Cherwell Service Management

Crisis Management mApp Solution

Release 1.0

Revision 1.0

27 March 2020

Cherwell Software

www.cherwell.com

Table of Contents

Legal Notices

Cherwell Software, LLC
www.cherwell.com
info@cherwell.com
+1.719.386.7000
10125 Federal Drive, Suite 100
Colorado Springs, CO 80908
USA

Crisis Management mApp Solution V1.0

Cherwell now offers a free Crisis Management mApp® Solution that enables organizations to efficiently track the status of their workforce in transition to remote work. You can provide your employees a simple way to self-report their status and location directly from the Cherwell Customer Portal. Give management the real-time visibility they need to ensure a safe, secure, and productive workforce.

Visit the Cherwell Marketplace to download this free mApp Solution today.

Platform Version Requirements: Tested on CSM 9.7.0, 9.7.1, and 10.0.0

Content Version Requirements: Tested on CSM 9.7.0, 9.7.1, and 10.0.0. The Crisis Management mApp Solution may or may not work on previous content versions, but as with any mApp Solution, you should test it on your customized environment.

This is a Cherwell Labs mApp Solution intended to showcase experimental or beta-level content features in Cherwell Service Management. Functionality, testing, and documentation are limited or incomplete. Cherwell support is not provided for this mApp Solution, so install it at your own risk on a test environment before installing it on a production system.

How the mApp Solution Works

CSM provides Remote Employee Management as a mergeable application (mApp) so that you can effectively manage the transition of employees from the office to remote work. Use the Apply mApp Wizard to apply the mApp Solution to your development CSM system, where the solution can then be viewed and published. After evaluating and testing the solution against the development system, apply it to your production environment.

The Crisis Management mApp Solution includes the following items:

Item Category	Item	Typical Merge Action
Major Business Objects	Announcement Crisis Employee Crisis Response Site	Import
Supporting Business Objects	Crisis Resource Task	Import
Lookup Tables	Crisis Employee Response Actions Taken Crisis Employee Response Taken Crisis Employee Response Status Crisis Resource Position Crisis Status Crisis Type	Import
Dashboards	Crisis Management User Crisis Management	Import
Teams	Crisis Management	Import
Security Groups	Crisis Management	Import

	Portal Customer Suggested Crisis Object Rights	
Automation Process	Automatically Send Crisis Response Reminders Create Crisis Responses Employee Not Ok Send Notification On Response Created	Import
Event Monitor	Suggested Employee Status monitor Included	Import
Searches	All Active Crisis All Active Crisis Assigned to Me All Active Crisis Assigned to My Teams All Crisis In Recovery All Crisis in Warning	Import
Site	Suggested Menu Configuration for Crisis Management	Import

- Import: Add new item.
- Overwrite: Replace target item.
- Merge: Merge differences.
- Don't Change: Referenced by the mApp Solution, but not altered in any way. The mApp Solution includes the definition for informational purposes only (the definition is not imported into the target system).

For detailed information on merge actions, refer to the Apply a mApp documentation:

- Apply a mApp Solution (CSM 9.7)
- Apply a mApp Solution (CSM 10.0)

Steps to Apply the mApp Solution

To apply the mApp Solution, perform the following high-level steps:

1. Download the Cherwell mApp Solution file.
2. Apply the mApp using the Apply mApp Wizard in CSM Administrator.
3. When publishing the mApp Blueprint, be sure to select option 11 (**Update validation foreign keys**) in the **Publish Options** window.

Apply Crisis Management

To apply the Crisis Management mApp Solution file, perform the following steps:

Download the .zip file, which includes the following:

- Crisis Management.mApp file
- CrisisManagementmAppDocumentation.pdf

To apply the mApp Solution, perform the following high-level steps:

1. Download the Crisis Management.zip file.
2. Extract the contents of the .zip file to a location that is accessible to CSM.
3. Apply the mApp using the Apply mApp Wizard in CSM Administrator.
4. On the **How automatic should the merge process be?** window of the Apply mApp Wizard, select either **Ask me about every decision** or **Make reasonable decisions, but ask me if unsure**.
5. Save and publish the mApp file.

Known Issue

A known platform issue exists when applying a mApp Solution that includes a Business Object with both Default and Portal Default View forms. This issue causes the Portal Default forms to be added to the Default View erroneously.

As a workaround, follow these steps:

1. At the end of Apply mApp Wizard, select **Open a blueprint so that I can preview the changes**.
2. Select **File > Blueprint changes** and expand the section for the Crisis Business Object.
3. Expand the list of forms and remove the duplicate **view-only** or **edit-existing** forms that do not say **(Portal Default view)** after them.
4. Publish the Blueprint.
   Now the duplicate forms no longer appear in the Default view.

