NSC Management Cloud

User Guide (Draft 10/21/2019)

Welcome to the NSC Management Cloud

(codename: Stratus)

We are excited to introduce you to the evolution of the intelligent home management. This entirely new platform will provide you with **full visibility** over all of your intelligent home deployments and provide **full control** of every element from anywhere in the world from a single management point so you can proactively **delight your customers**. As it evolves, starting this year, it will integrate with other products and platforms in the **Nortek Security & Control** portfolio to help you expand your business with that same simple, yet elegant flexibility you've come to know from ELAN.

Initial deployment is exclusive to ELAN Elite Dealers and Distributers so we can get vital and timely feedback on our direction and to inform product roadmap decisions. But our goal is not to merely test ideas and implementations, but more so, to empower you with every release. To make it easier for you to manage your customers but also to make it easier for you to do business with NSC.

Thank you in advance for your participation in this program!

The Management Cloud Team

Table of Contents

Note: Controllers must be running <u>ELAN core release 8.3.11 or later</u> when adding as a Location in Management Cloud. The ***Quick Connect*** function in Management Cloud is not dependent on Core Release versions.

Management Cloud is by Nortek Security & Control | © 2018 Nortek Security & Control

The Application

(Stratus) Management Cloud, in its first implementation, is a Windows application. Scanning and connecting to controller on a local network without internet access is a feature requirement best delivered through an application. Further, we continue to utilize Configurator as the local & remote configuration utility, which is a currently Windows-based application launched from the Management Cloud experience. Installers using the Windows-based application gTools and its variants should be able to seamlessly transition over to using Management Cloud. *Windows 10 is required.*

Login Screen

Use your current email and password to log into Management Cloud.

Note: Dealer Accounts are created using the Management Cloud Application Form and subject to approval. Once Dealer accounts are created, and owner can invite users to add an account. Accounts cannot be created without invitations, therefor "Create Account" function is not available on the login screen.
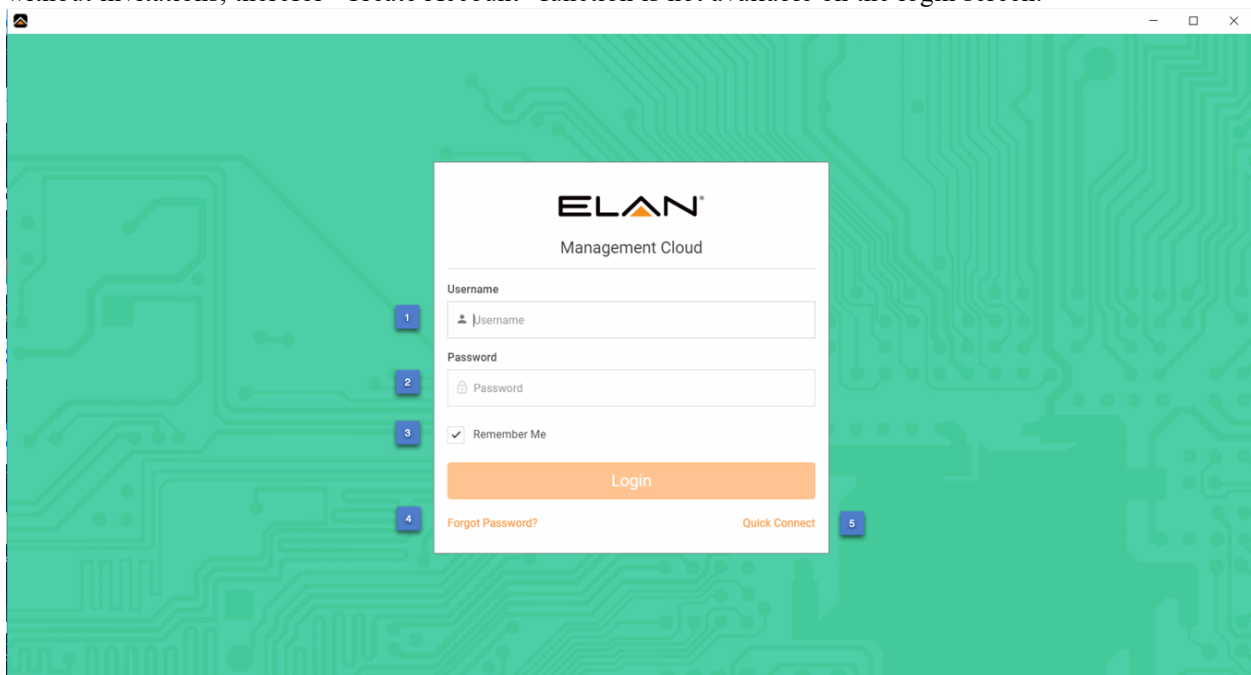
1. **Username**: Email registered with Management Cloud
2. **Password**: Associated with your username registered with Management Cloud
3. **Remember Me**: Checkbox will remember the username, but security purposes, passwords are not remembered.
4. **Forgot Password**: Initiates password reset flow by entering registered username.
5. **Quick Connect**: Links to the *unauthenticated* version Quick Connect, not requiring one to log into Management Cloud account to use.

Application Tabs

All locations area lists all the locations that [current user] has permissions to view and access.
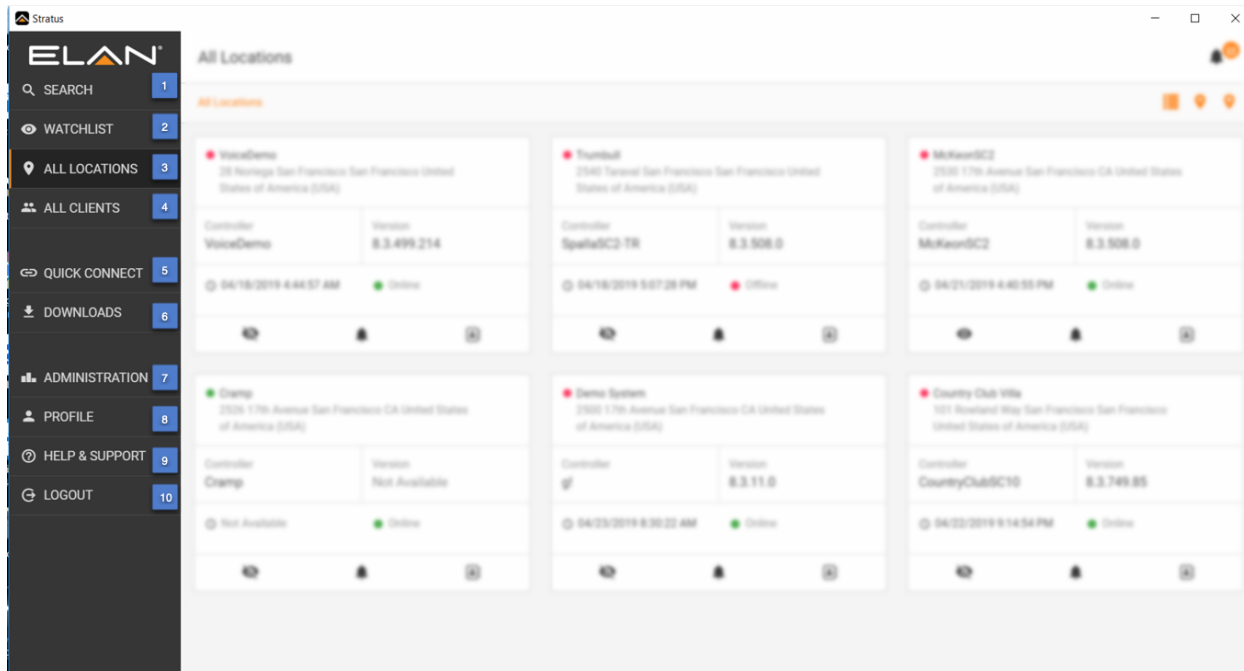
Application, Tabs

1. **Search**: Search across all repositories including location, client, controller details [including attached gear, drivers], help & support docs. Example: Search "Sonos" will find all Controller with Sonos (device/driver) attached.
2. **Watchlist**: This is a means for current user to separate select locations from "all locations" list. Can be used to quickly see and access your key locations. Alert weighting and Service Level Agreement (SLA) will be accessible for watchlist locations in near future.
3. **All Locations:** All the locations visible to current user. Depending on one's User Role for company you may see all or just some of the locations registered.
4. **All Clients:** All the clients and client contacts visible to current user. Depending on one's User Role for company you may see all or just some of the locations registered.
5. **Quick Connect:** This is tool similar to launcher in gTools to allow you to scan a network or enter controller details and launch into Configurator or Viewer. Enhancements including saving passwords with controller, add controller as a location.
6. **Downloads:** Core release and other downloads, release notes, integration notes, and (Stratus) download update functionality. This information will be indexed for search.
7. **Administration:** This is area where Role: Owner and Role: Team Lead can manage users & groups, and soon, analytics & reporting, subscriptions and shopping cart details for the company.
8. **Profile:** This is where current user can manage their details, including password reset and alerts and notification management.
9. **Help & Support:** FAQs, Video Notes, Support Resource links and contact options.
10. **Logout:** Logs one out of their account and showing login screen.

