SECURITY & USER ADMINISTRATION

- Niagara Site Security
- Best Practices
- Niagara Security Help
- Niagara Central – Security Central
Best Practices

- Change Default Platform Credentials
- Strong Passwords
- Account Lockout
- Password Expiration / History
- Individual Account for Each User
- Admin User Should be Rarely Used
- Guest User Should Remain Disabled
- SSL (Crypto / Cert Mgr)
- Secure Communications (VPN / RSAID)
Best Practices

- Change Default Platform Credentials
- Strong Passwords
- Account Lockout
- Password Expiration / History
- Individual Account for Each User
- Admin User Should be Rarely Used
- Guest User Should Remain Disabled
- SSL (Crypto / Cert Mgr)
- Secure Communications (VPN / RSAID)
Platform Credentials
Best Practices

- Change Default Platform Credentials
- Strong Passwords
- Account Lockout
- Password Expiration / History
- Individual Account for Each User
- Admin User Should be Rarely Used
- Guest User Remains Disabled
- SSL (Crypto / Cert Mgr)
- Secure Communications (VPN / RSAID)
What is a Strong Password in Niagara?

- Minimum of 8 characters
- Mix of letters, numbers, and symbols
- Cannot be all letters or all numbers
Strong Passwords

➢ Required by Default
Account Lockout

- Enabled by Default
- Lockout Period
  - Enter Wrong Password
  - 5 Times
  - Within a 30 second Period
  - Locked out for 10 seconds *

* You Really Need To Think About The Lockout Period!
Password Expiration

- 90-day expiration is common
- 15-day warning is common
- History length limits reuse of recent passwords
Password Expiration
Best Practices

- Change Default Platform Credentials
- Strong Passwords
- Account Lockout
- Password Expiration / History
- Individual Account for Each User
  - Admin User Should be Rarely Used
  - Guest User Remains Disabled
  - SSL (Crypto / Cert Mgr)
  - Secure Communications (VPN / RSAID)
Individual Credentials
Security Model

1. Create control logic with OBJECTS
2. Assign OBJECTS to CATEGORIES
3. Create needed CATEGORIES
4. Assign appropriate PERMISSIONS to each USER

Create PASSWORDS

WHO can access station?
WHO can access categories?
WHAT can be accessed?
WHAT can be done?

Objects: Components, Files, Histories

Users

Permissions

Categories

USER MGR

CAT BROWSER

Tridium, Inc. Copyright © 2013
Structuring categories starts when you begin to engineer the station. When you’re engineering the station, think about how the station is organized:

- **Categorize the containers & objects**
- **Map the function of each object to the types of operators that need access to it**
When adding new users, think about the person's job requirements. Do they need to:

- **View** Station information/status?
- **Revise/edit** Station information?
- **Control** equipment?
- **Silence** alarms?
Permissions define the **rights** that users have within each Category of the station, which are also mapped to specific objects.
OBJECTS
- Create in CatMan
- Assign in CatBrowz
- Lighting
- General
- USERS
  - Create in UserMan
  - Category Manager
  - Category Browser
  - User Manager
  - Permissions Browser

CATEGORIES
- Create in CatMan
- Assign in CatBrowz
- HVAC
- Lighting
- Categories Permissions
- Role-based or System-based
- Defines rights in each category – operations allowed on each object
- Think about job requirements and access requirements

PERMISSIONS
- Assign in UserMan or PermBrowz
- Operator
  - READ
  - WRITE
  - INVOKE
- Admin
  - READ
  - WRITE
  - INVOKE

USERS
- Role-based or System-based
- Joe
- Bob
- Sally
- George
- Manuel

Tridium, Inc. Copyright © 2013
### Category Browser

Category Service

Objects mapped to Categories

<table>
<thead>
<tr>
<th>Category Service</th>
<th>Objects mapped to Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherit</td>
<td>User</td>
</tr>
<tr>
<td>Config</td>
<td><img src="image1.png" alt="Icon" /></td>
</tr>
<tr>
<td>Services</td>
<td><img src="image8.png" alt="Icon" /></td>
</tr>
<tr>
<td>UserService</td>
<td><img src="image15.png" alt="Icon" /></td>
</tr>
<tr>
<td>CategoryService</td>
<td><img src="image22.png" alt="Icon" /></td>
</tr>
<tr>
<td>JobService</td>
<td><img src="image29.png" alt="Icon" /></td>
</tr>
<tr>
<td>AlarmService</td>
<td><img src="image36.png" alt="Icon" /></td>
</tr>
<tr>
<td>HistoryService</td>
<td><img src="image43.png" alt="Icon" /></td>
</tr>
<tr>
<td>AuditHistory</td>
<td><img src="image50.png" alt="Icon" /></td>
</tr>
<tr>
<td>LogHistory</td>
<td><img src="image57.png" alt="Icon" /></td>
</tr>
<tr>
<td>ProgramService</td>
<td><img src="image64.png" alt="Icon" /></td>
</tr>
<tr>
<td>BackupService</td>
<td><img src="image71.png" alt="Icon" /></td>
</tr>
<tr>
<td>WebService</td>
<td><img src="image78.png" alt="Icon" /></td>
</tr>
<tr>
<td>PlatformServices</td>
<td><img src="image85.png" alt="Icon" /></td>
</tr>
<tr>
<td>Drivers</td>
<td><img src="image92.png" alt="Icon" /></td>
</tr>
<tr>
<td>NiagaraNetwork</td>
<td><img src="image99.png" alt="Icon" /></td>
</tr>
<tr>
<td>NdioNetwork</td>
<td><img src="image106.png" alt="Icon" /></td>
</tr>
<tr>
<td>Cafeteria</td>
<td><img src="image113.png" alt="Icon" /></td>
</tr>
<tr>
<td>Calendars</td>
<td><img src="image120.png" alt="Icon" /></td>
</tr>
<tr>
<td>Files</td>
<td><img src="image127.png" alt="Icon" /></td>
</tr>
<tr>
<td>History</td>
<td><img src="image134.png" alt="Icon" /></td>
</tr>
</tbody>
</table>

