Quest

Quest® InTrust 11.4.2

Real-Time Monitoring Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

InTrust Real-Time Monitoring Guide
Updated - September 2020
Version - 11.4.2

Contents

Real-Time Monitoring Overview

The real-time monitoring service constantly listens for new events. This enables you to stay up to date on the state of critical objects in your network. This feature also provides automated response to events that occur in the network.

You activate a real-time monitoring policy that prescribes what monitoring rules must be applied to what InTrust sites. A monitoring rule specifies, in particular:

- The audit trail (event log, Syslog and so on) to be monitored
  These are known to rules as data sources
- Conditions against which event records must be evaluated
  These are the rule matching parameters
- What to do when the rule is matched
  Whether to generate an alert, send a notification, or perform a response action

For example, the “InTrust: Tracking log monitoring” policy is intended for monitoring of critical events from all the InTrust servers in the organization, and prescribes to process them using the “InTrust Log Monitoring” rule group.

The agent tracks audit trails on the target computer, looking for new events. If an event matches the conditions specified by a monitoring rule, then (in accordance with the rule settings), the following takes place:

- An alert is generated
- A response action is performed
- People in charge get notified of the occurrence and can take measures to resolve the issue

Alerts can be stored in the alert database, and authorized users can view and resolve them via Monitoring Console. In addition, you can configure reporting jobs to create reports on the alerts data.

Alerting and notification provide feedback on real-time monitoring. Each of these actions is initiated when specific events are detected.

Alerting

Alerting is a service that generates alerts. An alert is a signal that InTrust has detected a condition described by a rule. Alerts can be stored in an InTrust alert database. You can view the stored alerts with InTrust Real-Time Monitoring Console.

To view an alert, an account must be a member of Security group for both the rule group containing the rule that triggers the alert and for the site that the rule monitors. This is because rules, through policies, are bound to sites.

- To specify Security group members for a site, open the site's properties dialog box and click the **Security** tab.
- As for the rules, you must specify Security group members for the entire rule group. To do so, open the rule group's properties dialog box and select the **Security** tab.

You must also configure the following:

- Alert database
- Settings for the corresponding rules

An alert database is created automatically during InTrust setup. This database is used by default for storing alert records.

To use another alert database

1. In InTrust Manager, double-click **Configuration | Data Stores**.
2. Right-click **Databases** and select **New** from the shortcut menu to create the new alert database with the New Database Wizard.
3. Double-click **Configuration | InTrust Servers**.
4. Right-click the InTrust server you need, and select **Properties**.
5. Select the **Alert Database** tab.
6. Click the button next to the name of the alert database to open the Select Storage dialog box.
7. In the dialog box, select the database you need.

To access a rule's alert-related settings, open the properties dialog box of the corresponding rule, and select the **Alert** tab. For details, see the Understanding Rules topic.

Notification

Notification means creating messages (for example, email messages) and sending these messages to specified recipients. Notification is activated when specified events are detected during real-time monitoring. In addition to fixed text, messages can contain data included dynamically as messages are created.

To configure real-time notification, you should define the following:

1. Settings for the corresponding policies (see Understanding Real-Time Monitoring Policies for details)
2. Individual recipients or notification groups
3. Notification methods
4. Outgoing SMTP server (only required for email messages)
5. Settings for the corresponding rules

NOTE: Associate your recipient objects with people who are qualified to receive notifications about incidents.

Messages can be addressed to individual recipients or to notification groups into which recipients are organized. For detailed information about notification groups, see Notification Groups below.

Before you select email as the policy's notification method, ensure that an outgoing SMTP server is specified for the InTrust server that performs real-time monitoring.

To assign an SMTP server

1. Double-click **Configuration | InTrust Servers** in the treeview.
2. Right-click the server and select **Properties**.
3. Select the **Notification Parameters** tab. Specify the outgoing SMTP server in the corresponding edit box.

For notification-related settings of the rule, open rule properties and go to the **Notifications** tab.

Message Templates

Real-time notification messages are based on templates. To create a template, open a rule's properties dialog box, click the **Notifications** tab, and click **Add**. To edit an existing template, highlight it and click **Properties**.

Data from the live network can be included in notification messages. To achieve this, use special keywords in message templates to represent the values in audit trail fields.

You can insert keywords in the subject and in the body of the template. Use variable names delimited by two "%" signs, for example **%EventID%**. These variable names are substituted with values retrieved from audit trails when notification messages are generated. The rest of the message text that you specify is left unchanged.

Notification Groups

Notification groups list personnel who can receive notification messages when monitoring process is going on.

To create a notification group

1. Double-click **Configuration | Notifications | Notification Groups**.
2. Right-click **Notification Groups** and select **New Notification Group** from the shortcut menu to start the New Notification Group Wizard.

A notification group is populated with recipient accounts.

To configure a new recipient

1. Double-click **Configuration | Notifications**.
2. Right-click **Recipients** and select **New Operator** from the shortcut menu. A new recipient is created.
3. On the **General** tab of the properties dialog box, specify the address of the recipient.
4. Go to the Member of tab and specify what notification groups the recipient belongs to.

To populate an existing notification group

1. Open the notification group's properties dialog box.
2. Click the **Members** tab, and select the member recipients.

Understanding Rules

Rules are grouped settings that control event analysis and response to events. The content of alerts and notification messages is also defined by rules. Rules can be activated and deactivated according to schedule.

Rule settings define conditions that are evaluated as regular audit trail checks take place. The process of condition evaluation is called matching. If a rule is matched, real-time monitoring can notify a recipient, generate an alert and/or perform response actions.

