presentation in collaboration with BEST, specifically Terry Senter, that will be given to a group of NCID administrators from the Wave 2 agencies in order to improve the rollout of BEACON.

In doing so, we also want to take the opportunity to say what is NCID, why are we requiring NCID...what are the benefits so the administrators understand the enterprise scope of NCID and its impact.



What is the Enterprise Identity Management Program (NCID)?

The strategy of employing processes and technologies to manage information about the identity of users and control access to an organization's resources.

Includes:

- *Who is allowed in? (Authentication)*
- *What are they allowed to do? (Authorization)*
- *How are moves, adds and changes handled? (Identity Management)*

NCID provides a shared enterprise infrastructure that provides identity management, provisioning, authentication, logging and authorization.

The North Carolina Identity Service (**NCID**) provides an environment by which users can login and gain access to the applications they have been granted rights to use.

The NCID Service is the standard identity management and access service provided to state, local, business and citizen users by the Office of Information Technology Services. NCID enables its customers to achieve an elevated degree of security and access control to real-time resources such as customer based applications and information retrieval. Enterprise features of the NCID Service provide for an efficient and effective means for securing access to online services.

➤ **Authentication** is the act of a user providing credentials such as a user id and password in order for the system to verify that they are who they say they are.

➤ **Authorization** is a process that occurs automatically and determines what a user can access. It is often referred to as access control.



Why do it?

- Identity is an asset
- Most State agencies still manage digital identity on a per-application basis
- Identity can provide the advantages of security, regulatory compliance, risk and liability management, and other core business functions
- Identity must become persistent across business process, spanning not just multiple applications but also multiple organizations both inside and outside.

The state views identity as an asset and therefore that asset should be protected and handled appropriately throughout its lifecycle. That identity should only be given access to applications required to perform the given roles and responsibilities. Agencies in the past have built security solutions for individual applications, typically without any background in security. Result is varying security policies, potential non-compliance with regulations and/or best practice and therefore a higher risk of exposure.

Identities need to be persistent across business processes and organizations to minimize management of those identities. Key benefits of the NCID service is the positive impact of delegated authority and self management.

Delegated authority allows for the management of Ids at a “local” level ensuring better control and management of access. That identity can be given access to multiple applications.




NCID Benefits

- Reduces TCO and simplifies administration through task automation
- Provides a single view of the user
- Improves security through better policy enforcement
- Improves collaboration with internal and external entities

Total cost of ownership is reduced since now application owners are not having to build their own Identity and coarse grain authorization capabilities. Furthermore, that one single user can be given access to multiple applications within and across organizations. Instead of varying degrees of security, we have the capability to enforce a standard, best practice security policy across the state applications. By having a single view of the user and enabling him/her to access multiple applications using one userid/password combination, we improve the ability to effectively conduct business with the state and leverage our services.

Self management allows the ID holder to self register, reset password and manage their profile.

Provides one single view of that user



Risks and Costs Of Not Managing ID's

- **Lower productivity**
 - Avg. time to complete user provisioning request is 6 to 29 hours!
(1)
- **Duplicate and conflicting user information**
 - On average, internal user information is stored in 22 different identity stores and external user data is stored in 6 different identity data stores (2)
- **Security vulnerabilities**
- **Difficulty in meeting regulatory compliance**

1 & 2 Gartner research conducted on companies with over \$500 million in annual revenue

Increase in time to provision and de-provision a user. Multiple support organizations for identity management.

No trusted source for identities – multiple sources of user information.

Varying security policies resulting in varying degrees of risk associated with those identities. Increased management required for the multitude of Ids and therefore risk of Ids not being terminated appropriately.

Agencies are required to meet many security regulations and requirements such as Common Criteria and HIPAA. Ability to change application security frameworks to meet change regulations and requirements can be a massive effort. Having a centralized system and the flexibility to change policies enables agencies to more readily and easily meet regulations via a secure access control enterprise infrastructure.



