syntrio
HOTLINE

CASE MANAGEMENT SYSTEM

Track employee hotline and web reports in one easy-to-use tool

Get everything you need to track hotline reports from beginning to end in one easy-to-use online tool

For most organizations, keeping track of hotline reports can be a daunting challenge. Overlooked or missing information can lead to inefficient investigations and leave you vulnerable to potential litigation.

Syntrio can save you time and labor costs by including our powerful and efficient Case Management System (CMS). The CMS is a secure, web-based tool that allows you to manage and collaborate on all your hotline reports and investigations.

With our CMS, you can track every issue from a report's receipt through its resolution, allowing you to optimize investigations, reduce administrative oversight, ensure due diligence and create an audit trail.

CMS: The Way to Optimize Your Investigations

For companies with high call-volume, tracking and analyzing hotline reports can be complicated, not to mention highly labor-intensive.

Key CMS Features and Benefits

Our CMS provides you and the appropriate ethics and compliance personnel with the ability to:

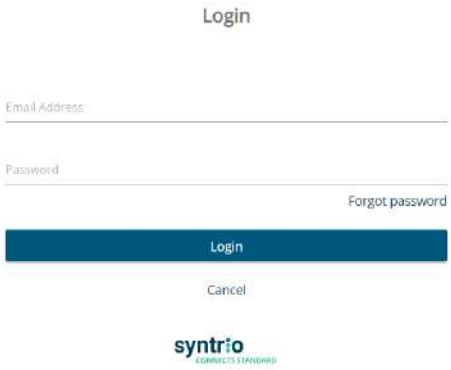
1. **View the Report Online** — You can access report information online even when away from the office. Because the CMS application resides on the Syntrio server, there is never a need to download software.
2. **Assign the Incident to a Person for Investigation** — You'll be able to assign the report automatically to the appropriate individual quickly, and you'll know the right person to contact if you have questions or concerns about any investigation.
3. **Assign Risk Level, Priority and Status** — This ensures that the most urgent or sensitive cases are given top priority and that all reports are handled in a timely and expeditious manner.
4. **Record Your Follow-Up and Outcome** — You'll be able to input all actions taken as well as each report's ultimate resolution, which is critical to creating an audit trail.
5. **Dialog with Reporter** — If the reporter chooses to create a report PIN, the case investigator or administrator can carry on an anonymous dialog with the reporter, allowing for the continuous exchange of information throughout the course of an investigation.
6. **Create and Manage Reports** — You'll have the capability to develop a variety of reports that can be issued to key personnel within your organization on a "need to know" basis. Templates can be created and scheduled for commonly used reports. Your CMS comes equipped with an advanced analytics dashboard with a view to all key metrics and trends and the ability to drill down to details using a comprehensive and easy to understand set of user controls.
7. **Attach Multiple Files to a Report** — You can supplement reports by uploading additional files as needed.
8. **Collaborate With Ease** — CMS allows users to share either detailed or summary information about a report with appropriate personnel or outside parties. Data from CMS is exportable with pushbutton simplicity. Our message board feature communicates client messages to system users. Information links allow easy access to company polices and forms relevant to your investigation activity.
9. **Link Reports** — You can add a Link ID to associate a report with other previously received reports you identify as having similar issues.

Operating the CMS

To access the system, log into the CMS website by clicking on this link: *https://connects-standard.syntrio.com*