> **NOTE:** Matching can be performed on the server side or on the agent side. If the agent does the matching, this helps to reduce traffic between the server and the agent. However, when you need to analyze data coming from multiple site objects (for example, failed logons from several domain controllers), you should perform matching on the server side.

Monitoring rules are logically united into rule groups. If you need a new rule, you can create it within existing group, or create a new group and then create a new rule in it.

To create a rule group, in InTrust Manager, right-click **Real–Time Monitoring | Rules** and select **New Group**.

To create a rule, right–click a group of rules, select **New Rule** and follow the New Rule Wizard.

The rule settings you have to specify when creating or modifying a rule are discussed below in this topic and in the following topics:

- Data Sources
- Matching
- Alerts
- Response Actions
- Notification
- Knowledge Base

To access the settings, right–click a rule and select **Properties**.

Types of Rules

When you create a rule using the New Rule Wizard, you are offered the following rule type choices:

- Single event
- Correlated events
- Events threshold
- Missing event

- Paired missing event
- Custom rule

These options define how detection of the necessary events works. The following table helps decide which rule type works best for you in which circumstances:

Rule type	Matching occurs when...	Use such rules when…
Single event	A single event with specified data is detected.	A single event indicates a situation that needs resolution and interference.
Correlated events	The InTrust agent detects a custom pattern among the audit data that it processes.	You need to detect a very specific situation, and define it in terms of event data that comes about around the same time.
Events threshold	The number of events with specified data exceeds the threshold value you define.	The threshold value is the number of events within the specified amount of time. You want to detect situations when similar actions are done in rapid succession. For example, such event patterns often indicate automated brute-force activity.
Missing event	An event with specified data is expected, but fails to occur within the period of time you define.	You expect specific events within a particular timeframe or on a regular basis. Failure to detect such an event means that something you expected did not occur.
Paired missing event	A specific event occurs, and another specific event is expected after it, but the second event fails to occur within the specified time interval.	You need to watch out for situations where actions that are normally two-part fail to get to the second stage.
Custom rule	The rule's underlying script evaluates to true.	You want to detect a situation that cannot be defined using any of the previous rule types. For details about using custom rules, see Customization Kit.

The “Correlated events” rule type is complex, and it is explained in more detail in the following section.

Rules that Correlate Events

Rules of the “Correlated events” type are the most advanced rules you can configure without having to write script code. With these rules, you can do the following in real time:

- Look at data from any available audit trails with the same data source type
- Find and compare specific data in specific event fields
- If necessary, expect this data in specific order

The following sections explain how to create or configure such a rule with the New Rule Wizard.

Defining Events

On the Specify Events step, define all events to be checked. An event is defined by its event ID and, optionally, a set of field values that must be found in it.

All the events you need must be in the Events list on this step. You can do the following with the list:

- Add event definitions from the Event Viewer snap-in
- Add custom-defined events by explicitly specifying the properties they must have
- Remove event definitions
- Edit existing event definitions
- Change the expected order of events or select to capture them in any order

To use Event Viewer

1. Click **Add | From Event Viewer** on the Specify Events step.
2. In the Event Viewer snap-in, right-click a suitable event and select **All Tasks | Add to InTrust rule**.
3. In the Add Events to InTrust Rule dialog box that opens, select which fields in the event definition must have the same values as the fields in your example event.

To add a custom event definition

1. Click **Add | Custom Event** on the Specify Events step.
2. In the New/Edit Event dialog box that opens, provide information about the expected event:
    - Data source (the audit trail that the event comes from)
    - Values of specific event fields
    - Name of the event definition

To edit any event definition in the Events list (whether added through Event Viewer or manually), select its entry and click Edit. This opens the New/Edit Event dialog box for the selected event definition.

Setting the Order of Events

On the Specify Events step, you can also tell InTrust to expect the events in a specific order or in any order. To set a particular order, use the arrow buttons next to the **Events** list, which move selected entries up and down the list.

The **Any order** option controls whether this order is taken into account. If it is selected, the events in the list can come in any order. If the option is not selected, the listed events are expected strictly in top-to-bottom order.

Configuring Dependencies

On the Specify Event Field Dependencies step, define the relationships between the values of different fields in different events—whether one should be the same as another, not the same, greater, less, and so on.

An important option that affects whether or not the rule is matched is the **This event can be included in multiple alerts** check box in the New/Edit Event dialog box. If this option is enabled for an event, the event's fields are compared to fields in incoming events until the timeframe expires, and the comparison does not stop if a match is found. If the option is disabled, and a match is found, the event is not considered any more until the same event occurs again.

Configuring the Time Interval

On the Select Timeframe step, specify the time interval within which this entire state must occur.

Example

The predefined “Windows/AD Security | Detecting Common Attacks | Gaining Administrative Rights | Suspicious activity under temporary administrative membership” rule is of the “Correlated Events” type. If you want to analyze what makes up such a rule, you can use it as an example. For that, open the properties of the rule and, on the **Matching** tab, click **Edit**.

Here is the summary of this rule as it appears in the Edit Rule Matching Parameters Wizard:

```
You chose to correlate the events:

User Added to Local Group (Windows Security Log, Event ID = 636, ...)

User Logged On (Windows Security Log, Event ID = 528, ...)

User Removed from Local Group (Windows Security Log, Event ID = 637, ...)

Where

User Added to Local Group.String10 = User Logged On.String1

User Added to Local Group.String11 = User Logged On.String2

User Logged On.String1 = User Removed from Local Group.String10

User Logged On.String2 = User Removed from Local Group.String11

This happens within

30 minutes
```

This information reflects the following:

1. The three Security log events added on the Specify Events step.
2. The correspondence between events as defined on the Specify Event Field Dependencies step.
3. The 30-minute timeframe set on the Select timeframe step.

