Quest® InTrust® 11.4.2 Report Lists

Administrative Reports

This section contains a list of reports included in the InTrust 11.4.2 Administrative Reports Report Pack.

InTrust Configuration

- InTrust agents
- InTrust servers
- InTrust sessions
- InTrust sites
- InTrust tasks

InTrust agents

This InTrust report summarizes information about InTrust agents deployed in your environment. It also directs you to details of events related to agents.

InTrust servers

This InTrust report shows information about specific InTrust servers and internal InTrust events related to those servers. The report helps analyze how InTrust functions in your environment.

InTrust sessions

This InTrust report summarizes information about InTrust sessions and directs to details of each session. You can use the report to investigate any problems that particular tasks or jobs may have had.

InTrust sites

This InTrust report shows information about specific InTrust sites and internal InTrust objects related to those sites. The report helps analyze how InTrust functions in your environment.

InTrust tasks

This InTrust report summarizes information about InTrust tasks configured in your environment. It also directs you to details of task progress.

InTrust Events

- InTrust Server events details
- InTrust Server events summary

InTrust Server events details

This InTrust report shows details of events logged by InTrust servers, helping you control how InTrust functions in your environment. This report is similar to InTrust events summary except that it does not provide statistics and is meant to quickly provide information on InTrust Server events that you are interested in.

InTrust Server events summary

This InTrust report shows statistics on events logged by InTrust servers, helping you control how InTrust functions in your environment.

Real-Time Monitoring Alerts

- Alert Details
- Alert Statistics

Alert Details

Alert Occurrences

Alerts Details

This InTrust report can help you in forensic analysis of the occurrences.

Alert Statistics

Alert Occurrences

Alert Statistics

This InTrust report displays the number of alerts that occurred and the average resolution time for the selected time period, environment and incident types. Note: If GMT time is desynchronized between the InTrust server and the computer where the agent operates, this can result in negative alert delivery times. These negative values are ignored when calculating the average resolution time. However, the number of alerts in the report does not depend on time synchronization.

Alerts Trend [chart]

This InTrust chart helps you to monitor and analyze security incidents which led to alert generation.

Top N Alerting Hosts [chart]

Use this InTrust chart to discover the computers that most frequently generate the alerts.

Top N frequent alerts [chart]

This InTrust chart helps you analyze the most frequent incidents that caused the majority of alerts.

Report Usage Statistics

Report Usage Statistics

Report Usage Statistics With Users

Best Practices Report Pack

This section contains a list of reports included in the InTrust 11.4.2 Best Practices Report Pack.

Auditing Domain Controllers

- Active Directory Changes (Based on Windows Logs)
- Critical Changes (Based on Change Auditor for AD Data)
- Domain Controller Operation (Based on Windows Logs)
- Logons (Based on Windows Logs)
- Regular Changes (Based on Change Auditor for AD Data)

Active Directory Changes (Based on Windows Logs)

Access to computer objects

This InTrust report shows attempts to access computer objects in Active Directory. Such activity may indicate unsolicited changes to the environment and should be tracked. The report is based on object access events from the Security log.

Access to group objects

This InTrust report shows attempts to access group objects in Active Directory. Such activity may indicate unsolicited changes to the environment and should be tracked. The report is based on object access events from the Security log.

Access to user objects

This InTrust report shows attempts to access user objects in Active Directory. Such activity may indicate unsolicited changes to the environment and should be tracked. The report is based on object access events from the Security log.

Audit policy changes

This InTrust report shows audit policy changes. Audit policy should be modified by administrative accounts only; otherwise these changes can indicate a security breach. Failure of the administrator to duly perform audit policy management tasks may lead to security violations.

Computer accounts management

This report shows instances where computer accounts were created, deleted, enabled or disabled. If these actions are performed by someone other than authorized administrators, this may lead to security issues and violations.

Domain Trusts Changes

This InTrust report shows domain trust changes. Domain trusts should be added, removed, or modified by administrative accounts only. If the administrator does not duly perform domain trust management tasks, this may lead to security violations.

Group management

This InTrust report shows local group changes. Groups should be created, deleted, or changed by administrators. If the administrator fails to duly perform group management tasks, this may lead to user rights misrule and security violations.

Group membership management

This InTrust report shows local, global, universal groups membership changes. User accounts should be added to or removed from groups by administrators. If the administrator fails to duly perform group membership management tasks, this may lead to user rights misrule and security violations.

Group Policy object access

This InTrust report shows Group Policy objects access attempts. Access to this type of objects may be unwarranted. Such events often indicate changes to the policies, and they need to be tracked. Note This report is based on object access events from the Security log.

Kerberos and domain policy changes

This InTrust report shows Audit and Kerberos policies changes.

Password resets

This InTrust report shows when account passwords were reset and who reset them. An entry in the report means that the password was either reset or changed. By default, only user accounts are included, but you can use the User Accounts filter if you want to include computer accounts as well.

User account lockouts

This InTrust report shows user account locked out and unlocked. A user account can be locked in accordance with the Account Lockout Policy (as a rule, after an incorrect password is entered several times in a row). Such a situation may mean password-guessing, especially if an administrative account gets locked. Click a user account in the report to view its details.

User account management

This report shows instances where user accounts were created, deleted, enabled or disabled. If these actions are performed by someone other than authorized administrators, this may lead to security issues and violations.

User rights management

This InTrust report shows changes to user rights. User rights should be assigned or removed by administrators. If the administrator fails to duly perform user rights management tasks, this may lead to user rights misrule and security violations.

Critical Changes (Based on Change Auditor for AD Data)

All change requests for GPOs by domain

This Change Auditor for Active Directory report represents both successful and failed attempts to change Group Policy object settings, delete or create GPO. An attempt fails if the system failed to perform requested operation for some reason. The most common reason of failure is insufficient permissions to make the change. The report shows either textual description of a failure or just the failure code if it is impossible to resolve the failure code to its textual description.

Changes to Active Directory schema by object

This Change Auditor for Active Directory report shows all changes to your Active Directory schema. Using this report, you can track what schema classes and attributes were modified, and how it has affected your Active Directory. Use the Class Operations filter to pinpoint schema modifications related to schema classes. Use the Attribute Operations filter to pinpoint schema modifications related to schema attributes. Schema modification may adversely impact the whole enterprise if performed carelessly.

Changes to assigned Group Policy priorities by container

This Change Auditor for Active Directory report shows changes to Group Policy Object links related to the order in which Group Policies are applied to a site, domain, or OU within your Active Directory. If set improperly, this order may seriously affect the Resulting Set of Policies calculated at the computer where the policies are applied. This report together with Group Policy Assignments report help you ensure that Resulting Set of Policies for you domain users and computers is calculated properly.

Changes to audit policy settings by audit policy

This Change Auditor for Active Directory report shows all changes to Audit Policy settings for all Group Policies of your Active Directory domains. Turning on extra auditing may impact your domain controllers and other domain members, while turning auditing off may weaken the security. So, every modification of Audit Policy settings must be thoroughly examined.

Changes to FSMO roles by domain

This Change Auditor for Active Directory report shows all FSMO role transfers and seizures in every domain and forest of your Active Directory. For every FSMO role the report displays the domain controller that held the role before the change, and the one that acquired the role as a result of the change. FSMO role changes (especially role seizures) should be made only if it is impossible to recover the original holder after it has become unavailable.

Changes to replication configuration by forest

This Change Auditor for Active Directory report shows all changes related to the replication configuration of your Active Directory forests. The report analyzes changes to Active Directory objects and explains what these particular changes mean to the replication. Use the Configuration Items filter to analyze changes related to particular aspects of the replication configuration, for example, site link schedule changes, replication connection creations and deletions, and so on.

Changes to site configuration by forest

This Change Auditor for Active Directory report shows all changes related to the site configuration of your Active Directory forests. Using this report, you can inspect what new sites were created, and what changes were applied to existing sites. It is recommended to modify your site configuration only if the physical AD topology has been changed. This report enables you to control that no accidental or unwanted changes to your Active Directory sites were made.