Search

Search across all repositories including location, client, controller details [including attached gear, drivers], help & support docs. Example: Search "Sonos" will find all Controller with Sonos (device/driver) attached.

Watchlist

A Watchlist is a way to separate specific locations from other locations for currently logged in user. In the case where you want to pay special attention to a site or just a means to quickly accessed commonly accessed site, add it to your watchlist. In later iterations of the platform, SLA rules will be optionally applied on a Watchlist basis.

All Locations

All locations area lists all the locations that [current user] has permissions to view and access.

All Locations, Location Card View

1. All locations area lists all the locations that [current user] has permissions to view and access
2. Location card with Location Name, Location Address, Controller Name, Controller Firmware Version, Last Update of controller firmware, controller online/offline status
3. Watchlist toggle to add/remove locations from watchlist
4. Alerts Mute will disable all alerts at a location level for a temporary basis. Saves one from having to disable individual alerts on a location when performing work that may trigger alerts.
5. Quick contact option for Client/Client Contact associated with the location
6. Alerts & Notification Menu
7. All Location List View/Card View toggle
8. All Location Map View
9. Add a Location

All Locations, List View

All Locations, Map View

Locations

A location, in the ELAN sense, is a one-to-one mapping with a master controller in this iteration of Management Cloud. All of a controller's attached devices, nodes, extenders and configuration will be brought in automatically when a location is created, and a standard set of alerts will be autoconfigured. It is generally suggested that a controller be configured as desired before adding as a location but note that most changes to *configuration* on the controller will be reflected in the Location in your cloud account within 5 minutes of the change made. Status, Alerts, Connected Devices and other select data is pulled directly from the controller in real-time and not subject to a configuration update delay.

Cloud Authentication & Permissions Layer

One of the more important and powerful functions Management Cloud brings the dealer is an authentication workflow that builds off of the current user concept on the controller but extends it to be more flexible and more secure.

- When a location is created, a special user account is created on the controller using the dealers' company name and contact details set when creating your cloud account. This helps inform the end user who has access to their controller, contact details etc., and gives them the ability to adjust the level of access or remove access completely.
- With this special user account there is also an encrypted and obfuscated password created for that account used just for a handshake between controller and Management Cloud. A simple click on "Configurator" or "Viewer" buttons on a location in Management Cloud will launch the respective app, authenticate automatically for the controller linked to the location. That makes Management Cloud login a new path and gate to access controllers.
- Permission to access a location via Management Cloud must be granted and/or revoked by dealer and tech lead roles. If an employee leaves the company, their Management Cloud account can be shut down and access to those locations removed. Employees, even the owners and tech leads themselves, do not have access to the password used for the dealer account so some risk is mitigated.
- A controller's Admin password, used to authenticate a location in Management Cloud, must still be changed post-installation, per training guidance. Use of the Management Cloud account management layer eliminates the need to a dealer to retain listing of the default admin passwords for all controllers once they are added as locations in Management Cloud.

Controller Tab

Navigating into a Location card with a click/tap will reveal options for managing a location as well as list devices assigned to a location
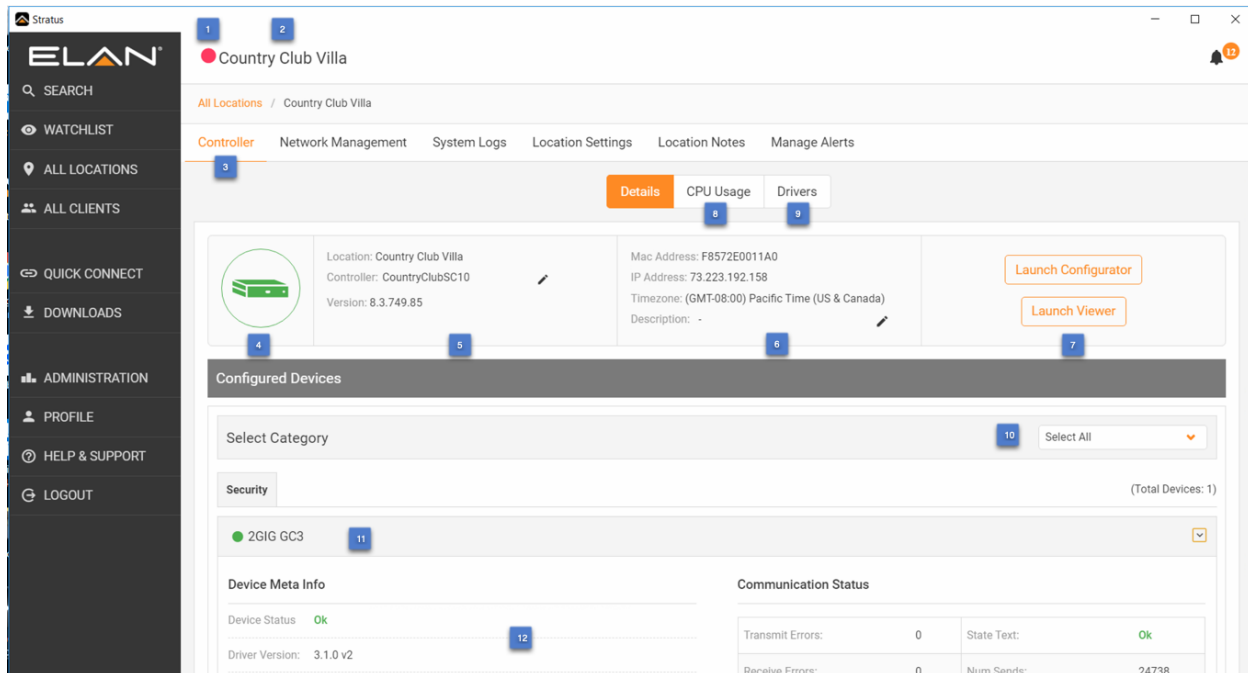
[Location], Controller Details View

1. Current Location Health Status Indicator
2. Location Name
3. Default tab for Location is Controller tab
4. Controller Network Status. Color and mouseover denote current status.
5. Controller details including location name, controller name and core software version
6. Controller details including controller MAC address, IP address, Time Zone (selected when adding a location) and an editable Description field, for quick notes about a location.
7. Launch Configurator and Launch Viewer buttons for a location. Note that access to these buttons are based on one's role and location permissions.
8. Access to controller real-time CPU, memory and I/O information
9. Drivers installed on controller, *indexed for Search*
10. Configured Devices subcategory pulldown for quick access and filtering.
11. Device Name and Status Indictor
12. Device details including status string, driver version, IP address, communication status
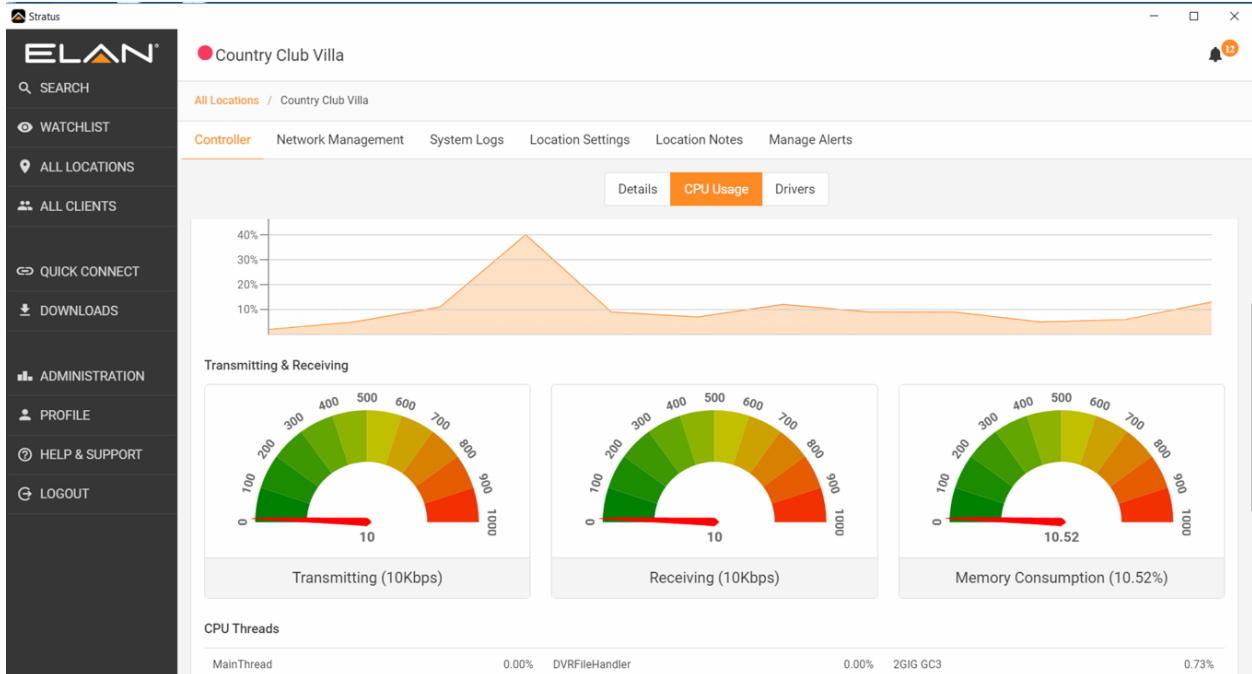
[Location], Controller CPU Usage View