The following settings are omitted from the summary, but are important for the rule:

1. In the “User Removed from Local Group” and “User Added to Local Group” events, the rule looks at insertion string 3 to make sure it is “Administrators”. This is the local group whose membership is watched.
2. The Any order option is disabled for the rule, so the events are caught in the order that they occur.
3. The This event can be included in multiple alerts option is disabled for all three events.

Rule Activity Time

This is the period or periods when the rule is in effect. Select the **General** tab and click **Configure Activity Time** to bring up the corresponding dialog box.

To configure rule activity time

1. Click a cell and drag the cursor to select an area.
2. Click Activate to activate the rule at the times specified by the selected area.

3. Click Deactivate to deactivate the rule during the selected period.

Enabling the Rule

To enable the rule, in its properties dialog box click on the **General** tab and select **Enable**.

> **NOTE:** Predefined rules are all disabled by default. To activate real-time monitoring, enable the rules you need and the policies they are associated with.

Data Sources

Data sources specify the audit trails that provide the event data. You can configure this setting on the **Data Sources** tab of the rule's properties.

It is recommended that you use only one data source per rule to avoid event filtering issues.

Matching

Matching conditions define what events to look for. As you create a rule, the New Rule Wizard offers you several templates on which matching will be based. You can use any of the following:

- Single Event
- Correlated Events
- Events Threshold
- Missing Event
- Paired Missing Event
- Custom

Also, you can configure an event filter, and specify values for matching parameters.

The rule's matching settings are displayed on the **Matching** tab:

- Parameters to be used when matching is performed
- Agent-side or server-side matching

You may need to configure matching parameters for certain rules, for example, handling unauthorized administrative actions. For instance, you can examine the "Group member added by unauthorized personnel" rule from the "Windows/AD Security | Administrative activity | Account management" rule group. Here you have to define authorized users and groups. These are users and groups who are allowed to perform administrative actions—so, for them the rule should make exceptions: no match will be registered when an authorized user or member of an authorized group performs the action that the rule watches out for.

Click **Edit** to edit the parameter values. You can also edit matching parameters for the entire rule in XML by clicking **Advanced**.

> **NOTE:**This option is intended only for advanced users. It can be used to change any aspect of rule matching. Also, this is the only way to configure matching conditions for a rule based on the "Custom" template.

As you can see, both parameters in this example are lists, but they are specified differently:

- When specifying authorized users in this rule, you can supply wildcards, as well as for any other rule parameter defined with the tag containing **wi**. For example, specifying ***\admin** is acceptable in a list of authorized users.
- On the contrary, authorized group names in this rule must not contain wildcards, and neither must any other rule parameter defined with the tag containing **member_of**. So, if you need to include groups with uniform names from multiple domains, you can supply just the name, as in **admins**, or the following: **.\admins**.

NOTE: When specifying parameters, note that quotation mark or backslash character must be preceded by the backslash escape character, for example: **\"c:\\windows\\\"**

Alerts

Alert settings define whether an alert is sent to an alert database when the rule is matched. Use the **Alert** tab in the rule's properties to configure the corresponding settings:

- Select the **Store the alert in alert database** option if you want to keep the alert and make it viewable in Monitoring Console.
- Click **Define Custom Fields** to add your own fields to the alerts that are generated when the rule is matched.
- Click **Alert Suppression** to specify whether to suppress duplicate alerts and define what alerts are considered duplicates. Suppressing an alert means adding it to a list of similar alerts rather than considering it a separate alert. When you use Monitoring Console to view alerts, you can see suppressed alerts where the alert counter is greater than 1.

Also, you can supply alert name and description, initial state, comment and alert code.

Using Named Fields in Alerts

In addition to predefined fields, your alerts can include any named fields that InTrust can calculate based on the events it captures. The following are examples of such fields:

