

\*\*\*The employee must have first created a password through Employee Web Services in order to use the Phone App, or a password must be created for them by a supervisor or administrator of the site. \*\*\*  
\*\*\*It is also suggested to only setup ONE phone at a time to reduce error when reading the Device ID in step 3\*\*\*

## App Setup

### Step 1: Download the App from the App Store (Or Playstore)

### Step 2: At the Device

#### For iPhone

1. Go to Settings
2. Scroll to the bottom until you see NOVAtime
3. Click on NOVAtime
4. Input your Client ID; found on the login pages of NOVAtime or in the top right hand corner of your screen (ITP15060) ITP must be capitalized
5. User name: Your employee ID
6. Input your password (if you have not created a password, then the password will be pa55word)
7. News URL is <https://news.novatimeanywhere.com>
8. Back out to Settings and open the app
9. Reenter your ID and Password
10. Click login, you will see an unsuccessful message, this is normal, continue with setup.

#### For Android

1. Open the NOVAtime App
2. HOST: hit the default button

3. Input your Client ID; found on the login pages of NOVAtime or in the top right hand corner of your screen
4. User name: Your employee ID
5. Input your password (pa55word)
6. Check "Single Employee"
7. Click Validate, you will see an unsuccessful message, this is normal, continue with setup.

### Step 3: At the computer



1. News, Audit Trail
2. Confirm that the device is in the audit trail, if not, either the URL, Client ID or Password is wrong. Reenter information and click validate again and refresh the Audit Trail by going to another page and then coming back to this page.
3. Click on the Device Authentication. In the Review Details copy only the Device ID

A screenshot of the 'Audit Trail' interface. At the top, there are tabs for 'Security', 'Default', 'Audit Trail', and 'Netsuite'. Below the tabs, there are search filters for 'From Date', 'To Date', and 'Select Service'. A table with columns 'Interface', 'Process Date', and 'Status' is shown. The 'Interface' column contains 'DEVICEAUTHENTICATION' entries. A blue arrow points from the 'Interface' column header to the first row. Another blue arrow points from the 'Device ID' field to the first row's 'Interface' cell. Below the table, there is a 'Review Details' section with the text 'itp\_demoNT7000\*\*\*\*5131245187NT7000 Ver.2.26B - OS V7.6(140120)002-101Invalid DeviceID or User name or Password'.

Interface	Process Date	Status
DEVICEAUTHENTICATION	8/7/2014 1:43:24 PM	002-101 - INVALID DEVICEID OR USER NAME OR PAS ...
DEVICEAUTHENTICATION	8/7/2014 1:43:22 PM	002-101 - INVALID DEVICEID OR USER NAME OR PAS ...
DEVICEAUTHENTICATION	8/7/2014 1:40:19 PM	002-101 - INVALID DEVICEID OR USER NAME OR PAS ...
DEVICEAUTHENTICATION	8/7/2014 1:40:19 PM	002-101 - INVALID DEVICEID OR USER NAME OR PAS ...
DEVICEAUTHENTICATION	8/7/2014 1:37:23 PM	002-101 - INVALID DEVICEID OR USER NAME OR PAS ...
DEVICEAUTHENTICATION	8/7/2014 1:37:21 PM	002-101 - INVALID DEVICEID OR USER NAME OR PAS ...

The Device ID for Android phones is the phone number. The device ID for the iPhone's usually looks something like 12D85888-0139-4F0D-B046-A6F7DBD92530

## Step 4: At the computer

1. News, Security
2. Click New
3. Device ID: Paste from the Audit Trail
4. Device Type: Mobile Employee
5. Create a description, usually Employee's Name
6. Client ID is ITP14495 (must be capitalized)
7. Select Timezone and Daylight Savings
8. User name is the employee ID, use the magnifying glass to find the employee
9. The password is the same as their login for the web services, should auto fill once you select the employee
10. Click on "Allow Downloaded Passwords"
11. Click Save



Example of Completed Security Page

**Security**

New Save Undo Delete

**Device Details**

Device ID: 12D85888-0139-4F0D-B046-A6F7DBD92530

Device Type: Employee Mobile Services

Description: Crystal's iPhone

Client ID: ITP\_DEMO

Device Timezone: (GMT-06:00) Central Time (US & Canad) Daylight saving

Username: 311 Allow multiple employees to share this device

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Authenticate against IP

IP Address: 0 . 0 . 0 . 0

Authentication expiration Period:

Days: 1 Hours: 0 Minutes: 0

Audit Level: ERROR ONLY

Allow download passwords

## Step 5: At the Computer

12. Go to HW Devices, Push Clocks
13. Click on the Clock tab
14. Change the site to "Unassigned"
15. Locate the newly added device
16. The Device information should fill in based on the information already added in the system
  - a. Select the site
  - b. Select the Function Key Setup
  - c. Clock prompt (optional)
17. Click Save, the device should disappear from the list.
18. The clock is moved to the new "site" (reverse step 14)



## Step 6: At the Device

1. Click validate (or login) again
  - a. If it does not say successful, start from Step 2 and try again