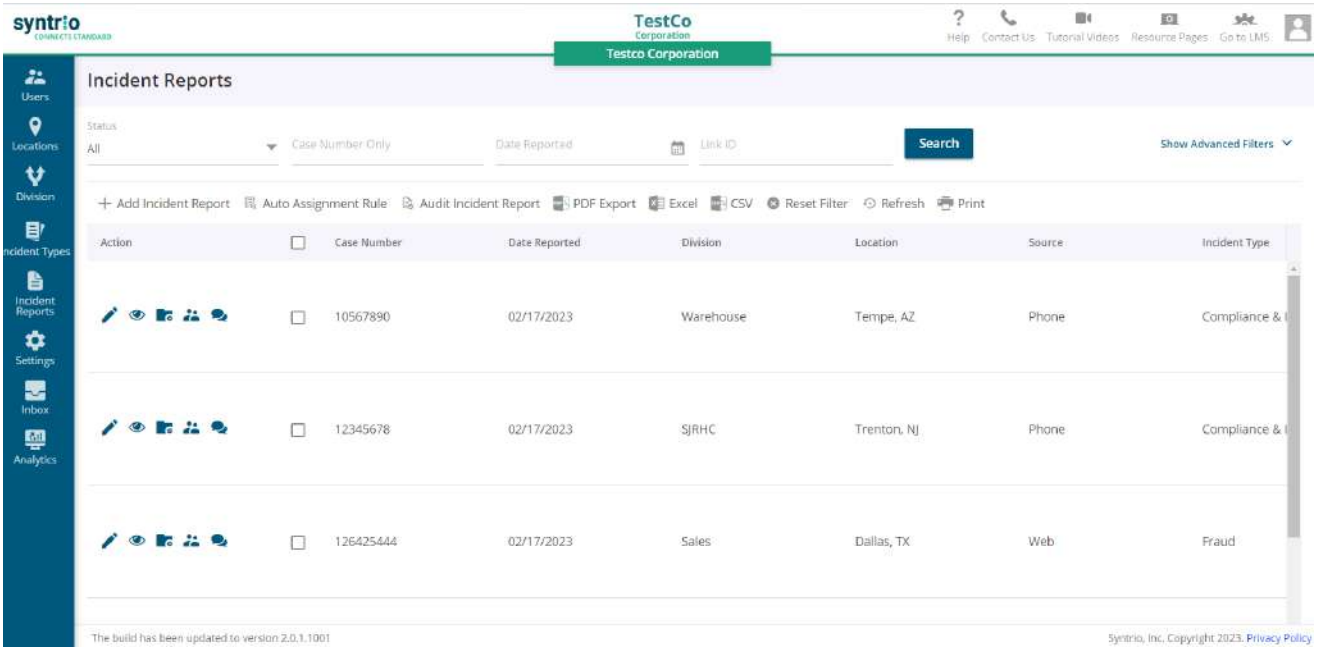
1 *Log In*

CMS will then prompt you to enter your unique user ID (your email address) and password.



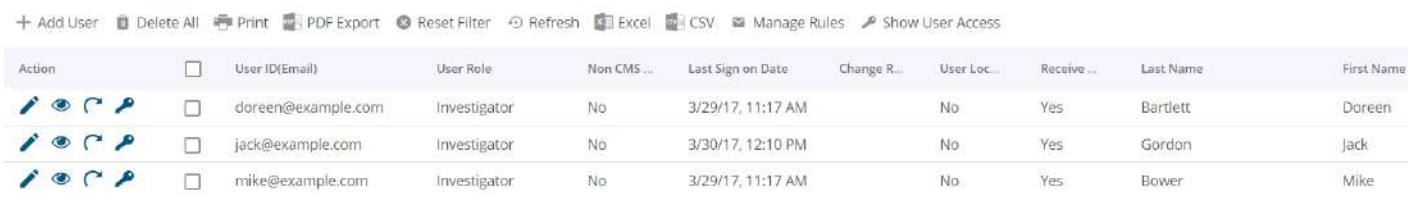
2 Visit the Incident Reports Tab

Once you have successfully logged on, the CMS will open in the Incident Reports tab. From here, you can easily manage all reported cases. Each incident is assigned a unique report number, and the built-in filters allow you to manage cases when using fields such as date, incident type, risk level, priority, status, nature of report, or by using a keyword. By placing your cursor over an object in the application, a tooltip showing a description of the function will appear.



3 Add New Administrators & Investigators/Non-Administrators Using the Users Tab

The CMS also allows you to designate individuals as Administrators who have access to all case records, and Investigators/non-Administrators who have access only to those records assigned to them by the Administrator. This feature helps you optimize the effectiveness and security of the CMS by providing an additional level of oversight and control.



Defined User Roles

The system has two levels of users:

1. Administrators: who have unrestricted access to the database, create new users, assign investigators and can add new internal reports.
2. Investigators/non-Administrators: who are assigned to individual records by the Administrator.

Investigator/non-Administrator user access can be modified based on the business and individual user's needs. By default, Investigators/non-Administrators have the ability to access only those records assigned to them. Records can be assigned to one or more Administrators or Investigators by clicking on the assign user icon in the Incident Reports tab.

Company Administrators have access to the entire system without impediment.

- They can add or delete users, change user roles and manage user profiles
- They can add and delete different divisions within your company as necessary
- They can access all incident reports, assign investigators, track progress, dialog, add files, etc.

Investigators/non-Administrators profiles are dynamic and can be modified based on a user's needs. However, by default Investigators/non-Administrators only have access to the Incident Report tab.

- They can only investigate, track progress, dialog, add files, etc.
- They cannot add investigators to reports
- They cannot modify system settings

Other Important Features

When a reporter chooses to create a report PIN, they enable dialog capabilities with both Administrators and Investigators. Reporters also choose whether they'd like to be anonymous.