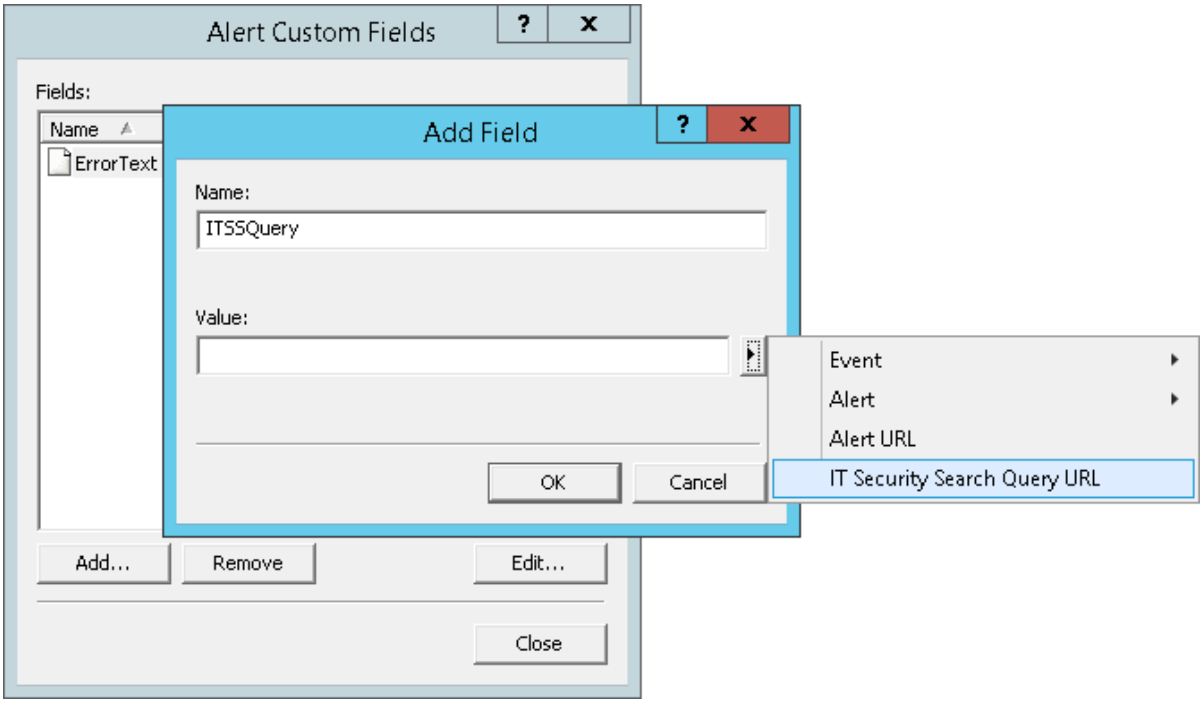
- Who
- What
- Where
- When
- Where From
- WhoDomain
- Whom

To use such a field as a variable, enclose it in percent signs (and omit whitespace); for example, **%Who%** or **%WhereFrom%**. There are numerous named fields defined for InTrust, and the set of such fields can vary from environment to environment.

Some of these fields are available from the field selection menu in the alert editor.

Providing IT Security Search URLs in Alerts

You can include relevant IT Security Search query URLs in alerts triggered by your rules. When the alert-handling user opens such a URL, they get the event that triggered the alert and also the context for that event: similar events shortly before and after the event. If you want to include such URLs in alerts, create a custom field for the query in the alert editor and use the **IT Security Search Query URL** command to set the field's value.



If InTrust doesn't know where IT Security Search is located at the time that you click this item, you will be prompted for the IT Security Search URL. Make sure you get the address right. If you need to change it later, you have to edit the **ITSearchAddress** organization parameter. For details, see Organization Parameter Editor.

Response Actions

A response action defines what measures are taken if certain rules are matched. Response actions can do the following:

- Execute scripts
- Send SNMP traps
- Execute commands
- Enforce audit policies
- Run InTrust tasks

Click the **Response Actions** tab in a rule's properties to configure the corresponding settings.

Response actions can follow one another. When you provide several response actions, they are executed in the order they are arranged.

For all response action types except “Execute Task”, you can specify whether the action is executed by the server or by the agent. To do it, open the response action’s properties dialog box and click the **General** tab. To

configure settings that are specific to each response action, click the **Settings** tab. These settings are described below.

If a response action setting relies on an external value, you can specify a predefined keyword that represents the value. These keywords are resolved when the rule is matched, the resulting event data is used to resolve the keywords, and the response action uses the values.

Execute Script

As a response action, InTrust can run one of the scripts available in the **Configuration | Scripts** container in InTrust Manager. The supported scripting languages are PowerShell, ECMAScript, JScript and VBScript.

NOTE: To execute PowerShell scripts, InTrust runs the 64-bit version of PowerShell, because this is the version mainly in use today.

InTrust provides several predefined scripts. These scripts assist in administrative tasks, such as adding a user to a group or changing the type of an account. If necessary, you can create your own scripts from scratch or as a modified copy of an predefined script.

To configure a response action that involves script execution

1. Open the properties dialog box of the corresponding rule.
2. Click the **Response Action** tab, and click **Add**. The Select Response Action Type dialog appears.
3. Select **Execute script** from the list and click **OK** to start the New Response Action Wizard. Select the script to be executed.

Each script has parameters that can be customized so that the script fits a particular situation. By specifying these parameters you define how the script is applied and what it is applied to. For example, the parameters for the **AddUserToGroup** script include Computer, Group, Protocol and User.

To edit a parameter

1. Select the parameter and click **Edit**.
2. Specify a value.

For details about setting up scripts for use in response actions, see InTrust Script Objects in InTrust Customization Kit.

Send SNMP Trap

To configure a response action that involves sending an SNMP trap

1. Open the properties dialog box of the corresponding rule.
2. Select the **Response Action** tab, and click **Add**. The Select Response Action Type dialog box appears.
3. Select **Send SNMP trap** from the menu. The properties dialog box is displayed.

4. On the **Settings** tab of the dialog box, specify the following parameters:

    - Address
      This is the network address of the recipient of the trap.
    - Community
      This is the SNMP community that will receive the SNMP trap.
    - Trap type
      This is a one of the standard trap types as defined in RFC 1157.
    - Specific type
      This is a specific trap type.
    - Parameters
      This is a list of OIDs and values that you consider relevant and need to include in the trap.

You can specify keywords for all the listed settings except the OIDs and value types in the list of parameters. Make sure that the value for which you want to use a keyword is the correct type. Otherwise, the SNMP trap is not sent.

NOTE: InTrust supports only SNMPv1 for this type of response action.