[Location], Controller Drivers View

Network Management Tab

Current implementation pulls network data from your controller's Discovery tab. <u>If Discovery is not enabled on your controller you will not see information in this tab.</u> This data is pulled in for Search indexing purposes

but will soon include functions setting ping alerts for any device on network and host advanced network functionality.

[Location], Network Management Tab

System Logs

This tab pulls the logs (Exceptions, Connections, System) from the controller for convenience. Column width adjustment and sorting available. Search, sort and functions to post logs for Tech Support will be soon.

[Location], System Logs Tab

Location Settings > General Settings

Location Settings tab provides details about a location as well as allow for permissions management.

General Settings allows for viewing editing of location name; time zone; Location Lock, which prevents members from editing important location details; client and client contact details; and **Delete Location** function. Access to view and/or edit this tab is based on your role and current location permissions.

[Location], Location Settings > General Settings

Location Settings > Permission Settings

Location Settings tab provides details about a location as well as allow for permissions management.

Permission Settings controls who on your team has access and the level of access granted. Note that only current user of your company can be added to a location. Permissions can be granted to individual users or to groups.

Permissions & Groups definitions will be handled later in this document.
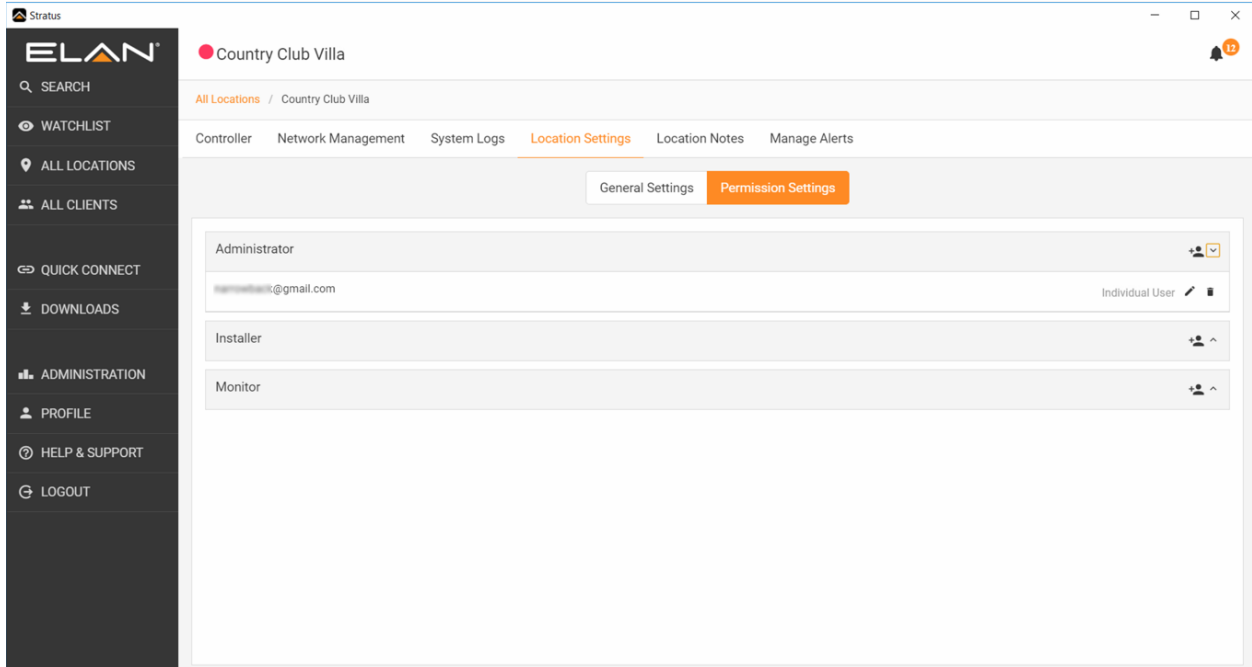
[Location], Location Settings > Permission Settings

Location Notes

Location Notes are a means for users to document time spent on a location. Timestamps, attribution and time tracking functions are visible in the interface and can be soon be accessed in custom reports on the Administration tab.

Note Categories, introduced in 1.0.1, accessed in the Location Notes section of each location, are used to help classify work performed. This will help standardize entries for forthcoming reporting functions.
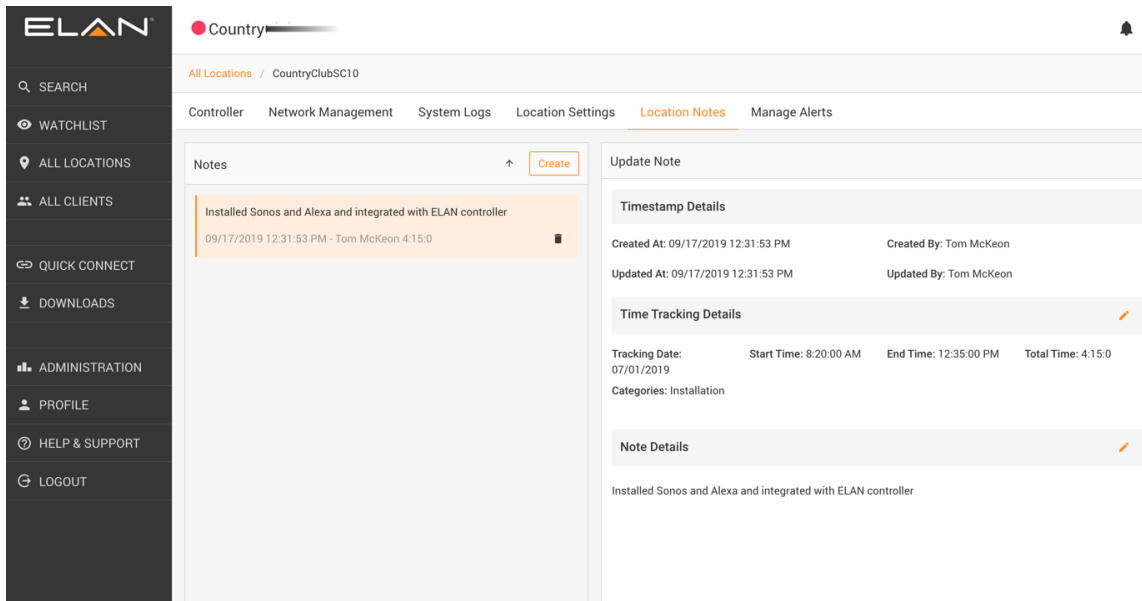
Manage Alerts

Manage Alerts tab shows the alerts available for a location. By default, a location admin (person who adds the location) and an Administrator Group, if assigned at location creation, are automatically assigned to receive alerts on all Configured Devices on a controller. Connected Devices, which show touchpanels et al but also local and remote client connections, can be inherently transient, so alerts are not set here by default. You can however add an alert as needed.