Dialog Capabilities

All Administrators and any Investigators assigned to an incident report will be copied on dialog emails, unless your organization elects to omit unassigned Administrators. However, if there is no assigned Investigator and Administrators have elected to not view dialog emails, reporter emails will be sent to all Administrators by default.

Manage Custom Fields

The CMS allows an Administrator to define up to three fields for a report. These custom fields will appear on the Add/Edit/Show Incident Report pages and will be included in exports of incident report data. The following types of custom fields are available:

- Numeric - Integer
- Number - Decimal
- Numeric - Currency
- Date
- Text (maximum 255 characters)
- Dropdown List

Audit Trail

The CMS provides you with fields for your Follow-Up and Outcome notes. These fields are available for entering progress notes and logging investigative activities. Username and time and date of entries are displayed whenever text is added in these fields. After entering and saving data into these fields it cannot be modified or removed. Additionally, the system keeps track of every change to a record via an audit interface.

Drop-Down Usability

For your convenience you can deploy the advantages of dropdown lists by creating your own throughout the system preventing users from entering erroneous data and allowing for a standardized data structure.

Easily and Quickly Respond to a Reporter

Company users have access to a library of quick response messages that can be quickly sent to/saved for a reporter from the Dialog page. With a few clicks of their mouse, a user can choose which message to send to the reporter.

Create Reports Not Submitted through Lighthouse

The CMS gives you the capability to create reports for any incident, even those not reported through the Syntrio system.

Investigator Oversight

Reminder notification emails send configurable email messages to CMS users assigned as investigators on a case. When the feature is enabled, users assigned to a case will receive reminder notification emails when the status of an incident report remains unchanged for a specified period of time.

Web API Access

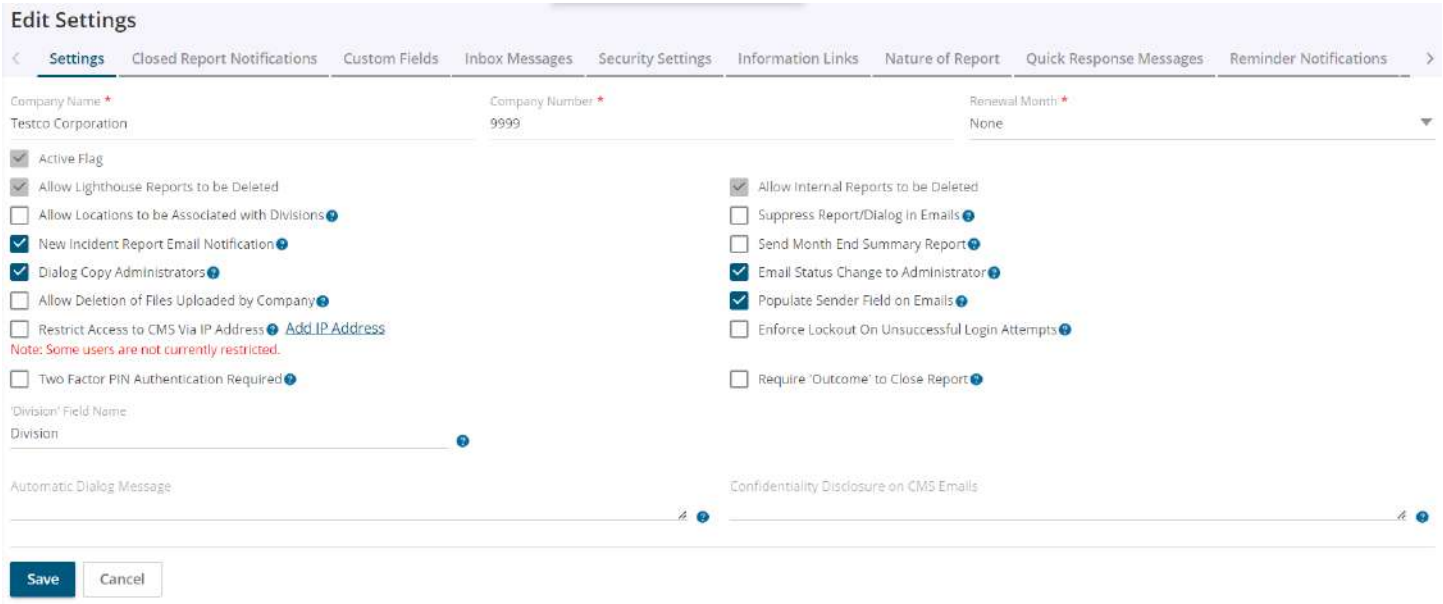
With CMS API enabled clients can initiate remote transactions seamlessly between systems to query the CMS and add incident reports.