Execute Command

To configure a response action that executes a command file

1. Select the **Response Action** tab, and click **Add**. The Select Response Action Type dialog box appears.
2. Select **Execute command** from the menu. The properties dialog box is displayed.
3. On the **Settings** tab of the dialog box, specify the following parameters:

    - The folder in which the command file will be executed
    - The path to the command file
    - Trap type
      This is a one of the standard trap types as defined in RFC 1157.
    - Any parameters that the command file requires
    - Whether command file execution will be synchronous—that is, whether InTrust should wait for the end of command file execution before proceeding to the next response action in line (provided one is present)

You can specify alert and event field names for the first three settings. Make sure that the field names you specify make sense as value settings.

Set Audit Policy

Audit policy enforcement may be an appropriate response action in many situations. For example, if an abnormal event occurs in your network, it may indicate that you are overlooking related events with your current audit policy. This response action enables you to automatically apply an audit policy that is most suitable under the circumstances.

To configure a response action that enforces a specified audit policy

1. Select the **Response Action** tab, and click **Add**. The Select Response Action Type dialog box appears.
2. Select **Set audit policy** from the menu.
3. Specify the audit policy you want to be applied by the response action. Select **Turn off audit** to stop all auditing activity for the listed events, or select **Audit these events** to specify the events to be audited. You can set auditing for successful and failed events. The options are as follows:
    - Use current settings (meaning, preserve the settings that are in effect during rule matching)
    - Audit
    - Do not audit

Notification

Notification settings, located on the **Notification** tab of a rule's properties, define:

- What messages will be sent to recipients
- What notification method will be used

Recipient is a role you assign to users to let them receive notification messages (usually, these are persons in charge for security issues resolution). To get a list of recipients, you can expand the **Notifications** node in InTrust Manager.

Add message templates, and select the type of each message.

You can add predefined fields to the text of the message template. These fields are replaced by corresponding data when a message is created. The recipientss specified by the policy receive these messages.

Using Named Fields in Notification Messages

In addition to predefined fields, your message templates can include any named fields that InTrust can calculate based on the events it captures. The following are examples of such fields:

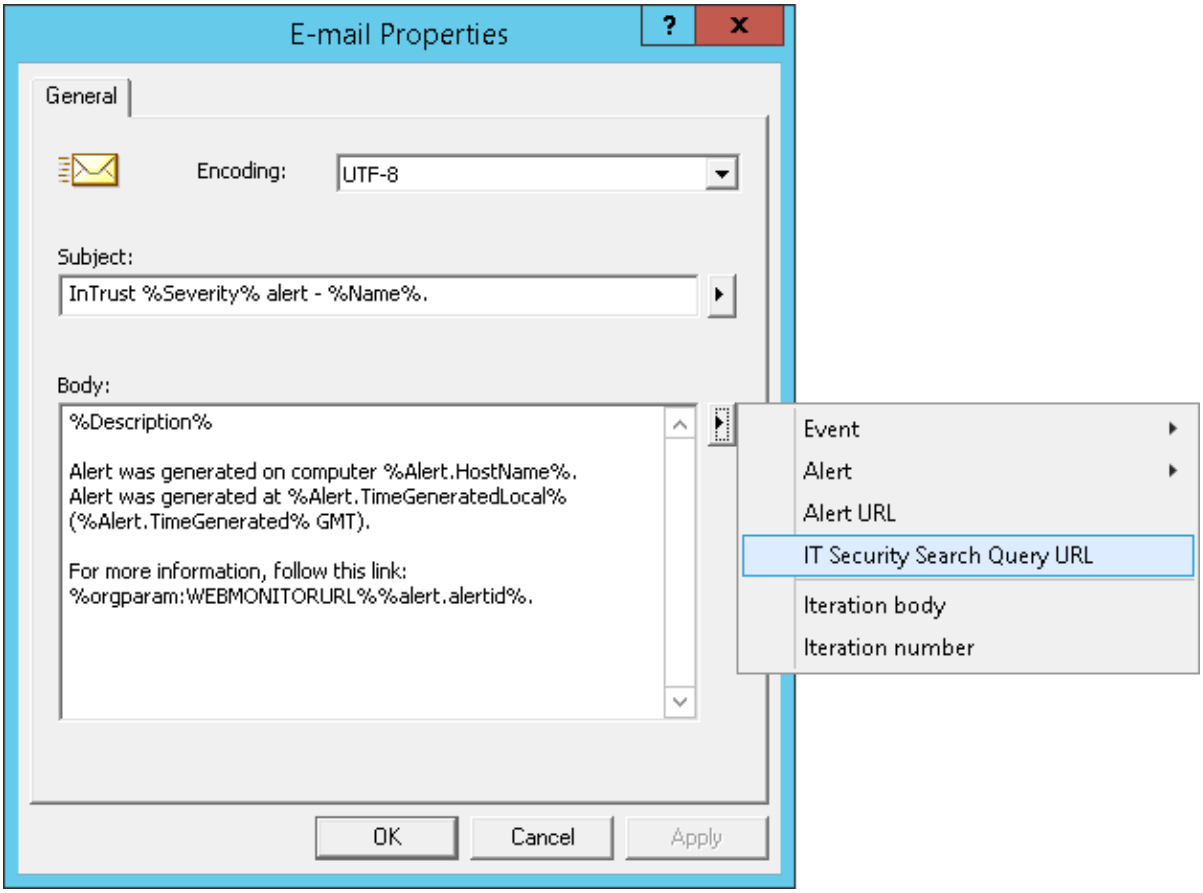
- Who
- What
- Where
- When
- Where From
- WhoDomain
- Whom

To use such a field as a variable, enclose it in percent signs (and omit whitespace); for example, **%Who%** or **%WhereFrom%**. There are numerous named fields defined for InTrust, and the set of such fields can vary from environment to environment.