NCID Capabilities

- Automated provisioning of new users
- User self-service functions (e.g. password reset)
- Workflow processes for approving account creation, modification, and assignment to specific roles
- Removing accounts when they no longer require access
- Coarse-grained, role-based authorization
- Supports multiple user types (state, local, business and individual)

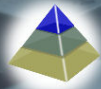
Note: Only state employee user types work with BEACON. If user has state employee NCID, he/she can use that NCID to authenticate with BEACON. User does not have to register to obtain another state employee NCID.

State and local user types require approvals, which leverages the delegated administration model to spread the support costs as well as enable appropriate vetting of users. Individual and business user accounts do not.

Self-service functions (password reset, forgot userid, profile changes)

Removing accounts – by deactivating a user say within ITS, that user's access to email, the Intranet, Remedy, Documentum, VPN, eBilling, CSBilling, BEACON and NCID are immediately removed.

At this point in time, NCID offers coars-grained authorization, meaning if your credentials are verified, you are able to gain access to that application. What a user can do within the application is governed by the role-based authorization



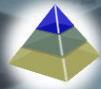
Delineation of Responsibility

- **ITS CSD**
 - Ability to unlock any account
 - Password resets only performed for ITS employees
 - NCID incidents should be reported to the ITS CSD
- **ITS NCID Team**
 - Handles NCID system incidents
 - Handles development of fixes for problems
 - Sets up initial organization/agency and promotes users to administrators where applicable

In talking points

-Examples of provisioning

-Talk to self service functions



Delineation of Responsibility

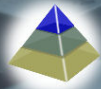
- Agency Service Desks
 - Ability to unlock accounts and reset passwords or act as first point of contact for password reset by agency administrators
 - Ability to unlock accounts and reset passwords for their agencies include: DHHS, DOC, DOJ, DOR, DOT, ESC, ITS, Judicial Branch, NCDA, OSC *
 - Agencies that have requested all agency NCID requests to go through their Service Desks: Judicial Branch/AOC, DCC, DCR, DJJDP, DHHS, DOJ, DOR, DOT, ESC, and NCSHP
(<http://www.its.state.nc.us/Support/CustomerSupportCenter/CSCInternet/Default.asp>)

** Agencies can request ability to centralize unlocks/password resets at their Service Desks. Send request to ITS.Incidents@ncmail.net
The request must come from an Agency Administrator.*

In talking points

-Examples of provisioning

-Talk to self service functions



Delegated Administration

NCID Delegated Administration includes the following responsibilities:

- Verify and approve accounts
- Unlock accounts
- Reset passwords
- Modify account information
- Move accounts (within the agency)
- Deactivate and archive accounts

To perform any of these administrator functions requires an administrator to log into the NCID system.



Delegated Administration

The NCID Service is designed with a **delegated administrator** model. The purpose of this model is to delegate responsibility of NCID user administration to the organizations.

The NCID user administration responsibility can be further delegated as needed down to 3 levels of administration within an organization. Examples are noted below.

- Organization (DHHS)
- Division (Division of Public Health)
- Section (Immunization Registry)
- Organization (DHHS)
- Division (Division of Social Services)
- Section (Child Support Enforcement)
- Organization (Department of Correction)
- Division (Division of Prisons)
- Section (Facility Number 3020 - FCCW)
- Organization (Department of Environment and Natural Resources)
- Division (Soil and Water Conservation)
- Section None

An NCID administrator will have rights to perform functions within their level in the organization. For instance, a division administrator will be able to perform functions in both the division and any sections within the division. However, a section administrator will only be able to perform functions in just their section(s).

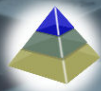
The administrator approving the account must be in a position to vet the individual.



Levels of Administration

Agency administrators can perform actions for any user in their organization regardless of the division the user is in. This level of administrator can do the following for users associated to the organization:

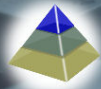
- Promote/demote others to/from organizational administrator
- Promote/demote users to/from division administrators
- Promote/demote users to/from section administrators
- Deactivate users
- Change selected information about users
- **Unlock user accounts**
- **Reset passwords**
- Reactivate accounts that have been deactivated
- Archive deactivated accounts
- Change selected information about organization and division records



Levels of Administration

Division administrators can perform actions for any user in division(s) that administrators have administrative rights for. This level of administrator can do the following for users associated to the same division(s):

