Acumen Int. Corp.
6F, No. 207-3, Sec. 3, Beisin Rd, Sindian Dist
New Taipei City 23143, Taiwan
Tel +886 (0)2 8913 22 33
Fax +886 (0)2 8913 22 55
sales@acumenin.com
www.acumenin.com

ACUMEN AiD
User Manual

Data Security

Copyright

◆ Copyright

◆ Note

The information in this document is subject to change without notice and should not be construed as a commitment by Acumen Int. Corp. While every effort has been made to assure the accuracy of the information contained herein, Acumen Int. Corp. assumes no responsibility for errors or omissions. Acumen Int. Corp. assumes no liability for errors in this document or damages resulting from the use of the information contained in this document.

Index

1. Introduction

1.1 Preface

Corporate information becomes more important under the era of intellectual economy. The critical factor for success is to protect information effectively. With the fast growth in information technology, internet becomes an important channel to communicate between customers and corporations. Despite its convenience, information is more easily leaked. As important information leakage brings loss to corporations, a comprehensive control of computer usage is important. It controls and reduces the risk of loss caused by leakage of the confidential information and/or abuse of corporate resources and intellectual property.

More and more employees spend their time in browsing websites that are unrelated to work during working hour. Such behavior decreases productivity. Many employees may think that the office computers are their personal property; they can do whatever they want with the computers. Corporations should control and monitor their behaviors in order to enhance productivity and minimize the risk of misuse of computer resources.

According to researches of the Gartner Group and Forrester Research, nearly 50% of time within the MIS department has been spent on computer installation and software upgrading which occupy a large proportion of the computer cost. System administrators spend 70-80% of time working on daily maintenance tasks which increase the cost of computers. Moreover, productivity drops when computer problems cannot be solved immediately. Therefore, it is necessary to reduce the workload of system administrators on minor tasks to increase their productivity so that they can concentrate on computer management tasks and information system enhancement.

AiD is powerful software to solve the above problems for corporations. AiD can monitor and record the utilization of every computer. Its functions include daily operation statistics, policy management, screen snapshot, real-time recording, asset management, system patch management, software distribution, and remote control, etc. AiD can automatically record screen snapshots, record computer utilization, and playback records. With all these functions, corporations can realize the computer resources utilization, secure corporation information, and enhance productivity.

1.2 Feature Introduction

AiD provides effective monitoring and managing capabilities to help corporates minimize their risks in information security. AiD is an application to effectively monitor and manage corporate network activities, including:

AiD main feature includes：

◆ Application Management

- Record application usage logs
- Statistics report on application usage time or percentage
- Restrict application usage

◆ Website Management

- Record browsed website’s URL and title
- Statistics report on website browsed time and percentage
- Restrict website domain or page access

◆ Document Management

- Record all document operation activities include operations on various type of storage device and document file type
- Record shared file modification and deletion
- Complex policy settings allows to control document read, modify and delete operation
- Backup important file before copy, modify and delete

◆ Print Management

- Record and log all print task
- Record printed content as image
- Control print events

◆ Device Management

- Control all computer external devices
- Control all newly added device

◆ Screen Snapshot Management

- Real time viewing of end user computer screen snapshots
- Record end user screen activities, recording interval can be set per application
- Convert screen history into WMV format for replay purposes

◆ E-mail Management

- Record sent and received email with complete content and attachments
- Control Email sending by defined policy

◆ Instant Message Management

- Completely record instant message conversation time, contact person and content
- Control file sending using instant message application
- Backup sent file

◆ Remote Maintenance

- Instant view of end user computer information and perform remote assistance
- Remotely connect to end user computer and perform remote control
- Ability to remote file transfer

◆ Storage Device Management

- Record USB storage device’s usage within the network

environment

- Set read and write authority to restrict USB access right
- Automatically encrypt or decrypt files copy to USB storage device, encrypted file on device will be unreadable in non-authorized computers