Some of these fields are available from the field selection menu in the message template editor.

Providing IT Security Search URLs in Email

You can include relevant IT Security Search query URLs in notification messages that your recipients get. When a recipient opens such a URL, they get the event that triggered the alert and also the context for that event: similar events shortly before and after it. To include such links in notification messages, use the **IT Security Search Query URL** command in the message template editor.



If InTrust doesn't know where IT Security Search is located at the time that you click this item, you will be prompted for the IT Security Search URL. Make sure you get the address right. If you need to change it later, you have to edit the **ITSearchAddress** organization parameter. For details, see Organization Parameter Editor.

Knowledge Base

The **Knowledge Base** tab in the properties of a rule contains the articles explaining the situation in which the rule is triggered, and possible reasons of the problem. Each rule is shipped with a Vendor Knowledge Base Article; to add your company's expertise to the rule, use the Custom Knowledge Base Article field.

NOTE: If the role-based administration feature is enabled, a user can edit the Knowledge Base (for example, add a Custom Knowledge Base Article to a rule) only if the user account has the **Modify** permission on that rule. This can be done on the **Security** tab. For details, refer to the Role-Based Administration of InTrust topic.

Understanding Real-Time Monitoring Policies

Real-time monitoring policies are essentially different from gathering policies (explained in Understanding Policies): they maintain rule and site dependencies, and handle notification.

When you create a monitoring policy, you bind rules to sites and define notification message recipients. By default, real-time monitoring policies are disabled. Enable policies manually.

To create a real-time monitoring policy

1. In InTrust Manager, right-click Real-Time Monitoring | Policies, and select **New Policy**.
2. Follow the New Policy Wizard.
3. On the final step of the wizard, activate the policy.

You can change monitoring policy settings using the policy's properties. The following is an overview of the settings that you can specify during real-time monitoring policy creation or for existing real-time monitoring policies.

Where the Policy Is Applied

The scope of the policy is defined by the sites that it is associated with, and it can be refined by applying an object filter to site members. In the properties of a policy, the sites are specified on the **Sites** tab and the filter on the **Filter** tab.

What Rules Are Associated

You can specify the set of rules for a policy by selecting individual rules or entire rule groups. In the properties of a policy, this is done on the **Rules** tab.

Who Is Notified about Rule Matches

Whenever a rule is matched, it generates notification messages of the types that are specified for that rule. A policy specifies who gets the messages. As long as the corresponding notification type is enabled for a rule, a message from that rule is sent to the recipients specified by the policy. For details, see Configuring Notification Groups and Recipients.

The following notification types are supported:

Notification type	Details
Email	In the properties of a real-time monitoring policy, this is configured on the **E-mail** tab. You can specify regular recipients, notification groups and dynamic operators.
Event Log	In the properties of a real-time monitoring policy, this is configured on the **Event Log** tab. You can specify only **Event Log Recipient**, which implements logging of rule match events. Using other recipients has no effect for this notification type. For details about **Event Log Recipient**, see Configuring Notification Groups and Recipients. Note that even though **Event Log Recipient** is not really a message addressee, you still need to enable it so that rules with the **Event Log** notification type can log their match events.

Who Has Access to Alerts

If you need to set up fine-grained access to the resulting alerts in Monitoring Console, you can do it on the **Alert security** tab in the properties of a policy. Specify Active Directory accounts and define alert permissions for them. This affects whether Monitoring Console lets these accounts view and resolve the alerts generated by the associated rules in the policy.

Handling Alerts

InTrust Real-Time Monitoring Console is a Web-based application that you can use to view and manage InTrust real-time alerts (stored in an InTrust alert database).

> **CAUTION: If you are using Monitoring Console installed on Microsoft IIS 6.0 or 7.0, make sure ASP extensions are allowed. Refer the documentation of your version of IIS for details about allowing extensions.**

Monitoring Console administrators control user access to the alerts by configuring *profiles*.

A profile defines which InTrust server provides the alert records a user can work with, and specifies other user preferences for Monitoring Console operation (such as language and display style). A user selects a profile and works with associated alert views. An alert view is a collection of settings that define alert choice and presentation.

Alert Security Settings

Alert records are available to users only if their accounts have sufficient privileges to view the alerts or change their state (for example, from New to Acknowledged, or from Acknowledged to Resolved).

By default, InTrust organization administrators (explained in the InTrust Organization Administrators topic) have all privileges for working with all alerts (Read and Change Alert State). If you cannot view the alerts you need, see the policy security settings.

To provide users with these rights, Alert Security settings should be configured in InTrust Manager in the following way:

1. In InTrust Manager, select **Real-Time Monitoring | Policies**.
2. Right-click the required policy that binds the rules you need to the InTrust sites you want to monitor, and select **Properties**.
3. Click the **Alert Security** tab, and configure access to alerts for user or group accounts, using the **Allow** and **Deny** options for the following privileges:
    - **Read**
      Allows users to view the alerts from the selected sites triggered by selected rules
    - **Change Alert State**
      Allows users to change alert status and add custom Knowledge Base articles to the alerts

Managing Profiles for Monitoring Console

Monitoring Console offers profiles to allow authorized users or groups work with the alerts they need. During InTrust suite setup, a default profile for Monitoring Console users is created automatically.