- **Receive and process new user account request (registration approvals)**
- Promote/demote users to/from section administrator (if used)
- Deactivate users
- Change selected information about users
- **Unlock user accounts**
- **Reset passwords**
- Reactivate accounts that have been deactivated
- Archive deactivated accounts



Levels of Administration

Section administrators can perform the following actions for any user that they have administrative rights for that section. This level of administrator can do the following for users associated to the same section(s):

- **Receive and process new user account request (registration approvals)**
- Deactivate users
- Change selected information about users
- **Unlock user accounts**
- **Reset passwords**



Tips

- **Searching**
 - Use equals (“=”) or “begins with” or “ends with”
 - User results are returned faster when entering user ID an using the operand equals (“=“)
 - Avoid use of “That Contains” search option
- **Approvals**
 - Email link for approvals faster response than searching for approvals
 - If user ID has a numeric at the end, the user may already have an NCID. Administrator should verify existence of NCID prior to approval.
- **Password resets**
 - To reset a password, you first must **Search** and **Select** the user to modify. Enter the **Modify** mode. Once in modify mode, click on the **Account Info** panel to display NCID Reset Password Screen.
- **User-related**
 - Remind user not to bookmark NCID login page
 - Administrators can change last name
 - Transfer process: user must be deactivated/archived and then re-register and associate himself/herself with new agency/division/section



High Priority Issues

- **Search and report performance**
 - Oracle is investigating root cause
 - Tips to improve search performance
- **Deactivation and archive performance**
 - Oracle investigating root cause for degraded performance
 - Oracle investigating why all deactivated users are not showing in deactivation search results
- **Password reset performance**
- **Transfers**
- **Stability of platform**
 - Oracle has identified a fix for Identity services' issue
 - Oracle has identified a fix for Access services' issue

Page should be replaced with service strategy w/talking points for details.



Recent Changes

- **Oracle Platform:**
 - Updated password policy for user types
 - Updated registration confirmation
 - Employee ID (BEACON #) shown in NCID account profile
- **Web Site Changes**
 - ITS CSD added agency service desk information for password resets
 - Text changes to registration and password help screens
- **ORBiT postponed from NCID**
 - Reduce impact to agency service desks during BEACON Wave 2 rollout
 - Reduce impact to NCID to allow for stability and performance efforts to be completed

Page should be replaced with service strategy w/talking points for details.



Planned Changes

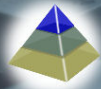
- **Stability and performance**
 - Oracle has identified a fix for Identity services' issue
 - Oracle has identified a fix for Access services' issue
 - Performance changes as identified from vendor
- **NCID Self-Service**
 - Failed login change (3 and go to forgot password)
 - Password expiration notification update (14 days prior to expiration and daily thereafter)
 - Implement usability requests

Page should be replaced with service strategy w/talking points for details.



Strategic Changes

- **Next version of NCID**
 - Minimize customization
 - Improve integration processes with NCID
 - Push unlocks and password resets out to user
- **BEACON as trusted source**



Portal Troubleshooting Guide

- **Portal Login Issues**
 - User Authentication Failed (EP101, EP 102, EP201)
 - NCID Account Locked
 - NCID Password Expired
 - 404 Page Not Found Error
- **SAP Activation**
 - SAP Activation Notification
 - Activation Failure
 - Activation Failure – Employee Record not Found
 - Activation Failure – Employee Record Inuse By Another NCID
- **SAP GUI**
 - Invalid Login on SAPGUI
 - Load Balancing Error
 - SAP GUI Font Change
- **ESS / MSS**
 - Page not found or not available
 - Service is Locked Error
 - Critical error – User has No RFC Authorization Error
- **Log Out**
 - Log Out Error



Information

NCID Information Website: <https://www.ncid.its.state.nc.us>

NCID Administrators Guide:

https://www.ncid.its.state.nc.us/NCID_Training_Materials.asp

NCID Login and Self Registration Page: <https://ncid.nc.gov>

ITS Customer Service Desk:

Email: its.incidents@ncmail.net

Phone: 800-722-3946 or 919-754-6000

BEST (BEACON Enterprise Support Team) <http://www.ncosc.net/BEST/>

Email: BEST@ncosc.net

Phone: 866-NCBEST4U (866-622-3784)