2. Installation and Deployment

2.1 Basic Structure

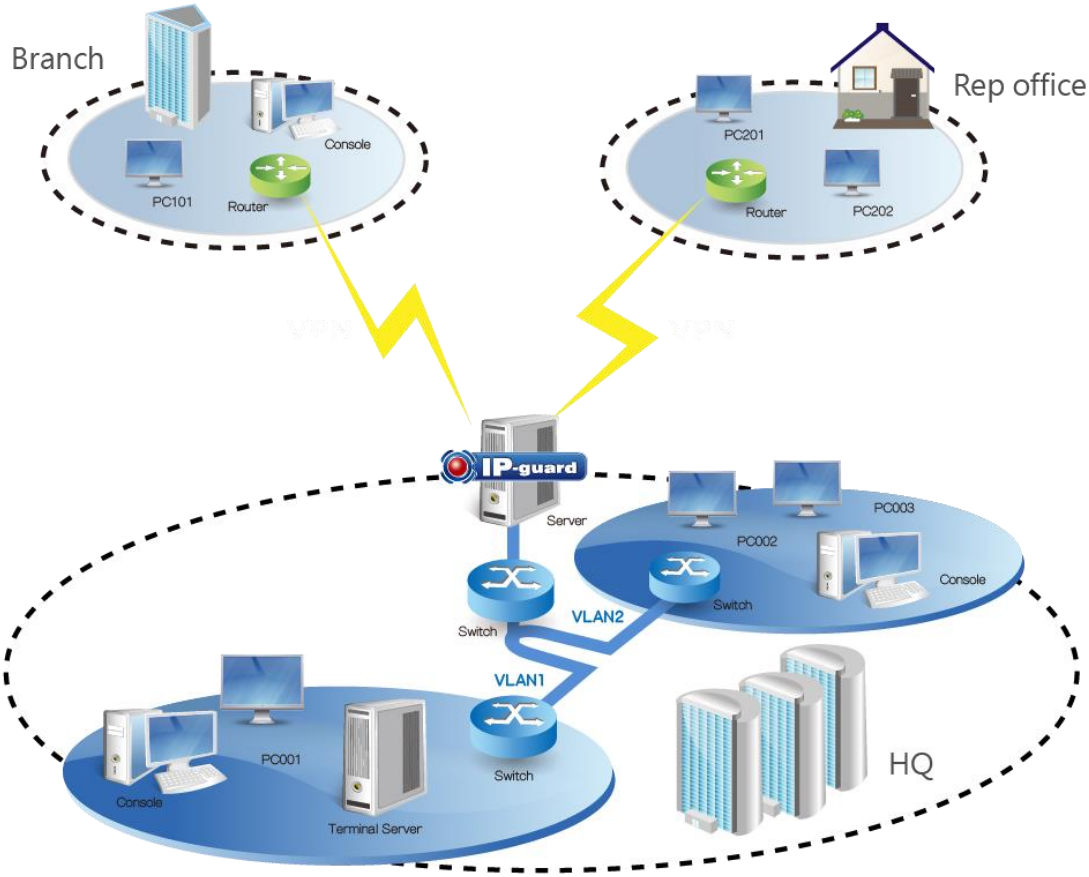
AiD consists of three major components, agent component, server component and console component. Components can be installed independently on the network environment.

Agent Component: Installed on end user computer to collect operation logs and execute defined policies

Server Components: Used to store system information, agents logs and policies. Generally server component installed on high performance servers with massive hard disk storage space.

Console Component: Used to view system log, set policies and instant maintenance. Console component can be installed on administrator's compute or on the same computer as the server component.

Basic system architecture：



AiD’s network structure based on TCP/IP protocol, LAN can be extended via VPN or the World Wide Web. Computers on the networks can be centrally manage and control via above-mentioned set up.

◆ Server component’s basic feature includes:

- Manage and communicate with end point computers
- Collect and store retrieved information from end point computers
- Provide easy to use interface to manage, view, category and search recorded logs

◆ **Console component's basic feature includes:**

- View and audit recorded log collected from end point computers
- Statistic, analysis and export end point computer logs
- Real time monitoring and system management to end point computers
- Define/Apply monitor and management policies

◆ **Agent component's basic feature includes:**

- Execute various type of policies defined by administrator
- Collect all end point operation logs
- Routinely sending retrieved data back to server
- Monitoring end point computer activities by following administrator's command
- Monitor and control end point computer per administrators request

2.2 Hardware/Software Requirement

Microsoft SQL database is a pre-requisite for any AiD server installation.