Changes to user rights by domain

This Change Auditor for Active Directory report shows all changes to User Rights Assignment settings for all Group Policies of your Active Directory domains. These settings affect security and availability of your domain controllers and other domain members, so it is important to watch them closely. Too strict a User Rights policy leads to people and services having problems with access to necessary network resources, but excessive permissions are a serious flaw in network security.

Connection schedule changes

This Change Auditor for Active Directory report shows changes to the replication schedule defined at the level of replication connections. The schedule is displayed for the local time zone.

Direct SYSVOL changes by domain

This Change Auditor for Active Directory report shows Group Policy setting changes made by direct modification of policy files stored on the SYSVOL share of domain controllers. Changes to both Security Policies and Administrative Templates are included. Note. The report does not display malformed SYSVOL file changes that violated the established format of the policy setting file.

DNS record changes

This Change Auditor for Active Directory report shows changes to zone data of Active Directory-integrated DNS zones. You can see what DNS records were added, deleted or modified in a DNS zone. For each type of zone record (SRV, A, etc) specific details are provided.

Domain changes

This Change Auditor for Active Directory report shows domain functional level changes. Use the report to track changes to the domain functional level and suffixes.

Domain trust relationship changes

This Change Auditor for Active Directory report shows changes to domain trust relationships. You can see what domains were defined as trusted for a specific domain and what domains had their trust relationship removed.

Group Policy assignments by GPO

This Change Auditor for Active Directory report shows the change history for Group Policy Object links in your environment during the specified period. It displays: who made the change, what GPO flags were changed (such as Disabled and No Override), what GPO links were established or removed for what containers, when the change was made For modified GPO flags, the report shows both the old and the new (modified) flag values.

OU creation or deletion by domain

This Change Auditor for Active Directory report shows what organizational units were created or deleted in what domains.

OU delegation changes

This Change Auditor for Active Directory report shows changes to security configuration of organizational units. The report helps track permissions granted to delegated administrators.

OU moved or renamed by domain

This Change Auditor for Active Directory report shows what organization units were moved or renamed. For either type of change, both the old and new canonical name of the OU's parent container are displayed.

Permission inheritance changes by domain

This Change Auditor for Active Directory report shows changes to Active Directory objects' permission inheritance flag. It shows you whether inherited permissions were copied or removed from the object when the inheritance flag was cleared.

Policy inheritance blocking disabled or enabled by domain

Typically, Group Policy is propagated from parent to child containers within a domain. You can block policy inheritance at the domain or organizational-unit level by opening the properties dialog box for the domain or organizational unit and selecting the Block Policy inheritance check box. This Change Auditor for Active Directory report shows who and when enabled or disabled policy inheritance on what containers.

Security options changes by Group Policy

This Change Auditor for Active Directory report shows all changes to Security Options for all Group Policies of your Active Directory domains.

Site link schedule changes

This Change Auditor for Active Directory report shows changes to the replication schedule defined at the level of site links. The schedule is displayed for the local time zone.

Universal group membership setting changes

This Change Auditor for Active Directory report shows changes to the configuration of universal group membership caching. You can use this report to track sites where this setting was turned on or off. It also shows changes to the site used for refreshing the contents of the universal group cache.

Domain Controller Operation (Based on Windows Logs)

Event Log cleared

This InTrust report shows event log cleared events. Event logs should be cleared only when there is lack of free space, which rarely occurs. Therefore, instances of event logs being cleared can indicate intruder activity and attempts to cover the tracks.

Event log errors

Errors or warnings from the event log could be an indication of intruder activity or an auditing system malfunction. This InTrust report shows situations when event logs generated warnings or errors.

Policy enforcement errors

This InTrust report shows some events from the security policy subsystem which could be an indication of intruder activity or a potential security breach.

Registry Access

This InTrust report shows attempts to access registry keys. Access to some registry keys (particularly the startup keys) may be unwarranted.

Server reboots (Windows Server 2003 and Windows Server 2008 only)

This InTrust report shows both expected and unexpected server reboots (Windows 2003, Windows 2008 only). Notes: Please ensure than Shutdown Event Tracker service is enabled at your servers.

Software installation

This InTrust report helps track what software products are installed or failed to install on which computers. The report shows only those products whose setup programs use Windows Installer. Using the Grouping filter, you can organize the information as necessary. To see what software was installed on particular computers, use grouping by computer. To find out where certain software products were installed, use grouping by software product.

Logons (Based on Windows Logs)

Administrative logons (Security log only)

This InTrust report shows successful and failed logons of all types by the specified privileged users. By default, only the "Admin" and "Administrator" user names are included. Change the filters to include any other privileged users you need. For failed logons, reasons are displayed. The report uses only Security log events.

Failed logons (NTLM audit only)

This InTrust report shows failed logons of all types. Failure reasons are indicated. The report uses only NTLM events.

Failed logons (Security log only)

This InTrust report shows failed logons of all types. Failure reasons are indicated. The report uses only Security log events.

Logons (NTLM audit only)

This InTrust report shows successful and failed logons of all types. For failed logons, reasons are displayed. The report uses only NTLM events.

Multiple failed account logons

This InTrust report shows patterns where multiple account logon failures occurred in a row, possibly indicating a brute-force attack. The report uses Kerberos events.

Multiple failed logons

This InTrust report shows patterns where multiple logon failures occurred in a row, possibly indicating a brute-force attack. Detailed information about the logon failures is provided. Data for the report comes from all relevant logs (Security, Kerberos, NTLM). Click a number in the Attempts column to view the details of logon failures in a subreport.

Multiple failed logons (Security log only)

This InTrust report shows patterns where multiple logon failures occurred in a row, possibly indicating a brute-force attack. Detailed information about the logon failures is provided. The report uses only Security log events. Click a number in the Attempts column to view the details of logon failures in a subreport.

Non-network logons (Security log only)

This InTrust report shows successful and failed logons of all types except 'Network'. For failed logons, reasons are displayed. The report uses only Security log events.

Regular Changes (Based on Change Auditor for AD Data)

Change requests for computer objects by domain

This InTrust report shows both successful and failed attempts to change attributes of computer objects in Active Directory. The most common reason for request failures is insufficient permissions to make the change. For each failure, the report shows a textual description where possible, or just the error code.

Change requests for group objects by domain - detailed

This InTrust report shows both successful and failed attempts to change attributes of group objects in Active Directory. The most common reason for request failures is insufficient permissions to make the change. For each failure, the report shows a textual description where possible, or just the error code.

Change requests for user objects by domain

This InTrust report shows both successful and failed attempts to change attributes of user objects in Active Directory. The most common reason for request failures is insufficient permissions to make the change. For each failure, the report shows a textual description where possible, or just the error code.

Changes to computer object attributes by domain

This InTrust report shows the history of changes to the attributes of computer objects in Active Directory during the specified period. It shows who changed what attributes, and when and how they were changed. This helps stay aware of what is happening to your Active Directory, and take corrective measures if required.

Changes to user account passwords by domain

The InTrust Plug-in for Active Directory report shows all changes to user account passwords. Passwords are changed by users themselves or reset by administrators on user request.

Changes to user object attributes by domain

This InTrust report shows the history of changes to the attributes of user objects in Active Directory during the specified period. It shows who changed what attributes, and when and how they were changed. This helps stay aware of what is happening to your Active Directory, and take corrective measures if required.

Computer object moves by domain

This Change Auditor for Active Directory report shows computers that were moved. The report displays both source and target locations, which can be organizational units and other containers.

Enabling and disabling of users by domain

To prevent a particular user from logging on for security reasons you can disable the user account rather than delete it altogether. The user account may be enabled again afterwards. This Change Auditor for Active Directory report shows the history of user account activations and deactivations.

Group creations and deletions by domain

This Change Auditor for Active Directory report shows what group accounts were created or deleted in what domains.

Group membership management by domain

This Change Auditor for Active Directory report shows all group membership changes. You can track which accounts were added to or removed from which groups, and who performed the management actions.

User account management by domain

This Change Auditor for Active Directory report shows all changes made to all user account attributes.

User account moves by domain

This Change Auditor for Active Directory report shows user accounts that were moved. The report displays both source and target locations, which can be organizational units and other containers.