[Location], Manage Alerts

1. **Configured Devices**: alerts are set up automatically for location creator and Administration Groups, if defined.
2. **On State Change:** Alerts are trigged "On State Change" which means when a device moves from one status state to another. As a tip, read it as "On State Change to…" when checking the color. State Change from Green to Yellow and Red are an obvious choice but also a "On State Change to…" Green will let you know when a device has started functioning again, saving you from having to drill into the device details.
   Alerts are coarsely categorized under green, yellow and red which generally translate to:
     a. **Green** – Device/Service functioning normally
     b. **Yellow** – Device/Service may be impaired. Check Status message in device details or alert notification.
     c. **Red** – Device offline or otherwise inaccessible. Check Status message in device details or alert notification.
3. **Alert Mode:** These are the paths for Alerts to take. "In-App" is a push notification accessible in the upper right corner of the application, bell icon. When one Unsubscribes from an alert, as in the Alert In-App menu, the Alert mode is affected and the alert email and "on state change" settings remain intact. This allows one to easily subscribe just as one unsubscribed without needing to navigate to the Manage Alerts tab and recreate the alert.

4. **Delete Recipient:** Deletes user from the alert.
5. **Add Alert Recipient:** Manually add a user to receive alerts for that particular device. Note a user (email) must be part of the current company account to add via this function.
6. **Add Recipient to All:** Adds a user to receive alerts for all Configured Devices for that location. This list (1.0.2) will only show users associated with dealer company. Alert settings (On State Change, Alert Mode, Alert Threshold) will be pulled by a user's "Default Alert Settings" in Profile > Settings.
7. **Connected Devices:** Connected Devices, which show touchpanels et al but also local and remote client connections, can be inherently transient, so alerts are not set here by default. You can manually add an alert to these devices as needed.

All Clients

All the clients and client contacts visible to current user. Depending on one's User Role for company some of the client records may not be visible.

Client is the end user, owner of the controller and its location.

Client Contact allows you to associate different contacts for the same Client, as in the case where a Client has multiple locations, and therefore multiple addresses and client contacts per location
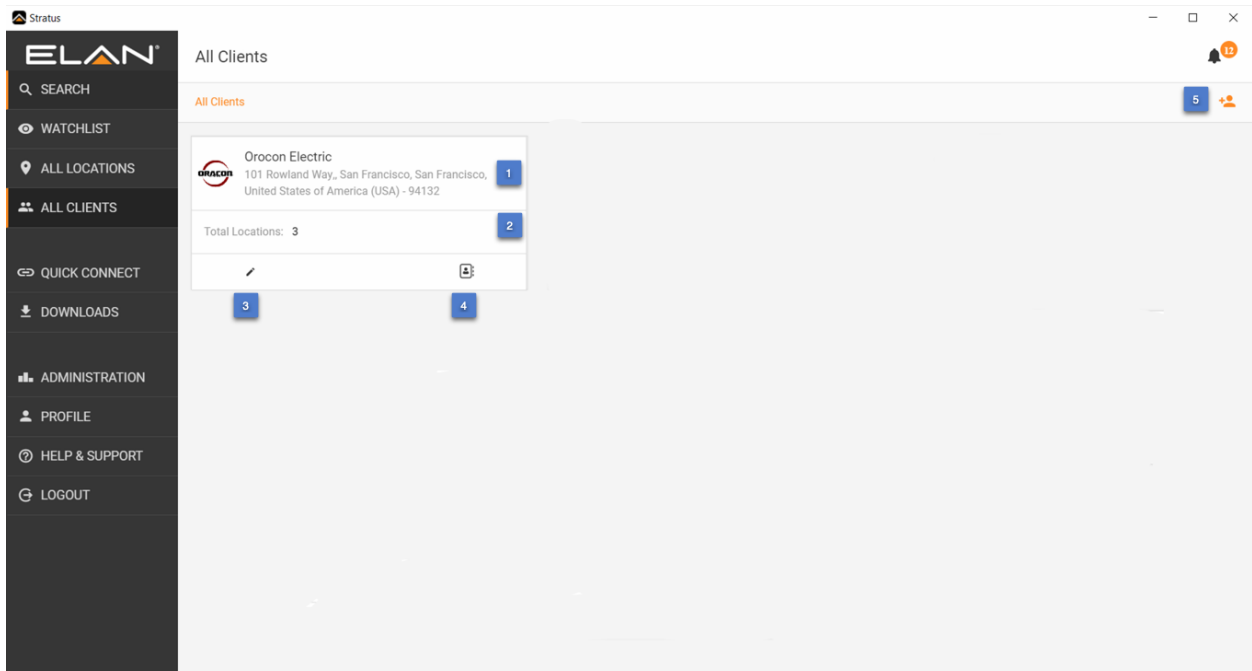
[Location], Location Notes

1. **Client Name, Image and Address**
2. **Total Location Count:** Number if location associated with this client
3. **Edit:** Edit the client records, based on permissions
4. **Show Contact Info:** Quick means to get main contact information
5. **Create Client:**

Quick Connect

This is function similar to launcher in gTools to allow you to scan a network or enter controller details and launch into Configurator or Viewer. Enhancement to Quick Connect method include saving passwords with controller, add controller as a location.

There are two levels of Quick Connect in the Management Cloud application:

- *Authenticated:* This is the instance of Quick Connect available in application once you have logged into your account.
  - o **Features:**
    - ▪ Scan and connect to local controllers
      - IP/ configuration coming soon.
    - ▪ Manually enter Controller name and Password to connect with Configurator and Viewer.
    - ▪ Save Controller, with or without password, to list of saved controllers. Because this data is stored in the cloud, it is accessible from any client that logs into this account.
    - ▪ If a controller is not already a location, you will see an "add" button in the Action column of you saved controller list. A click on that will start the "Create a Location" process.
    - ▪ If a controller is already associated with a location on your account, you will see a "View" button in the Action column of you saved controller list. A click on that will take you to the controller tab for that location.
- *Unauthenticated:* This is the instance of Quick Connect available via link on login screen when you do not log into an account. This can be used when internet access is not available, but you need to find and access a controller on the LAN.
  - o **Features:**
    - ▪ Scan and connect to local controllers
      - IP/ configuration coming soon.
    - ▪ Manually enter Controller name and Password to connect with Configurator and Viewer.
    - ▪ Note that one cannot save controllers in unauthenticated mode. This mode is intended to cover use case of no internet access. In all other cases, logging into the Management Cloud is recommended.

Saved Controllers
Available in Authenticated mode only
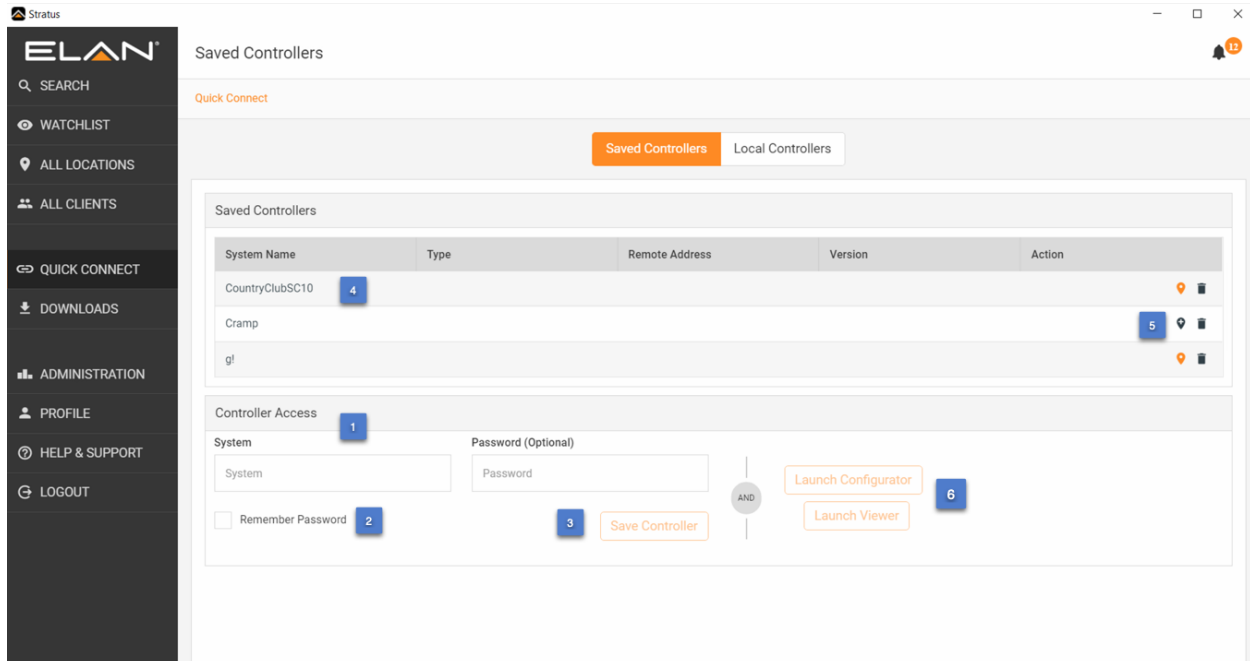
Quick Connect > *Authenticated*

1. Manually enter System (controller) name and password
2. Select Remember password* if you want it retained with Controller name when saved
3. Select Save Controller to place it in the Saved Controller List.
4. To recall a Saved Controller, tap on it in the Saved Controller list and its details will load in the Controller access area.
5. Action Functions to: View Existing Location, Create New Location, Delete from Saved Controller List.
6. Launch Configurator or Viewer using the credentials in the Controller Access area

Tip: To change a password for a Saved Controller, tap on it in the Saved Controller list and its details will load in the Controller access area. Overwrite the password and hit "Save Controller" to save new password with controller name.