Chat below shows each AiD components' minimum requirement

Component	Basic Requirement
Database	SQL Server 2000 SP4 / MSDE SP4
	SQL Server 2005 SP1（x86 / x64） / SQL Server 2005 Express SP1 (x86 / x64)
	SQL Server 2008 (x86 / x64) / SQL Server 2008 Express (x86 / x64)/SQL Server 2008 R2

Component	Basic Requirement
Server	OS: Win2000 SP4 / Win 2003 SP1(x86 / x64) / Win 2008 (x86 /x64) /Win 2008 R2 Minimum Requirement: Pentium4 2G / 512MB RAM / 20GB HDD Space Recommend Requirement: Pentium4 dual core or quad core / 4GB RAM / 120GB HDD Space
Console	OS: Win2000 / XP (x86 / x64) / 2003 (x86 / x64) / Vista (x86 / x64) / Win 2008 (x86 / x64) / Win7 (x86 / x64) /Win 2008 R2 Minimum Requirement: Pentium III 500/256MBRAM /256MB available HDD Space Recommend Requirement：Pentium4 / 512MB RAM / 1GB available HDD Space
Agent	OS: Win 2000 / XP (x86 / x64) / 2003 (x86 / x64) / Vista (x86 / x64) / Win2008 (x86 / x64) / Win7 (x86 / x64) /Win 2008 R2 Minimum Requirement: Celeron III 500 / 512MB RAM / 512MB available HDD Space Recommend Requirement：Pentium 4 / 512MBRAM / 1GB available HDD Space

Note: KB 891861 required when installing server component on Windows 2000 SP4

2.3 Installation

2.3.1 System Installation

Please select document according to your Microsoft SQL Server Version

AiD installation with SQL 2000 SP4.pdf

AiD installation with SQL 2005 express sp2.pdf

AiD installation with SQL 2008 express.pdf

AiD console installation.pdf

CheckCode.pdf

Remote Installation Requirement.pdf

AD script deployment.pdf

2.4 System Upgrade

2.4.1 Upgrade Server and Console

Please refer to the attached document to upgrade your product

Product upgrade.pdf

2.4.2 Agent Component Upgrade

After server successfully updated, agent update file will not be dispatch to end point computers, it requires administrators activation in order to dispatch update files to agents. To activate agent dispatch feature go to AiD console --> Server Management --> Agent Update Management to set up distribution time and computer.

2.5 Removal

2.5.1 Remove Agents

There are two methods to remove AiD agent from the end user computer by administrators.

- **Console Removal**

  Go to AiD console --> control --> uninstall agents to remove agent on computer no long require monitoring.

- **Agent Uninstaller Utility**

  AiD console allow administrators to generate an offline uninstaller to remove agents on offline computers. Follow steps below to generate uninstaller.

  1) In AiD console go to Tools --> Agent Tool -->Agent Offline Utility

  2) Select “Permanently uninstall agent” and next

  3) Set Parameters include maximum execution of the exe file, effective time, password, save path

  4) Execute the generated file on end user computer and AiD will be removed permanently

  Note: Removing agent using agent uninstaller utility tool will not reduce license count in AiD console. Manual deletion required to regain user license count.

2.5.2 Uninstall Server and Console

To uninstall AiD server and console, go to Windows start menu --> all programs --> AiD --> uninstall AiD or uninstall via Control panel --> Add/Remove programs.

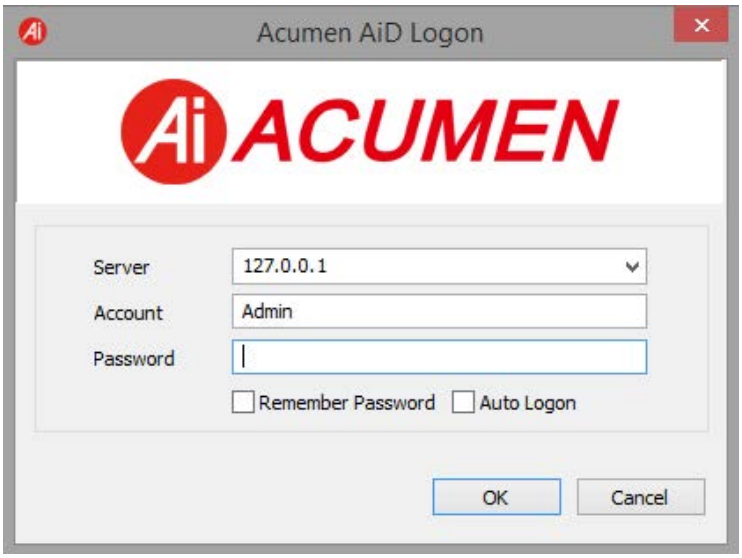
3. Console

3.1 Console Login

3.1.1 Console Login

Execute OConsole3.exe in AiD installed path or go to Start --> All Program files --> AiD Console

AiD server needs to be in service in order to allow console access.