Configure Crisis Management

Use CSM Administrator and CSM Desktop/Browser Client to configure Remote Employee Management. Configuration tasks include:

- Configure Security Groups
- Configure Teams
- Configure Sites
- Additional Configuration

Configure Security Groups

Two security groups are included in the Crisis Management mApp Solution. Due to the sensitive nature of information that could be provided by employees during a crisis self-reporting solution, restrictions should be placed on visibility of that information to ensure compliance with HIPPA guidelines.

Follow these steps:

1. Open CSM Administrator.
2. Select the **Security** category.
3. Select **Edit security groups** in the task list.
4. From the **Group** drop-down list, select **Crisis Management.** Crisis Management allows View, Add, and Edit rights for the Crisis and Employee Crisis Response Business Objects.
5. Select the **Users** tab.
6. Select the **Add** button to add users to the Crisis Management Security Group.
7. **Important:** Open all existing Security Groups in your database and remove rights for the Crisis and Employee Crisis Response Business Objects. This ensures the information is only available to those in the Crisis Management Security Group.
8. Update the Portal Customer Security Group**.**

   Recommendation: Use the provided **Portal Customer Suggested Crisis Object Rights** Security Group as an example for how you can configure higher security for Security Group users who are not directly responsible for managing the crisis (select **Portal Customer Suggested Crisis Object Rights** from the **Group** drop-down list). This example Security Group is a copy of the default CSM Portal Customer Security Group, with added view-only rights for the Crisis Business Object and limited rights based on criteria for the Employee Crisis Response object and related objects.

   To ensure higher security, note the following Security Groups and associated Business Object Rights in the example **Portal Customer Suggested Crisis Object Rights** Security Group:

   Note: No changes are recommended for the Admin Security Group.

Business Object/Security Group	IT Service Manager and IT Service Desk Levels 1, 2, and 3	Crisis Management	Portal Workgroup Manager and Customer
Crisis	Recall, View	Final, Recall, View, Add, Edit	View
Crisis Status	Recall, View, Add, Edit	Recall, View, Add, Edit	View
Employee Crisis Response	Recall, View, Add, Edit	Recall, View, Add, Edit	View, Add

Crisis Employee Response Action	Recall, View, Add, Edit	Recall, View, Add, Edit	None
Crisis Type	Recall, View, Add, Edit	Recall, View, Add, Edit	None
Crisis Resource Position	Recall, View, Add, Edit	Recall, View, Add, Edit	None
Crisis Resource	Recall, View, Add, Edit	Recall, View, Add, Edit	None
Crisis Employee Response Status	Recall, View, Add, Edit	Recall, View, Add, Edit	View

9. Save your changes and exit the **Security Group** window.

Assign Users to Team

The Crisis Management mApp Solution includes a new Team named Crisis Management. Use it to assign a Team and Individual son Crisis records.

Follow these steps:

1. Open CSM Administrator.
2. Select the **Security** category.
3. Select **Edit teams and workgroups** from the task list.
4. In the **Teams and Workgroups** window, select the **Crisis Management** team under the **User teams** radio button.
5. Select the **Members** tab for the Team.
6. Select the **Add** button.
7. Select **Available users** from the list and select **OK** to close the **Add Team Member** window.
8. Save your changes and exit the **Teams and Workgroups** window.

Configure Sites

The Crisis Management mApp Solution includes a Site with suggestions for configuring your Customer Portal. Use this Site as a guide for incorporating the Crisis Management mApp Solution within your Portal.

Follow these steps:

1. Open CSM Administrator.
2. Select the **Browser and Mobile** category.
3. Select **Site Manager** from the task list.
4. Go to **Sites > System** and locate the **Suggested Menu Configuration for Crisis Management** Site.
5. Right-click the Site name and select **Edit**.
6. Take note of the following configurations for your own Portal Site:
    a. Under **General**, the **Crisis** Business Object is added to the **Associated Business Objects** list.
    a. Under **Menu**, take note of three new navigation options for **Crisis Response, Crises,** and **Employee Crisis Responses.**

       The **Crisis Response** menu item is configured to only show when the **Crisis Total Impacted** metric is greater than 0. This page allows Portal customers to view Announcements that are related to the Crisis domain and report their status.

The **Crises** and **Employee Crisis Responses** menu folders can be included if you want those users with rights to the Crisis and Employee Crisis Response objects to report on crises and check on responses from the Portal.

Additional Configuration

Update the following stored values:

- Crisis Hotline: Add the phone number for the crisis hotline. Used in email and Dashboards.
- Enable Daily Employee Response Reminder: Set to true to allow system-wide daily reminders for Employee Responses to be available.

Also, to update the mail monitor, copy the Employee Status monitor from the **Suggested Employee Status Monitor Included** E-mail Event Monitor to your active monitor.