User creations and deletions by domain

This Change Auditor for Active Directory report shows what user accounts were created and deleted in what domains.

Auditing Exchange Servers

All Events (Based on ChangeAuditor for Exchange Data)

All Exchange-related audit events from Windows event logs

This report requires the InTrust Plug-in for Active Directory Service to be installed on domain controllers. This report contains combined Exchange-related information from the InTrust for Exchange event log, the InTrust for AD event log, and the Application log.

Exchange events statistics (Application log only)

This report shows general Exchange event statistics. You can click a number in the report to view a sub-report with details of the events that the number represents.

Configuration Changes (Based on ChangeAuditor for Exchange Data)

Exchange-related configuration object modifications

This report shows changes to the configuration of the Exchange organization in Active Directory. This report requires ChangeAuditor for Active Directory to be installed on domain controllers.

Logons (Based on Windows Logs)

Administrative logons (Security log only)

This InTrust report shows successful and failed logons of all types by the specified privileged users. By default, only the "Admin" and "Administrator" user names are included. Change the filters to include any other privileged users you need. For failed logons, reasons are displayed. The report uses only Security log events.

Failed logons (Security log only)

This InTrust report shows failed logons of all types. Failure reasons are indicated. The report uses only Security log events.

Multiple failed logons (Security log only)

This InTrust report shows patterns where multiple logon failures occurred in a row, possibly indicating a brute-force attack. Detailed information about the logon failures is provided. The report uses only Security log events. Click a number in the Attempts column to view the details of logon failures in a subreport.

Non-network logons (Security log only)

This InTrust report shows successful and failed logons of all types except 'Network'. For failed logons, reasons are displayed. The report uses only Security log events.

Mailbox Access (Based on ChangeAuditor for Exchange Data)

Store operations

This report shows store operations.

Use of Send privileges

This InTrust report helps you monitor how Send permissions are used. Set the MS Exchange diagnostics logging on the 'Send as' and 'Send on behalf of' on Exchange server to minimum level.

Mailbox Logons (Based on ChangeAuditor for Exchange Data)

Logons (Application log only)

This report shows successful MAPI logons to mailboxes in your Exchange environment. The MAPI protocol is used by clients such as Microsoft Outlook. The report helps you find out who uses which personal or shared mailboxes. This report requires setting the MS Exchange diagnostics logging on the MSExchangeIS at least to minimum level on Exchange server.

Permission Changes (Based on ChangeAuditor for Exchange Data)

Delegate management - brief

This report provides information about delegate assignment, including delegate creation, delegate removal, and changes to permissions granted to delegates via Microsoft Outlook.

Delegate management - detailed

This report provides information about delegate assignment, including delegate creation, delegate removal, and changes to permissions granted to delegates.

Folder permission changes - brief

This report shows changes to folder permissions in mailboxes (client permissions changes). The report contains old permissions value and new permission value.

Mailbox permission changes

This report shows details about changes to user mailbox security settings. The report displays Access Control Entries that were added, deleted, or modified in the ACL of the mailbox. The report helps identity which permissions on which mailboxes were granted to or revoked from which accounts. This report requires ChangeAuditor for Active Directory to be installed on domain controllers.

Public folder permission changes

This report shows Folder Permission changes.

Protection Group Configuration (Based on ChangeAuditor for Exchange Data)

Protection group object modifications

This report shows changes to the configuration of the Exchange organization in Active Directory. This report requires ChangeAuditor for Active Directory to be installed on domain controllers.

Summary (Based on ChangeAuditor for Exchange Data)

Mailbox access

This report shows a color-coded summary of all mailbox access events that occurred in your environment. The baseline is configured in a report parameter. From each section you can drill down to a list of changes associated with the selected number. Comparing the actual number within a particular category with the specified baseline can help detect abnormal administrative activity, discover violations, and improve procedures established in the environment.

Mailbox permissions

This report shows a color-coded summary of all mailbox permissions changes events that occurred in your environment. The baseline is configured in a report parameter. From each section you can drill down to a list of changes associated with the selected number. Comparing the actual number within a particular category with the specified baseline can help detect abnormal administrative activity, discover violations, and improve procedures established in the environment.

Protected groups

This report shows a color-coded summary of all protected groups changes events that occurred in your environment. The baseline is configured in a report parameter. From each section you can drill down to a list of changes associated with the selected number. Comparing the actual number within a particular category with the specified baseline can help detect abnormal administrative activity, discover violations, and improve procedures established in the environment.

Auditing File Servers

Recent Content Operations (Based on ChangeAuditor for File Servers Data)

Shadow copy modifications

This InTrust report shows details about actions preformed with shadow copies. Report contains information about create, delete and rollback actions.

Activity Research (Based on ChangeAuditor for File Servers Data)

Content Activity Research

This InTrust report shows who gained what type of access to files and folders that ChangeAuditor for Windows File Servers monitors. Data in the report is grouped by file server.

User Activity Research

This InTrust report shows who gained what type of access to files and folders that ChangeAuditor for Windows File Servers monitors. Data in the report is grouped by user, then by file server.

Content Usage Statistics (Based on ChangeAuditor for File Servers Data)

Most accessed objects

This InTrust report shows files and folders for which the largest number of access attempts occurred. The time of the last access attempt is included.

Most active content users

This InTrust report shows statistics for users who access monitored files and folders most actively. The time of the last access attempt is included.

Most modified objects

This InTrust report shows files and folders which were modified the most times. The time of the last modification and the user responsible are displayed.

Objects with most failed access attempts

This InTrust report shows files and folders for which the largest number of failed access attempts occurred.

Top active users per operation

This InTrust report shows statistics for users who access monitored files and folders most actively. The time of the last access attempt is included. Access attempts are grouped by operation.

Users with most failed access attempts

This InTrust report shows users with the largest number of failed attempts to access files and folders that ChangeAuditor for Windows File Servers monitors. The time of the last failed access attempt is included.

EMC Events (Based on ChangeAuditor for File Servers Data)

All ChangeAuditor for EMC events by action

This report shows all events from ChangeAuditor for EMC log

All ChangeAuditor for EMC events by IP address

This report shows all events from ChangeAuditor for EMC log

Logons (Based on Windows Logs)

Administrative logons (Security log only)

This InTrust report shows successful and failed logons of all types by the specified privileged users. By default, only the "Admin" and "Administrator" user names are included. Change the filters to include any other privileged users you need. For failed logons, reasons are displayed. The report uses only Security log events.

Failed logons (Security log only)

This InTrust report shows failed logons of all types. Failure reasons are indicated. The report uses only Security log events.

Multiple failed logons (Security log only)

This InTrust report shows patterns where multiple logon failures occurred in a row, possibly indicating a brute-force attack. Detailed information about the logon failures is provided. The report uses only Security log events. Click a number in the Attempts column to view the details of logon failures in a subreport.

Non-network logons (Security log only)

This InTrust report shows successful and failed logons of all types except 'Network'. For failed logons, reasons are displayed. The report uses only Security log events.

NetApp Events (Based on ChangeAuditor for File Servers Data)

All ChangeAuditor for NetApp events by action

This report shows all events from Change Auditor for NetApp log

All ChangeAuditor for NetApp events by IP address

This report shows all events from Change Auditor for NetApp log

Recent Share Operations (Based on ChangeAuditor for File Servers Data)

Recent share operations

This InTrust report shows who and when recently changed shares.

Auditing Workstations

- Activity on Workstations (Based on Windows Logs)
- Logons (Based on Windows Logs)

Activity on Workstations (Based on Windows Logs)

Concurrent user logon sessions

This report displays user logon sessions from different computers that overlapped in time. The report uses advanced logon events generate
d by InTrust agents.

Daily total duration of interactive logon sessions

This report shows how long users' interactive logon sessions lasted each day. The report uses advanced logon events generated by InTrust agents.

Local audit policy changes

This InTrust report shows audit policy changes. Audit policy should be modified by administrative accounts only; otherwise these changes can indicate a security breach. Failure of the administrator to duly perform audit policy management tasks may lead to security violations.