However, if Monitoring Console installation was not a part of InTrust suite setup (that is, Monitoring Console's own setup was used), no default profile is created, and you have to create it manually from the Monitoring Console Administration page.

> **CAUTION: To create or edit a profile, your user account should be granted an Administrator role for COM+ System Application on the computer where the Monitoring Console runs.**
>
> **To check if you have this role, open the Component Services MMC snap-in on the computer with Monitoring Console, and view the Computers | My Computer | COM+ Applications | System Application | Roles | Administrator | Users node.**

When configuring a profile, you are prompted for the Run As account. This account will be used to connect to the InTrust server responsible for alert generation. To ensure a proper connection and correct flow of the monitoring process, this account requires sufficient privileges. The minimal requirements are:

- Membership in **InTrust Alerting Admins**
- **Read** permission on monitoring-related items (policies, rules, rule groups, sites, data sources) from InTrust configuration – this can be set in each item's properties on the **Security** tab
- **Modify** permission on monitoring rules – this can be set in the rule properties on the **Security** tab; this is required for editing the Knowledge Base articles

> **CAUTION: Consider that the Run As account of the default profile is listed as an InTrust organization administrator, thus having all required privileges. New profiles with the Run As account listed as an InTrust organization administrator can be also created.**

To create a profile

1. Open the Monitoring Console Administration page, for example, from the Start menu.
2. Click **New** in the left pane to start the New Profile Wizard.
3. Supply the following:
    a. Profile name and optional description
    b. Path for quick access to this profile from your browser
    For example, if Monitoring Console is installed on the computer SERVER in the virtual directory **ITMonitoring**, then to access the profile with path Profile1, in the Address bar you should type **http://SERVER/ITMonitoring/Profile1**.
    c. Run As account to use when connecting to the InTrust server
    Depending on the user role in alerts handling process, this account should be an InTrust organization administrator. Alternatively, if you prefer more granularity in privilege assignment, the account should:
        - Be a member of the **InTrust Alerting Admins** group
        - Have at least **Read** access to monitoring policies, rule groups, sites, and data sources, and **Modify** access to rules for editing the Knowledge Base articles

4. Specify the InTrust server that provides alert records to this profile, and connection protocol information:
    a. TCP/IP and port
    b. Named Pipes and pipe name
    c. RPC and endpoint
5. When you select an InTrust server, the corresponding alert database is selected automatically. You only have to:
    a. Select the authentication method to use when connecting to the alert database: Windows authentication (with the credentials used for connecting to InTrust Server) or SQL Server authentication (specify access credentials here)

NOTES:

- Make sure the account used to connect to the Alert Database has been assigned the **dbo** role or the **InTrust Monitoring Console** role for this database. For details, see System Requirements.
- If you select to use SQL Server authentication, the Run As account should be included into local Administrators group on the computer where the Monitoring Console is installed.

    b. Supply the number of concurrent database connections to the alert database (note that actual number will be one more than specified in this field, due to the connection always used when recalculating alert statistics). If the connection rate is not enough to provide users with alerts they need in a timely manner, you can increase the number of connections.
    c. Configure the time interval for recalculating alert statistics; that is, how often to update statistics within the active views of users who utilize the profile at any moment (**Refresh alerts**).
6. Select:
    a. The working language that will be used for current profile
    b. The theme (display style)

You can also modify settings for existing profiles by selecting a profile from the list and opening the corresponding tabs.

For more details on working with the profiles, see the help topic for the Monitoring Console Administration page.

Creating Alert Views

After a new profile is configured, you can customize alert views for this profile in Monitoring Console. Monitoring Console can be opened from the Start menu.

To create a view

1. In Monitoring Console, click **New** to start the New Alert View Wizard.
2. Follow the wizard, selecting the rules and sites that you want to monitor, and specifying other settings. For details, see the Monitoring Console help.
3. After you finish the wizard, these preferences are saved as an alert view.

For an existing view, you can configure filters based on alert state and generation time in addition to the settings specified in the wizard.

Within a view, you can examine alert statistics, analyze the alerts in detail, or search for the alerts.

For more details, see the Monitoring Console help.

Sample Rule Configuration

The easiest way to configure real-time monitoring is to use predefined objects (making copies is recommended): sites, rules and policies.

To learn to watch out for activity that you are interested in, consider the following scenarios:

- Setting Up Monitoring for User Account Creation
- Setting Up Monitoring for Suspicious Processes
- Setting Up Monitoring for Suspicious PowerShell Activity

You can use them directly, adapt them to your own environment or make your own real-time monitoring configurations based on them.

Setting Up Monitoring for User Account Creation

In this scenario, let's assume you intend to monitor user account creation performed by unauthorized personnel, meaning:

- You want the monitoring to span your Active Directory domain.
- You want to be notified by email when account creation is detected.
- You do not want any automated response actions to be taken.

To achieve this, you must configure the following:

- A site that encompasses all Windows servers and workstations in the domain,
- A rule that defines the notification message and is matched when the specified event occurs,
- A policy that binds the site and the rule together, and specifies e-mail as the notification method.

All of the required elements are predefined in InTrust, so all you need to do is to make the copies of these objects and associate them with one another as follows:

1. In InTrust Manager, double-click **Configuration | Sites | Microsoft Windows Network**, and check that the following predefined sites exist:
    - All Windows servers in the domain
    - All Windows workstations in the domain

CAUTION: Populate your predefined sites with objects you need and confirm that the sites span objects reside in the right domain. (You can enumerate site objects by clicking Refresh on the site's Enumeration pane.)