ORBiT

Retirees/Benefit Recipients call 1-877-733-4191 (733-4191 within local Raleigh calling distance)

Active Members call 1-877-627-3287 (627-3287 within local Raleigh calling distance)



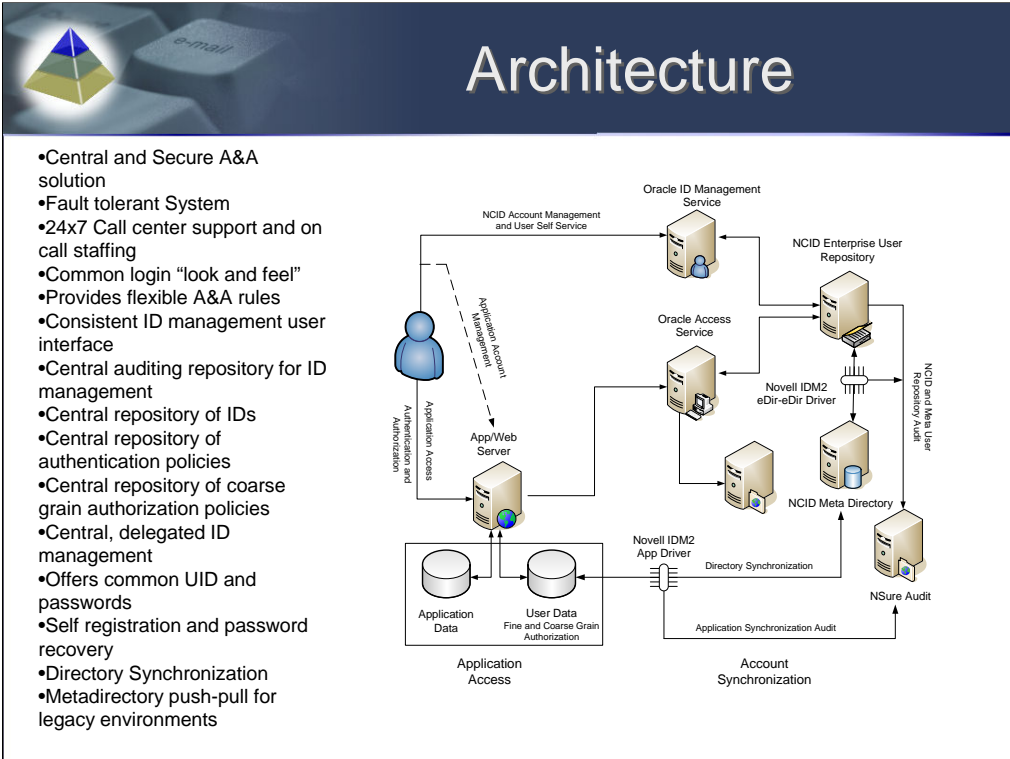
Questions

Questions?



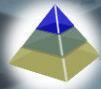
Backup Slides





- Central and Secure A&A solution
- Fault tolerant System
- 24x7 Call center support and on call staffing
- Common login “look and feel”
- Provides flexible A&A rules
- Consistent ID management user interface
- Central auditing repository for ID management
- Central repository of IDs
- Central repository of authentication policies
- Central repository of coarse grain authorization policies
- Central, delegated ID management
- Offers common UID and passwords
- Self registration and password recovery
- Directory Synchronization
- Metadirectory push-pull for legacy environments

Remove



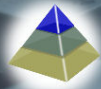
Process New User Requests

All division and section NCID administrators will receive notice via email when someone has requested an NCID account for their given division or section.

1. Open the email message
2. Click on the link in the body of the email message to process the request. You will be requested to authenticate to the NCID system if there is not an active session in NCID.
3. Login to NCID.
4. Click on Continue button.
5. Click on the Process button. This will take you to the NCID Process Ticket Information Screen.

Also, the NCID console can search for all requests which are pending for you to process, up to 35 days ago.

Refer to the NCID Administrator's Guide for additional information.



Unlocking a User Account

When a user attempts to access a protected application and fails a certain number of times in a row, the user's account will be locked. Currently NCID is configured to auto-unlock accounts after 24 hours from when it was locked.