Login screen include the following

Item	Description
Server	AiD server IP address
Account	Default administrator login account set as “admin” and Audit account as “audit” Administrators can create multiple account with different credentials by go to “Tools --> Account” in console
Password	Admin account’s default password set as blank, password may be changed by go to Tools--> Change Password in console

Item	Description
Remember Password	Remember password used to logon Remember password setting can be removed by go to Tools--> Options -->Console Setting --> Basic Settings --> Login Settings and unselect Remember Password
Auto Logon	Auto Logon will automatically login to console using last successful logon user's detail Auto Logon setting can be removed by go to Tools--> Options -->Console Setting --> Basic Settings --> Login Settings and unselect Auto Logon

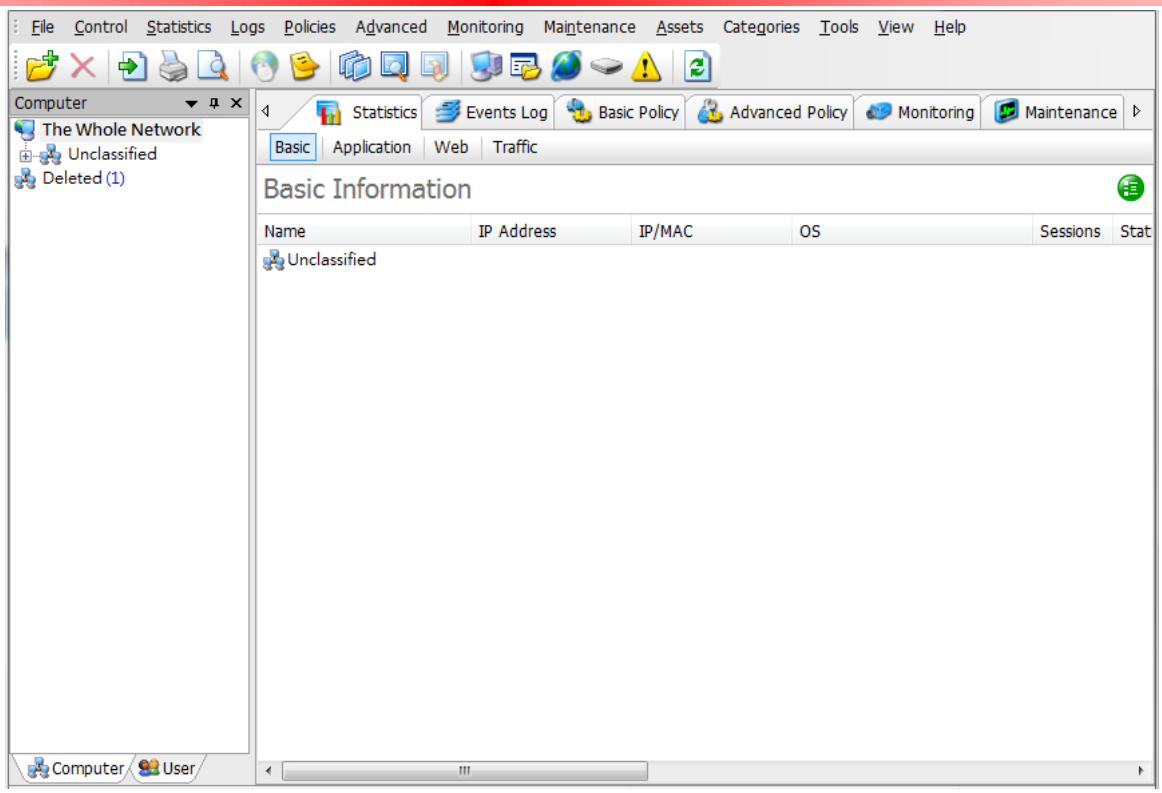
Tool --> Re-logon allows administrators to logon to another AiD server or logon to AiD server as using another user account

3.1.2 Change Password

Once logon to console password can be change in Tools --> Change Password, it require users to enter old password, new password and confirm new password to make change effective.