Local group management

This InTrust report shows local group changes. Groups should be created, deleted, or changed by administrators. If the administrator fails to duly perform group management tasks, this may lead to user rights misrule and security violations.

Local group membership management

This InTrust report shows local group membership changes. User accounts should be added to or removed from groups by administrators. If the administrator fails to duly perform group membership management tasks, this may lead to user rights misrule and security violations.

Local user account management

This InTrust report shows changes to local user accounts. User accounts should be created, deleted, enabled, or disabled by administrators. If the administrator fails to duly perform account management tasks, this may lead to account misrule and even security violations.

Logons to workstations

This InTrust report shows successful and failed logons of all types. For failed logons, reasons are displayed. This helps analyze who tried to log on to which computers from which workstations.

Removable media attach-detach by workstation

For correct results, this report relies on the "Workstations: Removable devices attached/detached" real-time monitoring policy and real-time monitoring rules from "Use of removable media" folder.

User account lockouts and unlocks by workstation

This InTrust report shows user account locked out and unlocked. A user account can be locked in accordance with the Account Lockout Policy (as a rule, after an incorrect password is entered several times in a row). Such a situation may mean password-guessing, especially if an administrative account gets locked. Click a user account in the report to view its details.

User logon session duration by day

For each interactive logon session this report shows its start and termination time and how long it lasted. The report uses advanced logon events generated by InTrust agents.

Workstation process tracking

This InTrust report shows whether the applications you specify were started. If an application is prohibited, its launch may indicate a security issue. What is more, running restricted software often means corporate policy violations.

Workstation registry access

This InTrust report shows attempts to access registry keys. Access to some registry keys (particularly the startup keys) may be unwarranted.

Workstation registry value modifications (Windows Vista and later)

This InTrust report shows modifications of the registry values on Windows Vista (and later) machines. The report is based on EventID=4657. Note: Some value changes cannot be displayed due to specific data type.

Workstation software installation

This InTrust report helps track what software products are installed or failed to install on which computers. The report shows only those products whose setup programs use Windows Installer. Using the Grouping filter, you can organize the information as necessary. To see what software was installed on particular computers, use grouping by computer. To find out where certain software products were installed, use grouping by software product.

Logons (Based on Windows Logs)

Administrative logons (Security log only)

This InTrust report shows successful and failed logons of all types by the specified privileged users. By default, only the "Admin" and "Administrator" user names are included. Change the filters to include any other privileged users you need. For failed logons, reasons are displayed. The report uses only Security log events.

Failed logons (Security log only)

This InTrust report shows failed logons of all types. Failure reasons are indicated. The report uses only Security log events.

Multiple failed logons (Security log only)

This InTrust report shows patterns where multiple logon failures occurred in a row, possibly indicating a brute-force attack. Detailed information about the logon failures is provided. The report uses only Security log events. Click a number in the Attempts column to view the details of logon failures in a subreport.

Non-network logons (Security log only)

This InTrust report shows successful and failed logons of all types except 'Network'. For failed logons, reasons are displayed. The report uses only Security

Reports for ACS

This section contains a list of reports intended for viewing via Microsoft System Center Operations Manager console; they are based on data from Windows security log collected using Audit Collection Services (ACS) and then stored to InTrust Audit database for analysis and reporting.

The special 'InTrust for ACS management pack deployment status' report displays the status of Quest InTrust for ACS Management Pack deployment to Operations Manager agents.

Reports for Operations Manager Console

Computer accounts changes

This InTrust report shows computer accounts changes. Computer accounts should be created, deleted, renamed, or changed by administrative accounts only. If the administrator fails to duly perform computer account management tasks, this may lead to security violations.

Domain Trusts Changes

This InTrust report shows domain trust changes. Domain trusts should be added, removed, or modified by administrative accounts only. If the administrator does not duly perform domain trust management tasks, this may lead to security violations.

File Access

This InTrust report shows file access attempts. Access to certain files may be unwarranted.

Group Management

This InTrust report shows group changes. Groups should be created, deleted, or changed by administrators. If the administrator fails to duly perform group management tasks, this may lead to user rights misrule and security violations.

Group Policy Object access

This InTrust report shows Group Policy objects access attempts. Access to this type of objects may be unwarranted. Such events often indicate changes to the policies, and they need to be tracked. Note This report is based on object access events from the Security log.

InTrust for ACS management pack deployment status

This report displays the status of Quest InTrust for ACS Management Pack deployment to Operations Manager agents (ACS-forwarders). The Management Pack provides for complementing ACS database records with the information required to comply with InTrust repository and Audit database format.

Logon activity trends

This InTrust chart graphically represents logon activity in your network, visualizing, for example, statistics for logons that failed due to different reasons (for example, bad password, disabled user account, etc.). The chart allows you to detect trends in logon activity and analyze anomalies.

Logon Statistics

In the Windows environment different logon types are registered by the system depending on what kind of resource a user accesses. This InTrust report shows all logon types such as interactive logons to domains, access to shared folders, dial-up connections to the network, and so on, and groups logon statistics.

Password resets

This InTrust report shows when account passwords were reset and who reset them. An entry in the report means that the password was either reset or changed. By default, only user accounts are included, but you can use the User Accounts filter if you want to include computer accounts as well.

User Accounts Management

This InTrust report shows changes to user accounts. User accounts should be created, deleted, enabled, or disabled by administrators. If the administrator fails to duly perform account management tasks, this may lead to account misrule and even security violations.

User rights management

This InTrust report shows changes to user rights. User rights should be assigned or removed by administrators. If the administrator fails to duly perform user rights management tasks, this may lead to user rights misrule and security violations.

Report Pack for Active Roles Server

This section contains a list of reports included in the InTrust 11.4.2 Report Pack for Active Roles Server.

Active Directory Management Bypassing ARS

Account management performed outside ARS (Security Log)

Jap This InTrust report shows changes to Active Directory accounts (users, computers and groups) that were performed with administrative tools other than ARS. Use it if the managed domain accounts reserved for the ARS service can be used by other applications or personnel. To detect account management activity outside ARS, the report checks both Security log events and ARS Server log events. If an event in the Security log has no matching event in the EDM Server log, this event is included in the report.

All activity within and outside of Active Roles Server

This InTrust Plug-in for Active Directory report shows a consolidated trail of Active Directory changes made both with ARS and with native Active Directory management tools bypassing ARS.

Active Directory Management using ARS

Deprovisioning of User Accounts

This InTrust report contains the history of Active Directory user account that were deprovisioned during the specified period of time.

Directory object management

For Active Roles Server this InTrust report shows all activity of particular users that has to do with Active Directory object management. The report helps check whether administrative activity complies with the corporate policy.

Directory object management summary by Initiator

For Active Roles Server this InTrust chart shows the proportion of particular users activity that has to do with Active Directory object management. The chart helps check whether administrative activity complies with the corporate policy.

Group Management by Initiator

This report shows group changes. Groups should be created, deleted, or changed by delegated administrators.

Group Membership Management by Initiator

This report shows group membership changes. User accounts should be added to or removed from groups by delegated administrators.

User Accounts Management

This report shows changes to user accounts. User accounts should be created, deleted, enabled, or disabled by delegated administrators.

User attribute management

For Active Roles Server this InTrust report shows all changes to user account attributes in chronological order. It indicates the changed attributes, who changed them, when and how they were changed. The report provides both the old and the new values of changed attributes. Using the report, you can easily find out who changed or reset user passwords within a given time period reflected in the ARS Server log.

Active Roles Server Events

Active Roles Server event statistics by Computer

This InTrust report summarizes Active Roles Server events and groups them by computer (where they were logged).

Active Roles Server events by eventID

For Active Roles Server 6.0 this InTrust report represents ARS events grouped by event ID. The upper pane shows how many events with specific IDs occurred. The lower left pane lists all events with one specific ID. Click an event to view its description or insertion strings in the lower right pane. Note. The report is intended for interactive use only, not for print.

Active Roles Server startup failures

This InTrust report helps determine the time period during which the ARS service was unavailable because it had not started. The report assumes that service recovery time is the time between nearest failure event and a successful service start. You can use the information when assessing your environments SLA compliance.

