

Visual Intercept Notification Services

When managing an incident from conception to completion, it becomes imperative that all those who are involved in the incident life-cycle be kept up-to-date on changes to the incident. Users should be notified on changes of status, priority, or if additional information is needed. To insure that this happens, Visual intercept Enterprise includes a Notification Service that delivers email notifications to those users specified as being part of an incidents life-cycle.

To receive Visual Intercept notifications the following elements must be in place:

1. [The service must be installed and configured.](#)
2. [Notification rules must be configured.](#)
3. [Contacts must be properly configured and associated with projects or incidents.](#)

Installing and configuring a new notification service

The Visual Intercept notification service is installed as part of the server setup process. This Windows NT service is accessed and configured through the Visual Intercept Services application.

To install and configure a new notification service:

1. From the Visual Intercept Enterprise Programs group, launch the Visual Intercept Services application
2. Select the Notification tab.
3. Click the Add button.
4. Logon to the Visual Intercept database for which you want to create a notification service.
5. On the resulting Notification configuration dialog select the Service tab.
6. Enter an appropriate service name that would show up in the Control Panel Services list. This defaults to the data source name.
7. Enter the Visual Intercept userID and password values that the service will use to connect to the Visual Intercept database. The notification service is governed by the same security as other users, so the UserID should not have restricted rights.
8. Enter a local or domain account with password under the Service group if the local system account does not have necessary privileges to create and run a service on the server.
9. Select the Notification Options tab.
10. Enter the interval on which the notification service operates. Notifications will be processed on this interval. This value should range from 5 seconds to 120 seconds depending on your database and mail server.
11. Select the Suppress Internal Notification option unless you are using the Visual Intercept Desktop internal notification mechanism. This option is for environments that do not have an SMTP server available for email notifications.
12. Select the Enable E-mail Notification option if you are sending email notifications through an SMTP server.
13. Enter the SMTP server address to send email notifications through.
14. Enter the fully qualified path to the notification template file used for this notification service. By default, a template file named isnotesv.tpl is installed in the primary Visual Intercept installation directory.
15. Enter the administrator address that will be used as the default From: email address for notifications originating where a valid from email address can not be determined.
16. Select the From Sender option to have the From: email address of a notification be that of the user who performed the action that generated the notification.
17. Click Apply and OK. The new service will appear in the service list of the Notification tab of the Visual Intercept Services dialog.

Configuring notification rules

A notification rule is a combination of events to monitor, such as change of status or priority, and a condition to evaluate. When a monitored incident property is changed, the condition is evaluated. If the condition is true, a notification is sent. If a notification rule is not specified when a contact, contact type, or contact variable is attached to an incident or project no notifications will be sent.

Visual Intercept ships with several standard notification rules and custom notification rules can be created using the Visual Intercept Notification Builder.

Configuring contact relationships

Visual Intercept notifications are sent to contacts that are related to incidents or projects with a notification rule. Contacts can be related to an incident or project as a specific contact, contact type, or a contact variable. Additionally, contacts can be indirectly related to incidents or projects through the project hierarchy. When a notification event occurs, such as a change in status of an incident, the notification service determines which contacts are related to the incident and evaluates the associated rule for each contact. If an associated contacts' notification rule evaluates to true, then a notification is sent to the contacts email address.

Assuming a notification rule of OnChangeStatus which evaluates to true when the incident status has changed from any value and a contact with a contact type "Programmer", the contact will be notified as the incident status changes when:

1. The contact is directly associated to an incident with the OnChangeStatus rule.
2. The contact type "Programmer" is directly associated to an incident with the OnChangeStatus rule.
3. The contact is directly associated to a project who parents the incident directly or indirectly with the OnChangeStatus rule.
4. The contact type "Programmer" is directly associated to a project who parents the incident directly or indirectly with the OnChangeStatus rule.
5. The contact userID is the AssignID, RequestID, QAID, Project LeadID, or QA LeadID of the incident and the corresponding contact variable is directly associated to an incident with the OnChangeStatus rule.
6. The contact userID is the AssignID, RequestID, QAID, Project LeadID, or QA LeadID of the incident and the corresponding contact variable is directly associated to a project who parents the incident directly or indirectly with the OnChangeStatus rule.

Given this mechanism for sending out notifications, you must be sure that each contact document contains a valid email address. If the associated Contact document does not contain an email address Visual Intercept notifications will not be sent.

Tip: *When you first set up your notification rules you may want to start by setting of notification rules at the root-level project. Because child projects inherit the rules applied to parent projects, this set of rules will apply to incidents registered against any project in the database. Once you have a set of rules you would like to apply to all projects, you can further refine the notification schedule by creating new rules for other projects and individual incidents.*

If you have other questions about issues not included in or beyond the scope of this Tech Tip, please contact Elsinore Technical Support Services at support@elsitech.com or 866.866.0034, option 2.