The user's NCID administrator may unlock the account immediately.

For an administrator to unlock an account, he/she must follow these steps:

1. Perform a **Search** and **Select** the user to modify.
2. Click on **Modify**.
3. Once you are on the user's profile page, click on the **Account Info** panel. If the account is locked it will be shown on the screen with an unlock date and count.
4. If account is locked, click on **Request to Modify** next to "Unlock Account."
5. Click **Save**.
6. The user's account will now be unlocked.



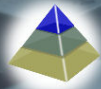
Password Resets

When a user needs to have their password reset and they can not login to perform this action themselves there are two options:

- Have the user try the “Forgot Your Password?” link on the login page. The user will be required to answer three (3) of their challenge questions correctly.
- A delegated administrator resets the password.

If the user is not able to answer the challenge questions correctly, then an administrator will need to reset the user’s password for them. To start this process, you must be an administrator of the user.

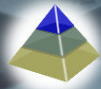
To reset a password, you first must **Search** and **Select** the user to modify. Enter the **Modify** mode. Once in modify mode, click on the **Account Info** panel. Click on the gray “Request to Modify” button then click save. A system generated password will be created; give the user the password. They will be required to change it at the first successful login.



Modifying User Information

To modify a user's profile information, follow these steps:

- Search for user
- Click on name of user to bring up the user's profile
- Once the user's profile is on the screen, click on the gray "Modify" button to start the process of updating information. When the screen refreshes the NCID Modify User Profile Screen will be displayed.



Modifying User Information

An NCID account will contain the following panels of information:

- **Personal Info** - User name, UID, user type, etc.
- **Password Info** - This is where a user can change their own password and challenge questions/answers.
- **Contact Info** - User's phone numbers, address, email address, etc.
- **Account Info** - The status of the account, locked dates, invalid login counts. This is where an administrator would unlock and reset passwords for other users.
- **Employee Info** - User's employment status, manager (if maintained), division, section (if used).
- **Member/Admin Info** - Organization the user belongs to and administrator if applicable in addition to group information.



Moving a User

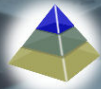
Users that are moving between divisions in the same agency are just a modification to their account. The NCD Administrator's Guide covers this information.

Once a user is no longer associated with your organization, they should be "deactivated". This will prevent them from accessing any NCID protected resources. This will assure that your organization is not allowing unauthorized users to have access to NCID protected systems.

To deactivate a user **Search** for and **Select** the user to deactivate. Follow the process outlined in the administrator's guide.

After a user's account has been deactivated, you should also archive it from the system. This will permanently remove the account from the NCID system.

If the user is transferring to another agency, this will allow them to register at the new agency and, if it still available, obtain the same UID.



Search for Users

To locate an NCID user, you will need to search for them in the system. The Search Menu has several fields to assist you in searching for a user. Keep in mind if there are an extensive number of accounts that match there will be some time delay.

- **User Attribute Dropdown** - Under the first dropdown selection menu, you can select different attributes stored in a user's profile, i.e. address or last name.
- **Type of Match** - Here you select the kind of match you want to perform. You can search on parts of words or numbers greater-than, equal to, etc. Keep in mind that if you select "=" you must supply an exact match.
- **Text to Search For** - In the blank (third) box enter the information you want to search, i.e. "Smith" or "john.smith@ncmail.net".
- The gray **Advanced** button allows you to do multiple attribute searches. This is helpful in reducing the number of "hits" where a single attribute search would result in a very long list.

Once you find the user profile you want to see, click on the user's name in the first column. This link will access the user's complete profile information.



Deactivating a User

Once a user is no longer associated with your organization, they should be “deactivated”. This will prevent them from accessing any NCID protected resources. This will assure that your organization is not allowing unauthorized users to have access to NCID protected systems.

To deactivate a user **Search** for and **Select** the user to deactivate.

To deactivate a user **Search** for and **Select** the user to deactivate.
Follow the process outlined in the administrator’s guide.

After a user’s account has been deactivated, you should also archive it from the system. This will permanently remove the account from the NCID system. The archive process is detailed in the NCID Administrator’s Guide.