All Active Roles Server events

This InTrust report represents ARS events as they appear in the event log. Click the description or insertion strings link to see the details in a sub-report.

Firewalls Reports

This section contains a list of reports included in the InTrust 11.4.2 Report Pack for Cisco PIX and CheckPoint Firewall-1.

CheckPoint Firewall-1

CheckPoint Firewall accepted connections

This InTrust report rates successful connections. In terms of the report, a connection is defined by the protocol, the local address within the environment and the foreign address outside it. The report helps analyze connection statistics and track abnormally frequent or numerous connections.

CheckPoint Firewall dropped connections

This InTrust report rates dropped connections. In terms of the report, a connection is defined by the protocol, the local address within the environment and the foreign address outside it. The report helps find out what kinds of connections are dropped by CheckPoint and track IP addresses at which such activity is attempted. The most numerous connections from a specific local IP address to a specific foreign IP address are on top.

CheckPoint Firewall events

This InTrust form helps you perform detailed analysis of CheckPoint Firewall events and easily detect frequent events of the same type. Use the top pane of the form to sort events. Click an entry in this pane to see details of grouped events below.

CheckPoint Firewall rules statistics

This InTrust report rates CheckPoint Firewall rules by number of rule matches. Rules that were matched the most times are on top. The report helps find out which rules are not matched and remove or modify them. Click a number to view a sub-report with the number of matches that the number stands for.

Cisco PIX

Cisco PIX connections

This InTrust report shows connections processed by Cisco PIX. In terms of the report, a Cisco PIX connection is defined by the protocol, the local address within the environment and the foreign address outside it. The report helps analyze statistical data on connections, find out anomalies and trends.

Cisco PIX events

This InTrust form helps you perform detailed analysis of Cisco PIX events and easily detect frequent events of the same type. Use the top pane of the form to sort events. Click an item in this pane to see its details of grouped events below.

Cisco PIX traffic

This InTrust report shows how much traffic was generated by connections through Cisco PIX.

Report Pack for Microsoft IIS

This section contains a list of reports included in the InTrust11.4.2 Report Pack for Microsoft IIS.

FTP Site Usage

Clients

FTP site top 100 most active clients

This InTrust report lists the 100 most active Microsoft IIS FTP site visitors.

Files Access

FTP site access to files

This InTrust report provides comprehensive information on files access events for your FTP site.

Traffic

FTP site daily traffic [chart]

This InTrust chart provides statistics on FTP site daily traffic for the specified date.

FTP site total statistics

This InTrust report provides aggregate statistics for Microsoft Internet Information Server FTP site.

Security

- Advanced Forensic Analysis
- Common Security Incidents

Advanced Forensic Analysis

Security Subsystem Faults

Audit subsystem faults

This InTrust report displays information on problems with Microsoft IIS logging. This data helps examine audit subsystem health of specified servers.

Suspicious Activity

Published Resources Access

FTP site detailed access analysis

- This InTrust report helps perform detailed analysis of FTP events.

Web site detailed access analysis

- This InTrust report helps perform detailed analysis of HTTP events.

Suspicious Requests

FTP site failed logons

- This InTrust report shows all failed FTP logons. Numerous FTP logon failures may indicate intrusion attempts.

Web site all requests

- This Intrust report displays general information related to the Web requests.

Common Security Incidents

Gaining Privileged Access

Administration web sites access attempts

This InTrust report shows attempts to gain access to administration sites from the Web. An administration Web site can usually be accessed on port 5466. Normally, access is allowed only from the local host, so access attempts from the Web can indicate unauthorized access.

Administrative folders access attempts

Administrative folders are critical resources, because they allow gaining access to server management. This InTrust report enables you to monitor administrative folder access attempts performed from the Web.

Gaining User Access

FTP site daily failed logons [chart]

This InTrust chart presents statistics on failed attempts to log on to an FTP server. Multiple FTP server logon attempts displayed as graph spikes may indicate a brute force attack.

Multiple Failed FTP Server Logon Attempts detailed

Multiple failed FTP server logon attempts may indicate a brute force attack. This InTrust report shows detailed information on each session all requests, date and time, client IP and server where the user tried to log on.

Web site daily failed logons [chart]

This InTrust chart displays failed Web server access events. Spikes in the graph indicate abnormal numbers of errors. Peaks might indicate Denial of Service attacks against the server. The X-axis represents time, and the Y-axis represents the number of events.

Web Site Usage

- Clients
- Diagnostics
- Referrals
- Traffic
- Web site total statistics

Clients

Web site daily unique visitors [chart]

This InTrust chart graphically shows the number of new visitors who have visited a Microsoft Internet Information Server web site for each day over a specified period of time.

Web site most active clients

This InTrust report lists the specified number of most active Microsoft IIS web site visitors. For each client the following information is provided: IP address, name resolution, country and the number of hits over a specified period of time.

Web site visits per client [chart]

This InTrust chart graphically shows the frequency of visits for all Microsoft Internet Information Server web site clients. This information can be used to determine the percentage of users that visit the site repeatedly.

Diagnostics

Web site failed access statistics [chart]

This InTrust chart shows Microsoft Internet Information Server errors. A large number of certain types of errors may reveal suspicious activity, or indicate potential problems

Web site unauthorized access attempts by client IP

This InTrust report provides information on unauthorized access attempts of Web resources grouped by visitor IPs.

Web site unauthorized access attempts by resource

This InTrust report provides information on unauthorized access attempts of web resources grouped by resource name.

Referrals

Web site access by referring sites [chart]

This InTrust chart provides statistics on access to a web site from referring sites.

Traffic

WEB site daily traffic [chart]

This InTrust chart provides statistics on web site daily traffic (in Kbytes) for the specified date.

Web site total statistics

This InTrust report provides aggregate statistics for Microsoft Internet Information Server WWW.

Oracle Reports

This section contains a list of reports included in the InTrust11.4.2 Report Pack for Oracle.

Administrative users audit

Administrative users activity [Unix]

This InTrust report shows the results of administrative users activity auditing. The report displays Oracle host and instance to which the user was connected, action date and time, user name and privilege, action taken, and action return code.

Administrative users activity [Windows]

This report shows the results of administrative users activity auditing. The report displays Oracle host and instance to which the user was connected, action date and time, user name and privilege, action taken, and action return code.

Common audit

Data Audit

Data retrieval and modification activity

This InTrust report shows the results of administrative users activity auditing. The report displays Oracle host and instance to which the user was connected, action date and time, user name and privilege, action taken, and action return code.

Database structure modification activity

This InTrust report shows the results of administrative users activity auditing. The report displays Oracle host and instance to which the user was connected, action date and time, user name and privilege, action taken, and action return code.

Management Activity

Rights Management

Use this report to examine the results of user and role rights management activity auditing. This activity includes granting or revoking rights. The report displays Oracle host and instance names, action type, action date and time, initiator, target object with its server and database, grantee, SQL text and action return code.

User and Role Management

This InTrust report shows the results of administrative users activity auditing. The report displays Oracle host and instance to which the user was connected, action date and time, user name and privilege, action taken, and action return code.

User Activity

User logons and logoffs

Use this report to view the results of users logon and logoffs auditing. The report displays Oracle user name, Oracle host and instance names, and action details, such as date/time, action type and return code.

Reports for Privilege Manager for Sudo

This section contains a list of reports included in the InTrust11.4.2 Report Pack for Privilege Manager for Sudo.

Privilege Manager for Sudo

All Events

This InTrust report shows all the user activity logged by selected Privilege Manager master hosts.

All Events By Result

This InTrust report shows all user events broken down by result logged by selected Privilege Manager.

Elevated Privilege Events

This InTrust report shows all the events logged by selected Privilege Manager master hosts where a user has attempted to run a command as a different user.

Master Events

This InTrust report shows all user events broken down by master host logged by selected Privilege Manager.

Out Of Bound Events

This InTrust report shows all the out of band user activity logged by selected Privilege Manager master hosts.

Rejected Events

This InTrust report shows all the user events that were rejected by the Privilege Manager master hosts.