*Note: The passwords entered and saved with Quick Connect are never the same as the password/user used in a location to access Configurator and Viewer from a location. As stated in the "Cloud Authentication & Permissions Layer," location passwords are hidden and encrypted. Keep this in mind when accessing the same controller from Quick Connect and Location.

Local Controller
Available in Authenticated and Unauthenticated modes.
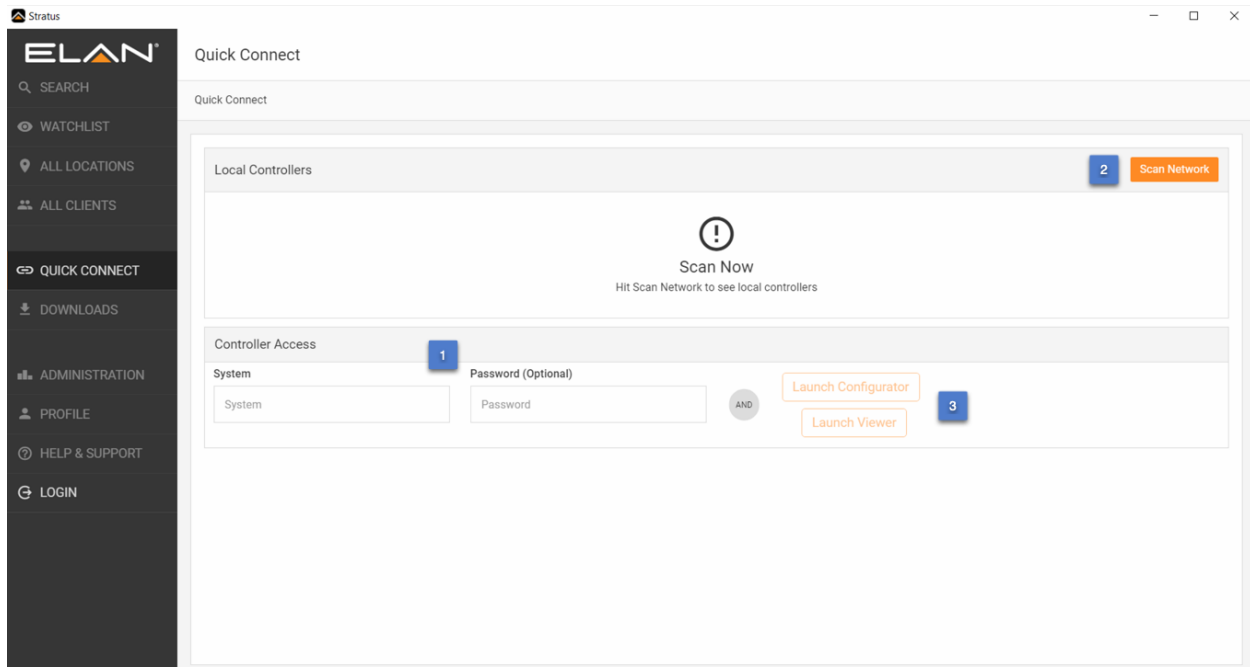
Quick Connect > *Authenticated* **(pictured)**

1. Manually enter System (controller) name and password, OR
2. Scan Network and select found controller to load its name into the Controller access area.
3. Launch Configurator or Viewer using the credentials in the Controller Access area

Authenticated mode allows you to save locally scanned controller to the Saved Controllers list as covered previously.

Downloads

Downloads section includes access to software downloads, documentation and updates for the Management Cloud application itself. At the top of Software and Documentation tab includes a filtering field to quickly find the file you are looking for.

- Software
  - ELAN Core Release Installers, Clients & Viewers, Utilities and Libraries.
- Documentation
  - Release Notes, User Guides & Integration Notes
- Updates
  - Check for updates for the Management Cloud application. Updates can be downloaded and installed via this function.

Administration

The Administration tab is accessed by permission only (Owner and Team Lead roles) and currently includes functions to administer users and groups for your company, and Note Categories. These categories can be defined by Admins and accessed by employees in the Location Notes section of each location to help classify work performed. This will help standardize entries for forthcoming reporting functions.

Profile

Profile tab contains information about and relevant to the current user logged into Management Cloud.

- **Details** – Name, Address and Contact information for current user. The Company Name is not editable.
- **Company Info** – Address information for the Company. Name and Contact email are not editable.
- **Manage Alerts** – This tab allows one to administer all the alerts one is subscribed to in a single screen. One can also administer alerts on the Manage Alerts tab on a respective site, but all alerts are aggregated here for convenience.
- **Manage Notifications –** Notifications are messages sent by Nortek Security & Control and fall into multiple categories. Unlike standard email which can be blocked at many junctures, the Notification loop in Management Cloud will help us ensure deliverability of important messages and information to our customer. Select Notification options here as desired.
- **View Groups - Lists** the Groups current user is associated with. Management of Groups is handled by Owner and Team Leads in the Administration tab.
- **Change Password -** Change password for your Management Cloud account.
- **Settings –**
  o Select Language, Time Zone, and preferred Date Format and Time Format for your application.
  o Set "Default Alert Settings" (1.0.2) to predefine your alert settings when you are added to a location, such as when you create a location, added to a location as a member of an Admin Group or manually added via the "Add Recipient To All" and "Add Alert Recipient" on the Manage Alerts tab.

Help & Support

Integrated Support options provide a one-stop-shop to help service your customers. This area will be dynamic, including the latest information and training options to keep your team updated and informed.

- **FAQs and KB** – Technical Information relevant to you and your subscribed NSC products and services.
- **Tech Alerts** - Technical Alerts relevant to you and your subscribed NSC products and services.
- **Video Notes** – Video Integration Notes and other training videos relevant to you and your subscribed NSC products and services.
- **Resources** – Technical, Sales and Support options for your reference
- **Contact Us** – In-App feedback form for this application & platform. This is not an avenue for Technical Support.

How To

Create A Location

All Locations > Create a Location (button)
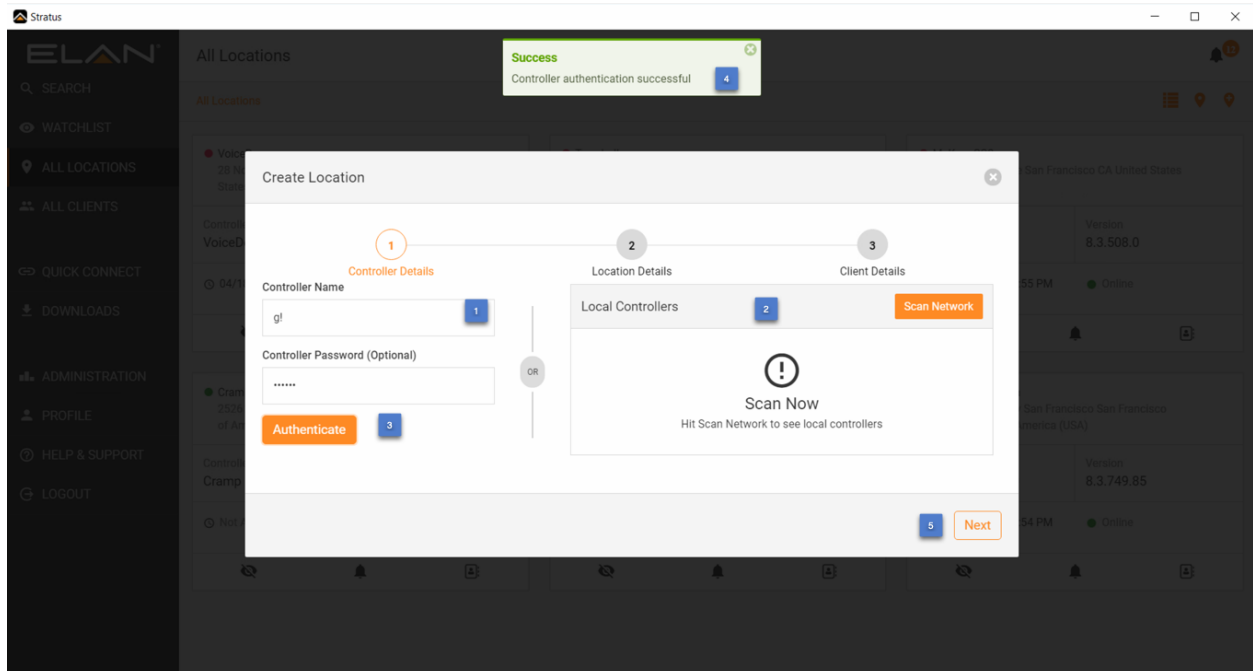
All Locations > Create a Location > Step 1 of 3