3.2 Console Introduction

Follow screen capture displayed first page after logon



Console includes the following:

Items	Description
Tool Bar	System menu
Menu Bar	Display short cuts of common functions
Computer List	Situate at left hand side panel of the console, display all computer and group information
User List	Situate at left hand side panel of the console tab can be switch between computer list and user list
Navigation Main Menu	Underneath menu bar is quick switch between main functions
Navigation Sub Menu	Quick access to the functions falling under navigation menu
Function Button Panel	Function buttons such as data sorting, add/delete/apply policy etc.
Data Display Panel	Area display all data

Items	Description
Chart Panel	Only available for statistics report to show result in chart format
Search Panel	Search Panel only available for Statistics Report, Event Logs, Instant Message, Emails
Property Panel	Available for setting policy purposes
Status Bar	Display current system status at bottom of this screen

◆ Color represent action of agent status

Icon	Color	Description
	Light Blue	Active agent
	Light Gray	Computer is not on the network or switched off
	Dark Gray	Agent uninstalled
	Light Blue with Clock	Active agent but user is away

◆ Color Representation of User Icon

Icon	Color	Description
	Colored	User on agent computer is active
	Light Gray	User not logon to the agent computer

System Logs and Search Conditions

Event logs will include following common columns

Column	Description
Time	Event log time

Computer	Name of the computer event occurred, computer name can be found in the computer panel
User	User trigger the event, user name can be found in the user panel

Searching condition for event log and statistic reports

Condition	Description
Time Zone	Used to search event log within a given period. To search between time range check on from and to check box to select starting and ending time
	Used to select previous week
	Used to select next week
	Restore to previous setting
Time	Time type (All Day, Working Time, Rest and Weekend) can be found in Tools --> Classes Management --> Time Types
Network Range	Click on the right hand side button to select single computer or group of computers

3.3 Computer and User Operation

3.3.1 Basic Information

Select from Statistics --> Basic will allow administrators to view computer, computer group, user or user group information.

1. **Computer Basic Information**

   Select a computer in computer panel at the same time data panel will display detail information of selected computer

Item	Description
Name	Displayed name in the Computer Tree can be changed, By default computer name will be used
Computer	Computer name
IP Address	Computer's IP address
Status	Agent status: Running, Offline, Uninstalled
Version	AiD agent version
OS	Operating System
Last Online	Last communication time between AiD Agent and Server
Last Active Time	Last time computer was record as activate
Installed time	Agent installed time
IP/MAC	All IP/MAC address of the Agent
Last Logon User	Last user logon to agent computer, status also displayed

In the event of multiple user logon to the agent computer, console will display time and name of all user current logon to the system.

2. Computer Group Information

All computers under a group will display in the data panel when computer group selected. By selecting "The Whole Network" and click on expend button "  ", information of all computers within the group will be displayed.

3. User Basic Information

Select a user in the user panel and user status will be displayed in the

data panel

Item	Description
Name	Displayed name in the computer tree can be changed, by default computer name will be used
User	User login name. For domain users domain/user name will be displayed
Status	Agent status: Running, Offline, Uninstalled
Last Online	Last communication time between AiD Agent and Server
Last Active Time	Last time computer was record as activate
Last Logon Computer	Last user logon to agent computer, status also displayed.

In the event of user logon to multiple computers, last logon computer column will show time and computer user logged on

4. User Group Basic Information

Select a group to list users in that group and expand "  " Button can be used to expand all subgroups.

3.3.2 Grouping

By default all new agent computers fall into unclassified group, group structure can be create for easy maintenance purposes

◆ Create New Group

In computer panel select "The Whole Network" and go to File --> New Group to create new group in computer tree. Computers can be drag and drop into created group. Administrators can repeat this process to create multiple computer or user groups.

Note Unclassified group been set as default group for both

computer and users. Unclassified group cannot be modify, delete or create sub-group within it.

◆ Assign and Change Group

To assign computers or users to a group follow steps below

1. Select computer or user and go to File --> Move and choose target group.
2. Drag and drop computer into targeted group

Note: To move multiple computers, select unclassified and go to Statistics --> Basic, hold Ctrl or Shift button to select multiple computers and move at once.

3.3.3 Search

Administrators can used search feature to find desired computer or user and view its related information

◆ Search Computer and User

Search function can be found by go to File --> Find. In the search window it support fuzzy search on user name, Computer name, IP Address, MAC Address or all above mentioned field. Click on the search result it computer basic information will be display on data panel.