Report Pack for Red Hat Enterprise Linux

This section contains a list of reports included in the InTrust11.4.2 Report Pack for Red Hat Enterprise Linux.

Administrative Activity

Redhat Linux Configuration files modifications

This InTrust report shows instances of plain text file modification. This lets you find out whether changes were made to particular Linux configuration files. The report displays when strings were added or removed, but does not include the actual changes. If a line was modified, the report treats this as a combination of line deletion and line addition.

Redhat Linux Group management

This InTrust report shows instances of group creation and deletion. Click the Details link for a particular group to see the details of the group management action in a sub-report.

Redhat Linux Group membership management

This InTrust report shows instances of members being added to groups and removed from groups. You can organize information in several ways for convenient analysis.

Redhat Linux User management

This InTrust report shows instances of user account creation and deletion. Click the Details link for a particular user to see the details of the user management action in a sub-report.

Reports for Recovery Manager for Active Directory

This section contains a list of reports included in the InTrust11.4.2 Knowledge Pack for Recovery Manager for Active Directory.

Recovery Manager for Active Directory

Backup Jobs History

This InTrust report shows the end times of backup jobs, their statuses, and details of possible backup errors. The report is based on Recovery Manager for Active Directory host events from the Application log.

Report Pack for Solaris

This section contains a list of reports included in the InTrust11.4.2 Report Pack for Oracle.

Administrative Activity

Configuration Files Modification

Configuration files modifications

This InTrust report shows instances of plain text file modification. This lets you find out whether changes were made to particular Solaris configuration files. The report displays when strings were added or removed, but does not include the actual changes. If a line was modified, the report treats this as a combination of line deletion and line addition.

Group management

This InTrust report shows instances of group creation and deletion for Solaris. The Solaris Accounts Monitoring data source should be configured to generate this report. Click the Details link for a particular group to see the details of the group management action in a sub-report.

Group membership management

This InTrust report shows instances of members being added to groups and removed from groups for Solaris. The Solaris Accounts Monitoring data source should be configured to generate this report. You can organize information in several ways for convenient analysis.

User management

This InTrust report shows instances of user account creation and deletion for Solaris. The Solaris Accounts Monitoring data source should be configured to generate this report. Click the Details link for a particular user to see the details of the user management action in a sub-report.

chmod command usage

This InTrust report shows usage of the chmod command, which changes file modes. Tracking this activity can provide useful information from a security standpoint.

chown command usage

This InTrust report shows usage of the chown command, which changes the owner of a file. Tracking this activity can provide useful information from a security standpoint.

passwd command usage

This InTrust report shows usage of the passwd command, which changes a users password. Tracking this activity can provide useful information from a security standpoint (for example, during security incident investigations.)

Forensic Analysis

All Solaris Audit Log events

Solaris Audit Log events

Solaris Syslog Events

This InTrust form helps you perform detailed analysis of security events in your Solaris environment.REQUIREMENT InTrust 9.6

Normal User Activity

- Logins
- File access
- Process execution
- su command usage
- User sessions

Logins

Failed logins

This InTrust report shows statistics on failed logins by all users. Click a number in the report to view details of the logins.

Successful logins

This InTrust report shows statistics on successful logins by all users. Click a number in the report to view details of the logins.

File access

This InTrust report shows details of file access attempts. Failed Click a Details link to view a sub-report with details of the relevant event.

Process execution

This InTrust report shows process execution data based on the exec() and execve() system calls.

su command usage

This InTrust report helps track the use of the su command. For each host, it shows the following information: date and time the command was used, audit user and real user who issued the command, and the corresponding Solaris Audit log message.

User sessions

This InTrust report shows details of user sessions, from login to logout, and lets you discover particular users activity patterns.

Report Pack for SQL Server

This section contains a list of reports included in the InTrust11.4.2 Report Pack for SQL Server.

C2 Log

Account Management

Logins audit

This InTrust report shows events from the C2 log which indicate that a SQL Server login is added or removed, a Windows login is added or removed, or a property of a login, including passwords, is modified. For each SQL server name and instance, the report displays the following event details login name, date and time, action type and action status.

Roles audit

This InTrust report shows events from the C2 log which indicate that a login has been added or removed as a database user. For each SQL server name and instance, the report displays the following event details database name, login name, role name, action date and time, action type and action status.

Users audit

This InTrust report shows events from the C2 log which indicate that a login is added or removed as a database user (with Windows or SQL Server authentication). For each SQL server and instance, the report displays the following details: database name, user name, login name, action date and time, action type and action status.

Change Management

Database structure modifications

This InTrust report shows events from the C2 log which indicate that a CREATE, ALTER, or DROP object command has been executed. For each SQL server and instance, the report displays the following event details: database name, object name, user name, date and time, action type and action status.

Permission modifications

This InTrust report shows events from the C2 log which indicate that a GRANT, DENY or REVOKE has been executed for a statement permission or for an object permission. For each SQL server and instance, the report displays the following event details database name, object or statement name, user name, date and time, action type and action status.

Logons

Logons c2 log

This InTrust report shows user logon events from the C2 log. For each SQL server and instance, the report displays the following event details: Server and instance, Date/Time, login, event class, host and application name.

All events in c2 log

This InTrust report shows all SQL Server events gathered from the C2 log. For each SQL server and instance, the report displays such event details as Server, Instance, Date/Time, Login, Event Class, Database, Success.

Error Log

- Maintenance
- Security
- All events in error log

Maintenance

Backup history

This InTrust report shows backup and restore events in Error log. For each SQL server or server instance, the report displays event times, database and action.

DBCC history

This InTrust report shows DBCC events in the Error log. For each SQL server and instance, the following event details are displayed: event times and DBCC output messages.

Server starts up shuts down

This InTrust report, based on events from the Error log, shows when SQL servers were started and shut down.

Security

Logons error log

This InTrust report shows logon events in Error log. For each SQL server and instance, the following event details are displayed: event date and time, event type and status.

All events in error log

This InTrust report shows all events in SQL Server Error log. For each SQL server and instance, the following event details are displayed: date and time, event type and status.

Replication

Miscellaneous agent history

This InTrust report shows events from the history of auxiliary agents. For each SQL server and instance, the report displays the following event details: agent name, date/time, step number (Step# - 0 for a job outcome), step, status, message.

Replication agent history

This InTrust report shows events from replication agent history. For each SQL server and instance, the report displays the following event details: agent name and type, date/time, agent status, error number and message.

Report Pack for SUSE Linux

This section contains a list of reports included in the InTrust11.4.2 Report Pack for SUSE Linux.

Administrative Activity

- Account Management
- Policy Changes

Account Management

SUSE Linux group management

This InTrust report shows instances of group creation and deletion. Click the Details link for a particular group to see the details of the group management action in a sub-report.

SUSE Linux group membership management

This InTrust report shows instances of members being added to groups and removed from groups. You can organize information in several ways for convenient analysis.

SUSE Linux user management

This InTrust report shows instances of user account creation and deletion. Click the Details link for a particular user to see the details of the user management action in a sub-report.

Policy Changes

SUSE Linux configuration files modifications

This InTrust report shows instances of plain text file modification. This lets you find out whether changes were made to particular Linux configuration files. The report displays when strings were added or removed, but does not include the actual changes. If a line was modified, the report treats this as a combination of line deletion and line addition.

Syslog

All SUSE Linux syslog Events

This InTrust report is designed for manual analysis of Red Hat Linux Syslog messages. Use filtering by date and time, host, message source and message content to find out the information you need.

SUSE Linux failed login attempts

This InTrust report shows details of failed Linux login attempts.

SUSE Linux login statistics

This InTrust report shows how many successful and failed Linux logins occurred within the specified period of time. It also displays the number of cases when there were multiple consecutive failed logins, which indicates possible password-picking activity.

SUSE Linux multiple failed login attempts

This InTrust report shows details of situations when multiple failed Linux login attempts occurred in a row. Click a number in the Count column for a particular attempt to view the original Syslog messages about each attempt.

SUSE Linux user sessions

This InTrust report shows details of the start and finish of Linux user sessions.

Reports for Syslog

This section contains a list of reports included in the InTrust11.4.2 Knowledge Pack for Syslog.