2. Double-click **Real-Time Monitoring | Rules | Windows/AD Security | Administrative activity | Account management**, right-click the **User account created by unauthorized personnel** rule.
3. Select **Properties** from the rule's shortcut menu. Click the **Notifications** tab and check that an email message is listed. Edit the message if necessary, as described in the Message Templates section of the Notification topic.
4. Select the **Response Actions** tab, and clear the check boxes next to the response actions listed– response actions are disabled.
5. Click the **General** tab and select the **Enabled** option to activate the rule. After you close rule properties, commit the changes.
6. Double-click **Real-Time Monitoring | Policies**, right-click the **Windows/AD Security: Administrative Activity Monitoring** policy and select **Properties**.
7. Click the **Rules** tab. The **Administrative activity** rule group is specified in the list by default. This group includes the required rule. If you want to select just this rule rather than the entire group, open the group and select the rule.
8. Select the **E-mail** tab, and click **Add** to specify who will receive the messages. For detailed instructions, see the Notification Groups section of the Real-Time Monitoring Overview topic.
9. Select the **General** tab and select the **Activate** option. After you close the properties dialog box, commit the changes. The configuration is now finished; InTrust agents will be installed automatically to the site computers to execute the monitoring tasks.

You can modify such settings as alerting, response actions, rule activity time, or others at any time as necessary.

To create your own InTrust object (site, rule, policy and so on), copy the corresponding InTrust predefined object and edit this object according to your specific needs. InTrust treats all sites, rules and policies the same whether they are predefined or user-defined.

Setting Up Monitoring for Suspicious Processes

This scenario is based on a Security log event that was enhanced in Windows Server 2016 and Windows 10. It will not work on earlier Windows versions, which do not have the enhancement. It uses a rule that incorporates knowledge about the following indications of common attacks that involve Windows processes:

- When someone runs a program that is named to pose for a well-known system application such as **lsass.exe** or **svchost.exe**; the giveaway is that such an impostor program doesn't have the right creator process
- When a process is started from a location where no programs are normally run, such as the system **Fonts** folder or a temporary folder in a user profile
- When someone launches specialized command-line administrative software such as **vssadmin.exe**; such occurrences can mean a script is at work, because manual use of such programs is uncommon
- Specific keywords that command-line hacking tools customarily use, such as "sekurlsa:"; these checks are process-independent

To watch out for these threats, configure the following:

- A site that encompasses the Windows Server 2016 (or later) and Windows 10 computers that you want to monitor
- A rule that defines the notification message and is matched when the specified event occurs
- A policy that binds the site and the rule together, and specifies e-mail as the notification method

The rule and policy are predefined in InTrust. However, you'll need a new custom site. Take the following steps to get these objects ready and associate them with one another:

1. In InTrust Manager, create a new site under **Configuration | Sites | Microsoft Windows Network** and include in it all the computers relevant to your scenario.
2. Double-click **Real-Time Monitoring | Rules | Advanced Threat Protection | Windows/AD Suspicious Activity | Backdoors**, right-click the **Suspicious process was started (Security log on Windows 10 / Windows Server 2016 and later)** rule.
3. Select **Properties** from the rule's shortcut menu. Click the **Notifications** tab and check that an email message is listed. Edit the message if necessary, as described in the *Message Templates* section of the Notification topic.
4. If you want InTrust to additionally log an event whenever the rule is matched, add **Event Log** to the list. For details about logging of rule match events, see Configuring Notification Groups and Recipients and Example: Emulating InTrust Real-Time Alerts in SIEM.
5. Switch to the **Matching** tab and decide if you need to make any changes to the matching parameters. The **Unusual Locations** parameter lists the folders from which processes are not normally supposed to be launched. You may also want to add your own exceptions in the following parameters:
   - **Whitelisted Creators**
     Creators in this case are parent processes, not users. If the predefined set of creator processes gives you too many alerts that you consider false alarms, you can whitelist specific parent processes.
   - **Whitelisted Processes**
     Add the processes that you think are safe and should not cause alerts.
   - **Whitelisted Users**
     Specify your administrators whom you trust to make responsible changes.
6. Click the **General** tab and select the **Enabled** option to activate the rule. After you close rule properties, commit the changes.
7. Double-click **Real-Time Monitoring | Policies**. You can use the predefined **Windows/AD Security: Detecting Common Attacks** policy, but it is recommended that you make a copy of it and use your copy instead. Right-click the policy and select **Properties**.
8. Click the **Sites** tab. In the site list, remove the default item and add the site you created earlier.
9. Click the **Rules** tab. The **Windows/AD Suspicious Activity** rule group is specified in the list by default. This group includes the required rule. If you want to select just this rule rather than the entire group, open the group and select the rule.
10. Select the **E-mail** tab, and click **Add** to specify who will receive the messages. For detailed instructions, see the Notification Groups section of the Real-Time Monitoring Overview topic.
11. If you added the **Event Log** notification option for the rule earlier, go to the **Event Log** tab and add **Event Log Recipient** to the list. For the logging to work, both this recipient in the policy and the **Event Log** option in the rule must be enabled.

12. Select the **General** tab and select the **Activate** option.
13. After you close the properties dialog box, commit the changes.

The configuration is now finished; InTrust agents will be installed automatically to the site computers to perform the monitoring.

Setting Up Monitoring for Suspicious PowerShell Activity

See the dedicated Preparing for Auditing and Monitoring PowerShell Activity guide for details about PowerShell activity tracking.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product