**Maps components, files and services to specific role- or system-based security categories**

**Can assign an object/folder to multiple categories**

**DIMMED** = object inherits parent’s category(ies)

**YELLOW** = categories are discretely assigned

To see objects mapped to Permissions

---

Tridium, Inc. Copyright © 2013
Permissions Dialog

For a specific user, map permission level (O or A) and permissions (R, W, I) to each Category.

User Service
- User Manager
- Edit dialog

To see permissions mapped to Objects.
### Permissions Browser

**User Service**
- Provides a quick view to see user permissions mapped to objects

**OBJECTS**
- Objects mapped to Permissions

#### Permissions mapped to Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Operator</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>R W 1</td>
<td>R W 1</td>
</tr>
<tr>
<td>Admin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>General</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HVAC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lighting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User/Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PlatformServices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NiagaraNetwork</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NiloNetwork</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cofactria</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calendars</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>History</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Double-click anywhere on a User column to see their Permissions Dialog

To see objects mapped to Categories

---

*Tridium, Inc. Copyright © 2013*
User Profile

- Account
- Expiration
- Permissions
- Passwords
- Auto Logoff
- Web Profile
- Nav File
Other Miscellaneous Security Features

Files Hidden / Blacklisted from Station files
- .bog not visible via Fox or Web
- You can Blacklist other file types / folders
  - Edit system.properties (see help)

Logon Dialog
- “Remember These Credentials” is unchecked

SuperUser Credentials Required
- Adding or Editing Program Objects
Best Practices

- Change Default Platform Credentials
- Strong Passwords
- Account Lockout
- Password Expiration / History
- Individual Account for Each User
- Admin User Should be Rarely Used
- Guest User Remains Disabled
- SSL (Crypto / Cert Mgr)
- Secure Communications (VPN / RSAID)
Secure Socket Layer

V3.7 and later:
- SSL is “Built In”
- SSL is part of Platform functionality
- Allows for secure Platform connections and station connections (FoxS and Web)

V3.6 and earlier:
- Crypto is an “Add On” and requires a license feature.
- The Crypto service is part of the Station
- Allows ONLY for a secure Web connection
Prerequisites for use of SSL

Niagara Platform must support Hot Spot VM
  ➢ Hint: JACEs 2, 4, & 5 still use IBM J9 VM

NiagaraAX V3.7 or later

Install Modules
  ➢ cryptoCore
  ➢ daemonCrypto
  ➢ platCrypto
Default Ports

Workbench Connection to a Platform

- Non-Secure: HTTP Port 3011
- Secure: HTTPS Port 5011 (Platform Admin)

Workbench Connection to a Station

- Non-Secure: Fox Port 1911
- Secure: Foxs Port 4911 (Fox Service)

Browser Connection to a Station

- Non-Secure: HTTP Port 80
- Secure: HTTPS Port 443 (Web Service)
Best Practices

- Change Default Platform Credentials
- Strong Passwords
- Account Lockout
- Password Expiration / History
- Individual Account for Each User
- Admin User Should be Rarely Used
- Guest User Should Remain Disabled
- SSL (Crypto / Cert Mgr)
- Secure Communications (VPN / RSAID)
Niagara Security Information

- Help System
  - docUser
  - docSSL
  - docPlatform
  - doc2013SecurityUpdates
- Niagara Hardening Guide
- Niagara Central – Security Central
Stay Informed To Keep Your Niagara System Protected

As your partner for automation infrastructure and technology, Tridium takes threats to the security of your systems very seriously. We are committed to providing our customers access to industry standard network security information needed to be better prepared for possible cyber intrusions. Based on a documented increase in cyber attacks on unprotected networks, Tridium recommends you take the following actions to help protect your systems, data and networked devices:

**STEP 1:** Install All Patches & Software Updates

**STEP 2:** Configure Your System For Optimal Security

**STEP 3:** Add Additional Layers Of Security

**STEP 4:** Stay Informed
Q & A

Please use the Chat function in WebEx and send your questions to Phil Stuckemeyer