Syslog

All Syslog events

This InTrust report shows all syslog events were gathered by InTrust for Syslog.

Report Pack for Microsoft TMG and ISA Server

This section contains a list of reports included in the InTrust11.4.2 Report Pack for Microsoft TMG and ISA Server.

Security

Advanced Forensic Analysis

Faults

Audit subsystem faults

This InTrust report displays ISA Server audit subsystem faults. It helps you identify logging and auditing problems. In some cases, these faults are specifically provoked to prevent logging. Therefore, such situations need to be monitored.

ISA services faults

This InTrust report displays ISA Server audit subsystem faults. It helps you identify logging and auditing problems. In some cases, these faults are specifically provoked to prevent logging. Therefore, such situations need to be monitored.

ISAS miscellaneous faults

This InTrust report shows miscellaneous faults, such as network configuration errors or insecure configuration errors.

ISAS Packet filtering faults

This InTrust report helps you analyze problems related to packet filtering, such as packet filtering protocol violations, disabled packet filtering, and others. Use the Events filter to specify what events will be included in the report.

Network Activity

Firewall all connections

This InTrust report helps you analyze sessions that take place through the firewall.

Firewall all connections [detailed]

This InTrust report helps you perform a detailed analysis of connections through the firewall.

Requests by Network [chart]

This InTrust report shows how many requests were received by the selected destination network from the selected source networks in the specified time period. The report is based on data from the ISAS Firewall and ISAS WebProxy logs.

VPN Sessions [by Server and User]

This InTrust report shows the VPN sessions grouped by RAS server and User. Information shown includes session duration and volume of the transferred data. Report is based on data from Windows System Log.

Web proxy all requests

This InTrust report helps you analyze Web proxy requests.

Server Management

ISA services tracking

This InTrust report displays tracking events (start, stop, pause, and resume) for ISAS services (Firewall Service, Web Proxy Service, and ISAS Control Service). Use the Events filter to specify which service tracking events will be included in the report.

Common Security Incidents

Attacks

Network Probes

- **Firewall port scanning**

  This InTrust report displays information on frequent sessions (or series) of port scanning. Port scanning is used by intruders to detect server configuration.

- **Firewall well-known ports connection attempts**

  Intruders scan well-known ports to determine specific services available on the server. Well-known ports are those with numbers from 0 to 1023. You can use the Ports filter to limit the report to a subset of these ports.

Firewall triggered rules

To prevent unwarranted access to resources, firewall rules are configured. When a firewall rule is triggered due to a corporate policy violation, an event is logged in the ISAS Firewall log. This InTrust report helps you determine who violated the firewall policy.

ISAS built-in intrusion detection

This InTrust report shows information on several well-known types of attacks detected by ISA Servers built-in intrusion detection system. The report provides information on spoof attacks, ping-of-death attacks, UDP bomb attacks, and others.

Prohibited User Activity

Web proxy web surfing daily statistics

This InTrust report displays attempts to browse restricted web pages by user. You can use the Restricted Pages filter to define what pages are proscribed. To do it, add a list of keywords to the filter. Such pages may include pornography or e-commerce sites.

Usage Statistics

- ISA Firewall
- ISA Web Proxy

ISA Firewall

Firewall daily traffic [chart]

This InTrust chart shows statistics on daily requests for ISA Firewall service.

Firewall total statistics

This InTrust report provides aggregate statistics for ISA Firewall service.

Firewall users activity daily distribution

This InTrust chart shows the daily activity levels of ISA Firewall clients.

Firewall users activity hourly distribution

This InTrust chart shows the hourly activity levels of ISA Firewall clients.

ISA Web Proxy

Authenticated Clients Audit and Statistics

Web proxy site requests by date

Web proxy site requests by user

Web proxy traffic by user [chart]

This InTrust chart provides traffic statistics (in Kbytes) for Web Proxy authenticated clients.

Files Statistics

Web proxy file downloads

This InTrust report lists all potentially dangerous files downloaded by the Web Proxy clients.

General Information

Web proxy daily traffic [chart]

This InTrust chart shows the daily incoming/outgoing traffic of ISA Web Proxy service.

Web proxy total statistics

This InTrust report provides aggregate statistics for ISA Web Proxy service.

Hosts Audit and Statistics

Web proxy requests statistics

This InTrust report contains information on all requests for ISA Web Proxy hosts.

Web proxy traffic by host [chart]

This InTrust chart provides traffic statistics (in Kbytes) for ISA Web Proxy hosts.

VMware vCenter and ESX/ESXi Reports

This section contains a list of reports included in the InTrust11.4.2 VMware vCenter and ESX/ESXi Reports. These reports are based on VMware vCenter, ESX and ESXi tasks and events retrieved via vSphere Web Services SDK.

VMware vCenter and ESX/ESXi

Virtual machine creations and deletions

This InTrust report shows information about virtual machine creation, deletion and cloning.

Virtual machine reconfigurations

This InTrust report shows virtual machine configuration changes.

Virtual machine snapshot activity

This InTrust report shows all captured activity that involves snapshots: creation, deletion and reversion.

Virtual machine startups and shutdowns

This InTrust report shows all virtual machine starts, shutdowns, suspends, and details as to who initiated them and when they happened.

VMware All Events

This InTrust report shows all events related to VMware vCenter and ESX/ESXi.

VMware ESX Configuration Changes

This InTrust report shows events related to vCenter and ESX/ESXi server configuration changes, such as account, host and data store management.

VMware Permission Changes

This InTrust report shows permission changes on virtual machines. The report refers to users and groups that get role-based permissions as grantees.

VMware User Logon and Logoff

This InTrust report shows all user logon and logoff attempts, both successful and failed, and provides reason information for the failed attempts.

Report Pack for Windows

This section contains a list of reports included in the InTrust11.4.2 Report Pack for Windows.

Administrative Activity

- Account Management
- Network Management
- Policy Changes

Account Management

Group Management

This InTrust report shows group changes. Groups should be created, deleted, or changed by administrators. If the administrator fails to duly perform group management tasks, this may lead to user rights misrule and security violations.

Group Membership Management

This InTrust report shows group membership changes. User accounts should be added to or removed from groups by administrators. If the administrator fails to duly perform group membership management tasks, this may lead to user rights misrule and security violations.

Password resets

This InTrust report shows when account passwords were reset and who reset them. An entry in the report means that the password was either reset or changed. By default, only user accounts are included, but you can use the User Accounts filter if you want to include computer accounts as well.

User Accounts Management

This InTrust report shows changes to user accounts. User accounts should be created, deleted, enabled, or disabled by administrators. If the administrator fails to duly perform account management tasks, this may lead to account misrule and even security violations.

User rights management

This InTrust report shows changes to user rights. User rights should be assigned or removed by administrators. If the administrator fails to duly perform user rights management tasks, this may lead to user rights misrule and security violations.

Network Management

Computer accounts changes

This InTrust report shows computer accounts changes. Computer accounts should be created, deleted, renamed, or changed by administrative accounts only. If the administrator fails to duly perform computer account management tasks, this may lead to security violations.

DHCP history

This report summarizes DHCP log data and represents the information as time intervals during which computers have certain IP addresses. If an event specifies the host as localhost or host from localdomain, the actual DNS name is determined by the MAC address. The report helps quickly pinpoint a computer at which certain actions were performed. For correct results, create this report for a single DHCP server or for several DHCP servers that work simultaneously and do not serve overlapping IP address pools.

Domain Trusts Changes

This InTrust report shows domain trust changes. Domain trusts should be added, removed, or modified by administrative accounts only. If the administrator does not duly perform domain trust management tasks, this may lead to security violations.

Policy Changes

Audit Policy Changed

This InTrust report shows audit policy changes. Audit policy should be modified by administrative accounts only; otherwise these changes can indicate a security breach. Failure of the administrator to duly perform audit policy management tasks may lead to security violations.

Kerberos and Domain Policy changed

This InTrust report shows Audit and Kerberos policies changes.

Forensic Analysis

- Detailed Reports
- Summary Reports

Detailed Reports

All user activities [details]

This InTrust report shows and expands statistics on security events. Security events capture the activity taking place in the network and show, for example, when and where users log on, what data they access, how they manage accounts, and so on.