Convenient Help Tutorials

With CMS, help is never more than a mouse click away. We offer easily accessible tutorial and onboarding videos for new users that enhance the user experience. Additionally, our customer service representatives are just a phone call or email away.

Customize Your CMS Site

The CMS is highly configurable with multiple setting options allowing you to align the system to meet your program objectives and accommodate user preferences.



Your Case Management System will be pre-configured with information that you provide in your Service Agreement.

Your Company's Confidentiality and Security is Our Top Priority

The Syntrio CMS is a cloud-based system that utilizes many levels of security including hardware and software firewalls, secure http access (HTTPS), optional two-factor authentication and IP access restriction, and client-controlled password complexity policies.

The data centers (production and disaster recovery) are located in secure, 24hr-monitored data centers. Our data center provider, Internap, is SOC2 compliant and utilizes many security protocols in their data centers including motion sensors, closed circuit video, anti-tailgating measures, security guards at all points of entry, escorting visitors at all times, walls extending from ceiling to floor, and alarms on all exterior windows and doors. Our servers are under a strict maintenance schedule for OS patch and 3rd party software updates.

Our data centers server is co-located in a SOC 2 certified facility that is equipped with proximity security badge access. Our servers are housed in a secure facility and are equipped with:

- Multiple Internet backbone connections
- Automatic fail-over through alternate secure connection
- All servers are protected with RAID drive arrays
- Secure, internally networked, high-speed data transmission between data centers
- 3 independent A/C feeds and robust UPS resources
- Cisco Systems 10G network
- Cisco Guard DDOS protection
- Geographically redundant DNS
- TippingPoint IPS/IDS protection
- Arbor Peakflow traffic analysis
- Arbor Atlas Global Traffic Analyzer
- Automated IP routing and management
- Server to Internet speeds up to 1 Gigabit
- ESET Anti-Virus

All of our servers are monitored and protected using Alert Logic Intrusion Detection software to identify and eliminate malicious external traffic to our servers. Lighthouse also conducts penetration and vulnerability testing using Veracode software which allow Lighthouse to shore up any system or network deficiencies to protect our clients' data.

Data at rest within our CMS is encrypted using AES 256-bit encryption and data in transit is encrypted using HTTPS. All production database backups are encrypted and stored at a distant, separate data center. Access to our servers by Lighthouse personnel requires VPN access, two-factor authentication, and complex credentials. Client access to their CMS requires complex credentials that are client-configured. Clients may also use extended security features of the CMS by enabling two-factor authentication and IP access restrictions. User credentials are stored in the CMS using a 256-bit, one-way encryption algorithm. Users are also notified of multiple login failures, requests for password changes and notification when their passwords have been changed. Clients may also enable an option to lock out user accounts after multiple login failures.

The following features in the CMS provide our clients with additional security measures:

• Account locking allows Administrator the ability to lock out specific user accounts

• Two-factor authentication requires users provide a randomly generated PIN for each session

• Customizable password requirements including password complexity and expiration rules

• Customizable session timeout rules and email link expiration settings

• Client enabled management of IP addresses with permission to access their CMS

• Enforce lockout on unsuccessful login attempts gives the Administrator the option to lockout a user or require them to respond to a CAPTCHA challenge

• Sign on access log lets users view a history of their previous sessions including IP address

Syntrio's CMS: The Cost-Free Way to Optimize Your Investigations

With CMS, there's no need to be overwhelmed by or worry about the mishandling of a high volume of hotline reports. Make the most of your Syntrio reporting hotline by using the CMS to manage your reporting and investigation process. Don't leave anything to chance.

ABOUT SYNTRIO

Syntrio is a global leader in governance, risk, compliance and human resource solutions that help more than 6,000 organizations make the workplace a better place – one organization, one culture, one person at a time. Easy, high-value and innovative Syntrio solutions include a robust employee experience platform, reporting hotline and case management system, and more than 1,000 elearning courses in Employment Law and Harassment, Ethics and Compliance, Diversity and Inclusion, Health and Safety, Business Skills and Cybersecurity. For more information visit syntrio.com.

Visit the resource center at syntrio.com for complementary ethics hotline reporting and learning information, including essential guides and checklists to improve your culture and compliance initiatives.

For more information visit syntrio.com.

888.289.6670 | SYNTRIO.COM