1. **Controller Name and Password button**: Name of controller and admin password (if preset).
2. **Scan location network** for attached controllers. Select a controller in the found list to have it loaded into the Controller Name field on the right.
3. **Authenticate:** You must authenticate controller name and password before moving to next screen.
4. **Successful Authentication message**
5. **Next button***:* Becomes active when controller authenticated

Note: Controllers must be running ELAN core release 8.3.11 or later when adding as a Location in Management Cloud. The ***Quick Connect*** function in Management Cloud is not dependent on

Create Location

All Locations > Create a Location > Step 2 of 3

1. **Location Name**: Can be named whatever desired or follow Controller name when using checkbox. With this box checked, controller name changes will affect location name accordingly.
2. **Installation Date:** Defaults to today's date but can be edited
   a. **Daylight Saving –** Not functional in this iteration.
3. **Time Zone:** Required
4. **Select Admin Group (optional):** Add a new location to a preexisting group for quick location permissions set up. Groups are covered later in this document.
5. **Next***:* Becomes active when required fields are entered.

All Locations > Create a Location > Step 3 of 3

Locations require Client association. When adding a Location, a Client must be selected or created. Deleting a client will warn about also deleting client locations.

1. **Select Existing Client**: Pulls list of current clients available for this account, based on permissions.
2. **Create a New Client:** Defaults to today's date but can be edited
3. **Finish:** Will create the location, add dealer user cloud account to controller with hidden, encrypted password, pull all configuration details and auto-configure alerts.

Create a Client

Creating a Client from the All Clients > Create Client dialog

Create Client > Screen 1 of 2

1. **Client Image** (optional)
2. **Client Name**
3. **Client Address**
4. **Search Address: (1.0.2)** Uses Google API to search and suggest address for quick setup. Use of this service will ensure more accurate pin placement of location on the map.
5. **Primary Contact:** Primary contact is the main contact for this client. Additional client contacts can be added to the Client record as needed.
6. *Next:* Button becomes active when all required fields validated.

Create Client > Screen 2 of 2

1. **Select Existing Location:** Select location that already has different client connected to it to use this client instead. (not common)
2. **Create a New Location:** If you want to add a new client and a new location for that client, you can do that all in this Client creation flow. See "Add a Location" for details on this flow.
3. **Skip Location:** (not shown in this image, but at bottom of scrolled window) Use this option to just all a client and not associate with location yet. Adding a location later you can choose any client you have added.
4. **Finish:** Button becomes active when all required fields validated. This will add the client and associated records.

Create a Client Contact

Creating a Client Contact from the All Clients > [Client Name] > Client Contacts tab.

Details of the Client Contact form a self-evident. Note that client contact form starts with fields from the main client account but can be edited as required.
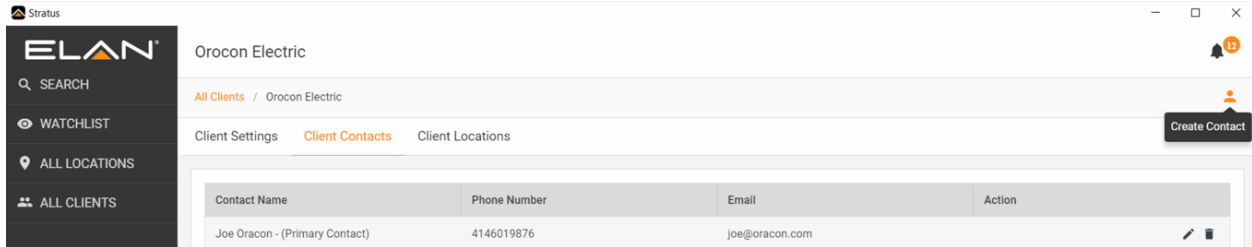
All Clients > Client Contacts > Create Contact

Add A User

A User is considered an employee or contractor for your company who can be assigned access privileges to platform and your locations that you choose to assign. NOTE: An email address can only be associated with one Dealer account at this time.

1. On the Users tab, select Add User option in the upper right of window:
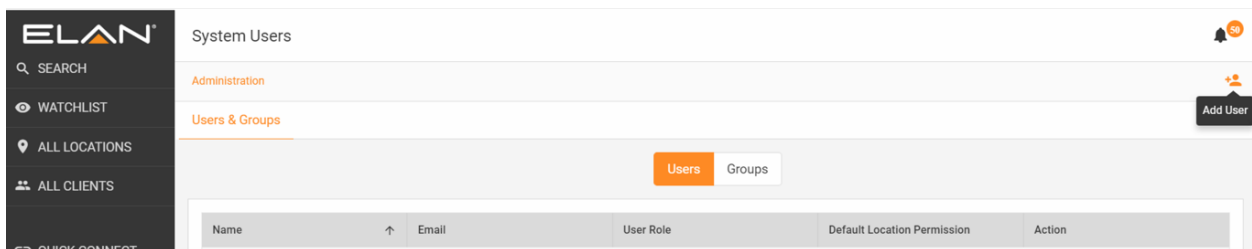
2. On the Add User dialog, enter email address and select System **Role** and *Default* **Location Permission.** Role can be adjusted in this dialog after account is created and default Location Permission, which is used when adding a User to a Group, can be adjusted in the Group as needed. See section on Roles & Permissions for details on each.

Users added will receive an email to verify their email address and then sent an email with a temporary password to log into Management Cloud. Upon first login, users are shown their Profile page to encourage filling out the rest of the details for their account.

Add A Group

Groups are used to great teams from your users and assign them locations so you can manage them in bulk fashion. When you Add a Location, you have the option to assign that location to an Admin group, saving time from having to add individual access later.

- On the Groups tab, select Create User Group option in the upper right of window:
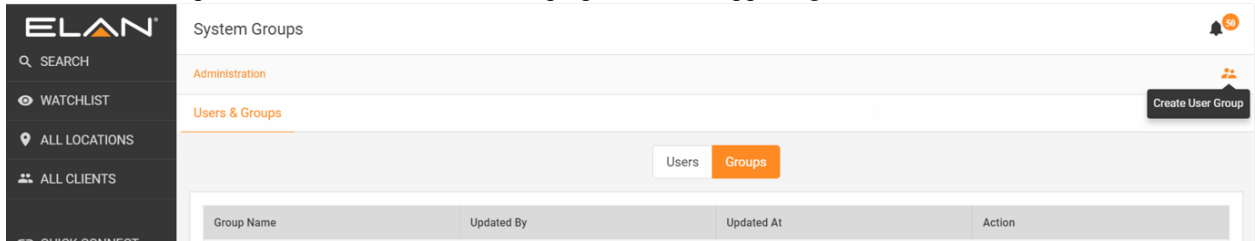
3. On "Create User Group" dialog, add a Group Name t and select locations to be administered by the group. NOTE: Locations can currently only be included in one group, so locations already accounted for will be greyed out. Select "Next"

4. On "Select Users" dialog, select the Users that will be part of this group. There is also an option to add a New User via this dialog, which will add/invite user as described in the Add A User flow. NOTE: Users can currently only be included in one group, so users already accounted for will be greyed out. Select "Next"

Create User Group

✓ Select Locations — 2 Select Users — 3 Select Permissions

Select Users

☐ Tom McKeon	tom.mckeon@nortekcontrol.com	☐ Nee Raj	neeraj.rajpure@corebrands.com
☐ Mayank Saxena	mayank.saxena@nortekcontrol.com	☐	robert.wehrfritz@nortekcontrol.com
☐	neema.mehta@capgemini.com ⚠	☐	neema.mehta@nortekcontrol.com ⚠
☐ Neal Ellsworth	Neal.Ellsworth@nortekcontrol.com	☐	wehrfritz@gmail.com ⚠
☐ Jason Davis	jason.davis@nortekcontrol.com	☐ Tommy Roy	tomdinamoxback.com

Create User

User Email	System Role	Location Permission	
User Email	Select Role ⌄	Select Permission ⌄	Save

Previous   Next

5. Select location permissions for each user in your group. The Default Location Permissions chosen when adding a User will be the default here, but you can adjust the permissions for a user in each location as desired by clicking the up arrow to the far right of each user in the list. Hit "Finish" to create the Group.