Event Log Gaps

This InTrust report shows situations when events are missing from logs for a time period that you specify. For example, if a file server with classified data does not appear to have logged events for an hour, this is suspicious, all the more so if the server is supposed to be up at all times. It is possible that the server was down during that time or the log was cleared. Such a situation does not necessary mean a problem but should be investigated.

Events related with the specified event [advanced]

This InTrust report helps you analyze the background of an event you are interested in by exploring related events.

Raw data analysis

This InTrust report shows event data from specified event logs of selected computers.

Summary Reports

Account management statistics

This InTrust report shows the number of accounts created, changed, and deleted within a specified time period for such important types of accounts as user accounts, security groups, and distribution groups. It also shows group membership modification for both security and distribution groups.

All user activities [summary]

This InTrust report shows statistics on security events grouped by users and their domains. Security events capture the activity taking place in the network and show, for example, when and where users log on, what data they access, how they manage accounts, and so on. The report is primarily intended for presenting statistics in printed form but, when working interactively, you can click any number to view the details of all events that the number stands for.

Logon Statistics

In the Windows environment different logon types are registered by the system depending on what kind of resource a user accesses. This InTrust report shows all logon types such as interactive logons to domains, access to shared folders, dial-up connections to the network, and so on, and groups logon statistics.

Major Security Events

Event log cleared

This InTrust report shows event log cleared events. Event logs should be cleared only when there is lack of free space, which rarely occurs. Therefore, instances of event logs being cleared can indicate intruder activity and attempts to cover the tracks.

System Time changed

This InTrust Report shows the occurrences of System Time Change event. Time synchronism is a critical condition for most network environments. Unauthorized manual time change can cause improper functioning of services, business applications and authentication subsystem.

User account lock-unlock

This InTrust report shows user account locked out and unlocked. A user account can be locked in accordance with the Account Lockout Policy (as a rule, after an incorrect password is entered several times in a row). Such a situation may mean password-guessing, especially if an administrative account gets locked. Click a user account in the report to view its details.

Normal User Activity

- Logons
- Object Access
- Remote Access

Logons

Suspicious Logons

Logons during non-business hours

Users do not normally logon to the system during non-working hours. An abnormal number of logons during non-business hours may indicate an intrusion attempt. With this InTrust report, you can examine every attempt in detail to find out who was doing what during the specified time interval.

Logons with built-in account names

This InTrust report shows logons with built-in account names. Almost every system includes a number of built-in accounts (Guest, Administrator, etc.). These accounts are primary targets for intrusions and attacks because their names are well-known. Intensive successful logons using these accounts can indicate an intrusion attempt.

Multiple Logon Failures

Multiple logon failures can indicate a brute-force attack. This InTrust report provides detailed information on logon failures, including the user account, the reason for failure, the logon type, etc. Click a number in the Attempts column to find out details of logon failures in a subreport.

Multiple logons failure [Windows-Kerberos-NTLM]

This InTrust report shows failed logons that came in series. In the report, a series is several logons of the same type from the same computer within the specified time interval. Kerberos, NTLM and Windows events are displayed separately for each domain.

Usual Logons

Account logon events [NTLM]

NT LAN Manager is a traditional password-based authentication protocol for Windows-based networks. This InTrust report displays information on NT LAN Manager audit results.

Active Directory Administrator Logons

This InTrust report documents all logons to domain controllers by users with administrator equivalent user rights.

All logons

This InTrust report shows successful and failed logons of all types. For failed logons, reasons are displayed. This helps analyze who tried to log on to which computers from which workstations.

All logons [with hyperlinks]

This InTrust report shows successful and failed logons of all types. For failed logons, reasons are displayed. This helps analyze who tried to log on to which computers from which workstations.

Domain Account Authentication

This InTrust report is intended to show account logon events on Domain Controllers including both NTLM and Kerberos authentication.

Logon activity trends

This InTrust chart graphically represents logon activity in your network, visualizing, for example, statistics for logons that failed due to different reasons (for example, bad password, disabled user account, etc.). The chart allows you to detect trends in logon activity and analyze anomalies.

Successful Authentication ticket granted

This InTrust report shows successful account logons based on kerberos events.

Object Access

Active Directory object access [DS logging]

This InTrust report shows Active Directory object access attempts. Access to some types of objects may be unwarranted. The report is based on information from the Directory Service log, and it complements the Active Directory object access report.

Active Directory objects access

This InTrust report shows Active Directory object access attempts. Access to some types of objects may be unwarranted. Such events often indicate changes to the environment, and they need to be tracked. Note This report is based on object access events from the Security log.

File Access

This InTrust report shows file access attempts. Access to certain files may be unwarranted.

Group Policy Object access

This InTrust report shows Group Policy objects access attempts. Access to this type of objects may be unwarranted. Such events often indicate changes to the policies, and they need to be tracked. Note This report is based on object access events from the Security log.

NTFS audit [Windows XP 2003 and later]

This InTrust report helps you analyze the files and folders audit events from the Security log (Windows XP, Windows Server 2003 and later). If files or folders are accessed through network shares rather than locally, the report does not show such situations. Use report filters to precisely find out the information you need.

Registry Access

This InTrust report shows attempts to access registry keys. Access to some registry keys (particularly the startup keys) may be unwarranted.

Registry Value Modifications [Windows 2008 Vista]

This InTrust report shows modifications of the registry values on Windows 2008, Windows Vista machines. The report is based on EventID=4657. Note: Some value changes cannot be displayed due to specific data type.

Remote Access

RAS authentication failures

This InTrust report shows situations when a user failed to authenticate with the remote access server. Sometimes this means a failed attempt to gain unauthorized access to resources.

Software and System Audit

- Security Subsystem Events
- Software Applications

Security Subsystem Events

Active Directory security subsystem faults

Active Directory subsystems (for example, Net Logon) provide for security functions; therefore, errors in their operation may indicate security breaches. This InTrust report helps track such errors.

Event Log Errors

Errors or warnings from the event log could be an indication of intruder activity or an auditing system malfunction. This InTrust report shows situations when event logs generated warnings or errors.

Logon Components Failures

This InTrust report shows situations when a logon failed because the Net Logon service was not running or because an unspecified error occurred. The Net Logon service is used for authenticating users and services via a secure channel between a workstation and a domain controller. The report helps respond to such significant errors as soon as possible.

Policy enforcement errors

This InTrust report shows some events from the security policy subsystem which could be an indication of intruder activity or a potential security breach.

Windows File Protection System Events [except Windows 2008 Windows Vista]

This InTrust report shows windows file protection system events. They indicate activity that might affect critical system files. Events not caused by legitimate tasks (such as installing or uninstalling software) may indicate intrusion attempts.

Software Applications

Process executed summary

This InTrust report summarized each program executed by server and how many times the program was executed during selected time period.

Process tracking

This InTrust report shows whether the applications you specify were started. If an application is prohibited, its launch may indicate a security issue. What is more, running restricted software often means corporate policy violations.

Server Reboots

This InTrust report shows the number of reboots for the servers in your environment within a specified time period. Click a number in the Count column to view details of each reboot event in a subreport. If reboots are too frequent or too numerous, this may indicate a problem with the computers where they occur.

Server reboots [Win2003 Win2008]

This InTrust report shows both expected and unexpected server reboots (Windows 2003, Windows 2008 only). Notes: Please ensure than Shutdown Event Tracker service is enabled at your servers.

Service installation attempt

The set of system services installed is a significant term of server configuration. Unauthorized service installation attempt may indicate that system intrusion is occurred. This InTrust report is based on the following events: 4697 for Windows 2008/Vista, 601 for other Windows versions

Software installation

This InTrust report helps track what software products are installed or failed to install on which computers. The report shows only those products whose setup programs use Windows Installer. Using the Grouping filter, you can organize the information as necessary. To see what software was installed on particular computers, use grouping by computer. To find out where certain software products were installed, use grouping by software product.

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

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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.**

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

InTrust [Guide Name]
Updated - September 2020
Version - 11.4.2