Business Objects and Associated Items

Crisis Object

New Team: Crisis Management

Security: New Crisis Management Security Group: a new security group with rights to manage crises and view/update employee responses.

New Object: Crisis is a new Major Business Object for tracking key crisis information and initiating core communications.

Status values: Warning, Risk Assessment, Response, Management, Resolution, Recovery, Completed

Tabs:

Overview: Title, Reported By, Crisis Type, Crisis Team Manager and Team assignment, Declared/End Dates, Description, Notification List

Resources: Add representatives from the key business areas to be part of the virtual Crisis Management Team. Uses the Customer-Internal table.

Activity: Regular journal tracking.

Employee Crisis Responses: Automatically links the employee response records. One record is created for every customer with an email address and a status of Active. These records are updated through the Portal or email response.

Affected Sites: Manually link the affected Sites.

Tasks: Work Item: Create tasks for work during the crisis lifecycle.

Actions:

- Assign to Me
- Send Manual Update Email: A free-form email template that is sent to everyone on the default notification list.
- Recalculate Check-in Totals: Updates the total status numbers in the record header.
- Start Employee Response Process: Initiates the creation of the employee response records and sends an email to notify employees of the process and allow them to check in. This link is disabled after running the processes.
- Automatically Request Employee Status Updates**: I**nitiates the daily emails asking employees to check in
- Stop Request for Employee Status Updates: Discontinues the daily check-in email process.

Employee Crisis Response Object

Employee Crisis Records are created from the **Start Employee Response Process** process and updated from the check-in process.

Security:

Security on Employee Crisis Response objects: Restrict view, add, and update to only the Crisis Management team.

New Object: Employee Crisis Response is a new Major Business Object that tracks employee check-ins and associated Crisis Management actions.

Fields:

- Crisis Title (from the associated Crisis Record). Auto populated.
- Employee Name (auto populated)

Status: Shows the last check-In status and the date/time.

Actions:

- Take Management Action: This action is associated with the need to take action for employees who check-in with a **Not Ok** status or have not reported in the last 72 hours. These are tracked/appended in the **Notes** area.
- Add Check-In: This manual action is taken by the Crisis Management Team to provide the current status of an employee. This action updates the last checked-in date/time.

Process: Create a new Crisis record with the relevant information (Add Resources, Affected Sites, and Tasks to support the crisis management process). One of the key functions of this new object is to initiate and track employee communications. The following Actions initiate the ongoing employee communication process:

- Start Employee Response Process: Automation does the following:
    - Creates an Employee Response record for all active employees with an email address in the Customer-Internal table.
    - Sends an email to active employees with information about how the process will proceed and explain the importance of employee check ins.
- Daily emails are sent to each of these employees with a slightly different email format. This daily process continues until the Crisis Management team turns off the notifications (One-Step Action).
- Ad-hoc emails as appropriate from the Crisis Management Team.

Initially, an employee will receive a message from the Crisis Management Team that an urgent situation has been identified that will have a direct impact on the employee community. Additional information is provided, as needed. This initial email also contains an employee check-in link with additional instructions for accessing the Portal.

The response is captured in the employee's Employee Crisis Response record, which includes their status (**OK**, **Not Ok**) plus any additional information provided. Additional processes are initiated based on the response (or lack of a response):

- If **Ok**, no crisis team action is needed. Green displays on the Employee Crisis Response grid on the crisis record.
- If **Not Ok**, red appears in the Employee Crisis Response grid on the crisis record. Additionally:

    - An email is sent to the Crisis Management team indicating that an employee has checked in with a **Not Ok** status.
    - The Employee Crisis Response record is also marked to indicate that Crisis Management action is needed.
    - The Crisis Management team contacts the employee to determine next steps needed and when a manual check-in warrants a change of status to **Ok**.
- If **Unreported**, black appears in the Employee Crisis Response grid on the crisis record.
- If the Employee Crisis Response record last check-in date is over 72 hours, a **Crisis Management Action Needed** flag is set and the record appears on the Crisis Management Dashboard to be reviewed by the Crisis Management team.

Announcements

A new Crisis domain has been added so that Announcements can be filtered for viewing on the Crisis Management Portal Dashboard.

Portal

A new menu bar is available to allow easy access to the crisis landing page without interfering with the customer Home page. Employees can report their status on this new page and view the crisis announcements.

Portal Default Security Group: An example Security Group with suggested configuration of rights for Portal customers to view and edit their own Employee Responses and view crises.

Email Notifications

Notifications include:

- Initial email to notify employees about the Crisis Team and the check-in process (includes the initial check-in)
- Daily emails asking for a status check-in
- Notification that the check-in response was received
- Notification to the Crisis Management team when an employee status is **Not OK**
- Ad-hoc email sent from the crisis record