Create User Group

✓ Select Locations — ✓ Select Users — 3 Select Permissions

Nee Raj	neeraj.rajpure@corebra...	Default Permissions: ● Administrator ○ Installer ○ Monitor	⌄
	Spalla	● Administrator ○ Installer ○ Monitor	
	CountryClubSC10	● Administrator ○ Installer ○ Monitor	
Neal Ellsworth	Neal.Ellsworth@nortekc...	Default Permissions: ● Administrator ○ Installer ○ Monitor	^
Jason Davis	jason.davis@nortekcont...	Default Permissions: ○ Administrator ● Installer ○ Monitor	^

Previous   Finish

Manage Your Alerts

Alerts are set so you can be notified by device and node changes in near real-time. Understanding how to manage alerts will help you more proactively respond to issue but also allow you to filter out alerts that are not relevant to you.

Subscribe

- If you add a location, or are part of an Admin Group selected when adding a location, you are automatically subscribed for all Configured Devices alerts, which includes all state changes and both In-App and Email notifications.
- You can also manually add yourself to alerts in the following manner:
  - Location > Manage Alerts
    - "Add Recipient to All" function will add the entered email address to all Configured Devices.
    - To add to User to specific devices, click on the 👥 icon to the right of the device.

Unsubscribe

- You can also manually remove yourself to alerts in the following manner:
  - Location > Manage Alerts
    - Uncheck Alerts, Alert Modes or Delete User from respective devices
  - Profile > Manage Alerts
    - Uncheck Alerts, Alert Modes or Delete User from respective devices
  - TIP: In-App notifications, one can unsubscribe from the overflow menu:
    -
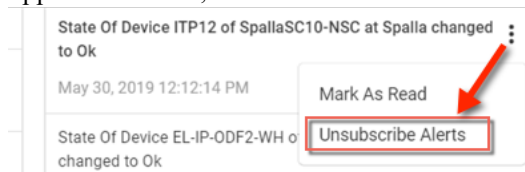
    - Note: If unsubscribed via this menu, the alert will remain but the option to Subscribe will be present as long as the alert remains in the menu.

Alert Threshold

- Refine in-app and email alert frequency by customizing threshold on a per-component basis. Reduce alerts for oscillating devices. Select from 0 (no threshold), +3, +5, +10, +15, +30, +60, +90 minutes. Note that Threshold time is *in addition to* the polling increment a controller uses to check devices, which can be from 0 to 90 seconds, depending on when the alert event occurs relative to the polling time.
- Alert Threshold is found on the Manage Alerts pages, with a default Alert Threshold is +3 min.
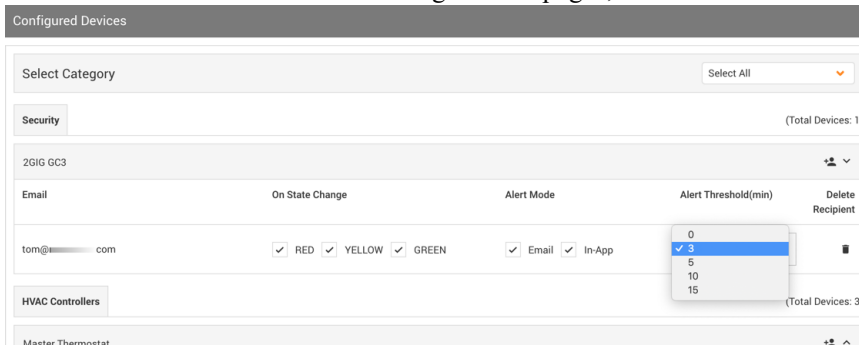
Manage Location Status

Location status is a rollup of the status from individual devices and nodes in a location into a single-color status that can be seen at a glance, and soon, by search, sort and filter. Location health color indicator is located next the location name in card view, list view and at the top of the screen when you navigate within a location.

Exclude from Location Status

Not every device/node that has the capacity to report status does so. For example, some 3rd party device drivers work as expected but have not been updated yet to report status to Management Cloud. Rather than let the incorrect status for these devices affect the location health status, you can exclude the devices so have a more accurate overall location health status.

For each device desired, select the "Exclude from Location Status." Note the icon for that device will still show its current color status but the exclusion is denoted by a dash through the status indicator.

Rename a Controller

One of the key features and timesaver introduced in the Management Cloud platform is the ability for Dealers to rename controllers in real-time without the need to contact ELAN Technical Support. And it's as simple as you would expect.

- Add controller as a location
- On the Controller Details tab, if permissions allowed, you will see a pencil next to the Controller name
- Enter a new name for the controller and Save
    o Names must be unique, and you will be given a message if name is not available.

Rename Controller

Controller Name

ELANCloud2

A name change from this application updates our global controller registry. Clients linking to the controller using the old name will need to be updated. All name changes and change attempts are tracked to your account.

Cancel   Save

NOTE: All controller name change requests, successful or unsuccessful, are logged to your user account. Use the function as only necessary.

Add/Remove Location to/from Watchlist

Locations can be added to and removed from Watchlist very easily by accessing the Watchlist button on the location card or list.

"Add to Watchlist" icon as seen on the All Locations tab. Tap to add.
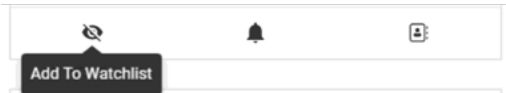
"Remove from Watchlist" icon as seen on the Watchlist tab. Tap to remove this location from your watchlist.
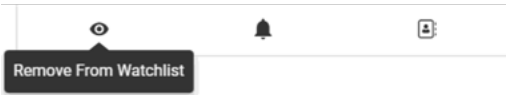
Update the Management Cloud Application

Application updates with feature/fix updates will be posted regularly through the platform's Notifications channel. You can manually check for and update your application in the Downloads > Updates > Check for Updates button.
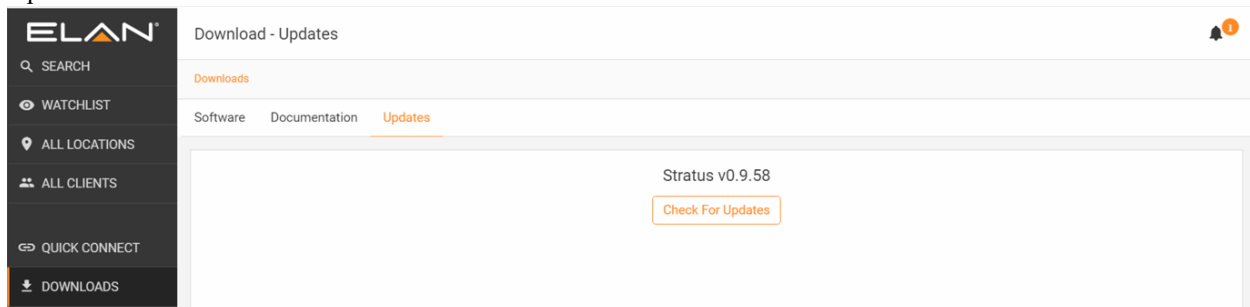
How to Use Management Cloud: A Suggested Workflow

As detailed in this document and in accompanying video tutorials, there are several features and functions in the 0.9 release of the platform that can be leveraged as desired based on the circumstance. Here we will suggest a simple workflow to help new users discover the features of the platform in a practical manner.

The following flow assumes that a dealer account has been created, the application installed.

1. Launch the application and sign in.
2. Add Users to invite others to join the company account
3. Quick Connect Tab – Find local controller or enter details for remote controller.
4. Save Controller, with password, in Saved Controller list
5. Launch Configurator and configure controller as desired. While Management Cloud will track configuration updates after a location is created, it is suggested that the controller configuration be as complete as possible before adding as a location.
6. If this is a new client, go to All Clients and Create Client
   a. Option: In the Create Client flow, you can specify controller to create location or defer until later
7. If location not created in Create Client flow, click on the gray "+" icon next to the controller in the Quick Connect "Saved Controller" section to start the process to add that controller as a location.
   a. Option: You can add a location at any time on the All Locations tab
8. Select the client created in step 5.
9. Once location is created, navigate into the location and rename the controller as desired.
10. Navigate to Manage Alerts and adjust the default alerts as desired
11. Assign user permissions for a Location
    a. On Location Settings > Permission Settings assign users their site permissions
    b. Option: Once you have at least one location created, and Owner or Team Lead can navigate to the Administration tab and "Add Group" to start to link Users from step #2 to the locations created. Groups will allow you to quickly assign permissions to users in a group when subsequent locations are added.
12. Configurator and Viewer access for each location, based on location permissions, found on Location > Controller Details page allow for 1-click access to a controller utilizing the Dealer account automatically created on the controller as part of the Add a Location workflow.
13. Location Notes should be added/accessed by teams for time and issue tracking.

Reference

Status: Colors & Strings

Management Cloud endeavors to provide actionable status at a glance. As such, we use a combination of colors and string data to quickly convey the health of individual devices and nodes and a rollup of all to a location health status.

Device Color Coding:
(#1 in image below) On the controller tab, and referenced on the Manage Alerts tab, are color status indicators that can be interpreted as the following. interpret the color.
- Green – Device is working/communicating as expected
- Yellow – Device may be impaired but working; Check Device Status for information
- Red – Device unavailable or malfunctioning. Check Device Status for information
- Grey – Device not reporting status. Device driver may not currently support status posting.

Device Status String:
(#2 in image below) Check the string in Device Status for greater detail on the device state. This string will vary based on the device type and can may custom strings when 3rd party device drivers are in use.

Location Health Color Coding:
(#1 in image below)

- Green – All Devices/Nodes in Location are Green (or
- Yellow – Devices/Nodes in Location are Yellow and/or Green
- Red – At least one Device/Node in Location is Red

User Roles, Location Permissions & Remote Access

Management Cloud, for ELAN Dealers, defines various Roles and Location Permission types to allow a more granular and secure level of access to the platform and to locations associated with one's account. In short, **Roles** define permissions one has to the Management Cloud application/platform whereas **Location Permissions** define the permissions one has on a location basis. **Remote Access**, a paradigm that has existed in ELAN for some time, provides the end user with ultimate control over level of access a dealer account has to a location.

Special Note: The Management Cloud platform was designed to be flexible and serve different product lines, channels and audiences. At the platform level, we package roles, permissions, pricing and other governing parameters into a **subscription** which is then assigned to a Dealer account at account creation. What is described in this document is the default subscription for ELAN Dealers which will be refined, based on user feedback in the pre-release period and beyond.

Roles

Roles essentially define the functions and tabs one has access to in the Management Cloud environment. You can think of it as application/platform level permissions one is assigned when an account is created.

Role Types:
- **Owner**
  - This role is assigned to the owner of the business account. It is assigned by Management Cloud team when an application has been approved. It can only be edited by the Management Cloud team. There is only one owner per account.
- **Team Lead**
  - This role is intended to include many of the same permissions as owner, so owner not obliged to actively manage the account, but with some exceptions around managing the account.
- **Member**
  - This role is intended for most employees.

Role Permissions Detail

Function	Owner	Team Lead	Member
User Profile:			
Update Profile Fields	X	X	X
Change Password	X	X	X
Manage Location Device Alerts	X	X	X
Manage Notifications	X	X	X
Show Groups	X	X	X
Manage Settings	X	X	X
View Company Info	X	X	X
Update Company Info	X	X	
Administration Groups:			
List All Groups	X	X	
Create Group	X	X	
Update Group	X	X	
View Group	X	X	
Delete Group	X	X	
Administration Users:			
List All Users	X	X	
Create User	X	X	

Update User	X	X	
Delete User	X	X	

All Clients:

List All Clients	X	X	X
Create Client	X	X	X
Update Client	X	X	X
Delete Client	X	X	

Client Contacts:

List All Client Contacts	X	X	X
Create Contact	X	X	
Update Contact	X	X	X
Delete Contact	X	X	

All Locations:

List All Location	X	X	
Only List Locations Assigned to Me			X
Create Location	X	X	X

Watchlist:

List Watchlist Locations	X	X	X

Help & Support:

List FAQs	X	X	X
List Tech Alerts	X	X	X
List Video Integration Notes	X	X	X
List Resources	X	X	X
Show Contact Info	X	X	X
Send Feedback	X	X	X

Downloads:

List Software Downloads	X	X	X
Allow Software Downloads	X	X	X
List Documentation	X	X	X
Download/View Documentation	X	X	X

Search:

Allow Search	X	X	X

<u>Alerts & Notifications:</u>

List All Alerts	X	X	X
Mark Alert as Read control	X	X	X
Unsubscribe Alert control	X	X	X
List All Notifications	X	X	X
Mark Notification as Read control	X	X	X
Unsubscribe Notification	X	X	X

<u>Quick Connect (authenticated):</u>

View Controller	X	X	X
Add to Saved Controller	X	X	X
Delete Controller	X	X	X

Location Permissions

Location Permissions define the level of access a user has to view and manage a location associated with a dealer account.

Location Permission Types:
- **Administrator**
  - Provides full access to view, modify, lock and delete a location.
- **Installer**
  - This role includes monitoring permissions and some editing functions.
- **Monitor**
  - Intended for personnel who are tasked with viewing site and device status. Editing and remote functions disabled.

Location Permissions Detail

Function	Admin	Installer	Monitor
Location Card View:			
Add/Remove Watchlist	X	X	Only for subscribed
View Location Details	X	X	Only for subscribed
Mute/Unmute Location Notifications	X	X	
View Contact Info	X	X	Only for subscribed
Controller Details			
Access Controllers Tab	X	X	Only for subscribed
Rename Controller	X	X	
Edit Description Note	X	X	

Launch Configurator	X	X	
Launch Viewer	X	X	
View Configured Devices	X	X	Only for subscribed
View Configured Devices	X	X	Only for subscribed
Network Management			
Access Network Management Tab	X	X	Only for subscribed
System Logs			
Access to System Logs	X	X	Only for subscribed
Exception Logs			
Access to System Logs	X	X	Only for subscribed
Connection Logs			
Access to System Logs	X	X	Only for subscribed
Location General Settings			
Access to General Settings	X	X	Only for subscribed
Update Location	X	X	
Delete Location	X	X	
Location Permission Settings			
Access to Location Permissions Tab	X	X	
Add Individual User	X	X	
Edit Individual User	X	X	
Delete Individual user	X	X	
Location Notes			
Access to Location Notes Tab	X	X	Only for subscribed
List All Notes	X	X	Only for subscribed
Create Note	X	X	Only for subscribed
Update Note	X	X	
Delete Note	X	X	
Manage Alerts			
Access to Manage Alerts Tab	X	X	Only for subscribed
Add Recipient to All	X	X	
Edit Alerts	X	X	
Delete Alerts	X	X	

Remote Access

Remote Access, a paradigm that has existed in ELAN for some time, provides the end user with ultimate control over level of access a dealer account has to a location.

When an ELAN controller is added to one's account as a location, a new user (and user type*) is created on that controller to give visibility to the end user but also provide ultimate control over the level of access they grant.

*Cloud User for a Management Cloud account on a controller differs from other user accounts in the following ways:

- It is autogenerated on a controller when it is assigned as a location within Management Cloud
- These special user accounts include Company Name, email and phone contact information, and remote access level.
    - The name of the user is derived from the Dealer name associated with the Management Cloud account and cannot be edited.
    - Contact information in the user account included phone and email, which can be updated by Owner or Team Lead in the Administration tab in Management Cloud as needed. However, update of email and phone will only affect new user account creation; User accounts already created in the field will not be updated, **so it is strongly suggested that a general email and phone number be used when creating an account to ensure future relevancy.**
    - Password for this account is autogenerated, encrypted and obfuscated so permissions can be gated in Management Cloud for one's account.
    - Remote Access levels can be adjusted by end user to define the highest level of access allowed by that user on a controller, keeping ultimate control in hands of the end user. A selection of "None" can be a means to temporarily disable Management Cloud access.
    - Deletion of the account is allowed, keeping ultimate control in hands of the end user.

The Remote Access levels as they have been in ELAN, with one addition for Cloud user accounts. Since a cloud user is actually a dealer company with potentially multiple users, Remote Access defines the highest level of access to the control for that account. As described in the location permissions section, one can define varying permissions levels for users but are subject to Remote Access level granted by end user.

- All
    - Allows for Configurator, Viewer and Status access.
    - This is the default Remote Access level assigned for Management Cloud-created accounts.
- Programming
    - Allows for Configurator and Status access. No Viewer access allowed.
- Viewer
    - Allows for Viewer and Status access. No Configurator access allowed.
- Status
    - A new Remote Access type specific to Management Cloud-created Accounts.
    - Allows for Status access. No Configurator or Viewer access allowed.
- None
    - Will disable remote access permissions for that user