3.3.4 Delete

Computer/ computer group/ user/ user group can be deleted by go to **File->Delete.** Deleting computer (group) will uninstall Agents on selected group or selected computers. Deleted computer will be placed into deleted group and history logs are available for query.

Computer in the deleted group will not take up license count. In the event of reinstall AiD agent onto deleted computer, computer will automatically fall into its original group.

3.3.5 Restore

Restore found in File →Restore, feature can be used to restore computer in deleted group to its original group. . After restore process license will be calculated regardless of agent activation status.

3.3.6 Rename

For management purposes, administrators have the ability to rename computers into meaningful names. To rename computer go to File --> Rename it will make change on the console immediately

3.3.7 Data Sync

Priority sync setting gives a computer first priority to sync policy and data with server. To activate this feature, right click on the target computer --> Data Synchronization -->Priority to Sync Data.

Note system will only allow one computer set as priority computer per server.

3.4 Control

Administrators control active agents via AiD console component; however console can only control agent computer in running state.

Note: Control does not work in user mode.

3.4.1 Notification

Console component can send notifications to agents on the network. Follow steps below to send notification message

1. Select group or a computer name
2. Go to Control --> Notify
3. To send pre-define message click on  to select message or type in any

message in the content window

3.4.2 Lock/Unlock Computer

AiD has the ability to lock an agent computer or group of computer's to prevent further misbehave event occurs. To lock computer go to Control --> Lock, locked computer will not have control over mouse and keyboard.

To unlock go to Control --> Unlock to enable mouse and keyboard of the locked computer

3.4.3 Log off user, Shutdown and reboot

AiD has the ability to power down/ log off/ restart/ agent's computer. To perform above mentioned actions go to Control --> Log Off/Power Down/Restart

3.5 Other Features

The following are the descriptions of common features that share with all modules

3.5.1 Import/Export

◆ Export Data

AiD's statistics report, event logs, policies, instant message contents, emails and asset management can be exported and saved as HTML /Text(CSV) / Excel (computer must be installed Microsoft's Excel program first) files.

1. Export Current Page

   To export current page logs, right click on event logs and select Export --> Records of current Page. By default page size is set at 20 rows per page, to change maximum page display go to Tools--> Options -->Console Settings --> Log viewing --> Number of records display per

page

2. Export All Match Records

   To export all match record, right click on the event logs select Export --> All matched records

   Exported document can be stored in CSV, HTML or Excel format

   Note: Microsoft office required for export in HTML and Excel format

◆ Import/Export Policies

Import policy generally used to synchronize policies between AiD servers, policies can be import to a computer or group of computers.

To import policy, select a group or a computer from the computer tree, right click on the policy panel and select a XML file to import.

To export policies right click on policy setting panel and select Export/Export Selected/Export All to export policies to XML format.

Export: Export all polices set for a specific computer or group

Export Selected: Export only the select policy

Export All: Export all policies in the server

3.5.2 Print and Print Preview

All data logs in Console can be print by select File --> Print, to preview print go to File--> Print Preview

4. Statistics

AiD can produce statistic report on application usage, internet browsing, and network usage as guideline for employees working performance.

4.1 Application Statistic Report

Application statistics provide powerful statistical result in computer daily operations and application usage. The statistical data can be used as reference by managerial personnel to assess employees' working behavior.

To generate statistic report go to Statistic --> Application then select date and time range, computer or group. By default system will query on today's application usage.

Button Descriptions

Items	Description
	Mode Button: can be change to By Category, By Class, By Name or By Group
	Expend Button: only active when mode changed to By Category, its use to expand all sub-categories. The button will display in gray when the button is not active
	Display Button: Set to display top 10/20/self-define number of records. Button will display in gray when not available

Running time and active time displayed by default; running time is the time computer has been run since start up. Active time means actual time in computer operation.

There are four different type of Application Statistics：

1. By Category

In category management, administrators can categorize used applications

into different categories. By producing category statistics report it can help managerial personnel to understand employees working behaviors

Select Mode Button --> By Category, the following information will show

Item	Description
Category	Self-define category in category management
Time	Time spend on the application of the category, in descending order
Percentage	Percentage of time spend on the application with in the category in descending order

2. By Name

Generate statistics report by selecting “Mode -> By Name”, report include display application name, time spend and percentage of select computer or computer group.

3. By Detail

List “By Detail” produced very similar report as “By Name” except “By Detail” list application by exe name rather than by applications. It implies two different version of Skype will be display as two separate records.

4. By Group

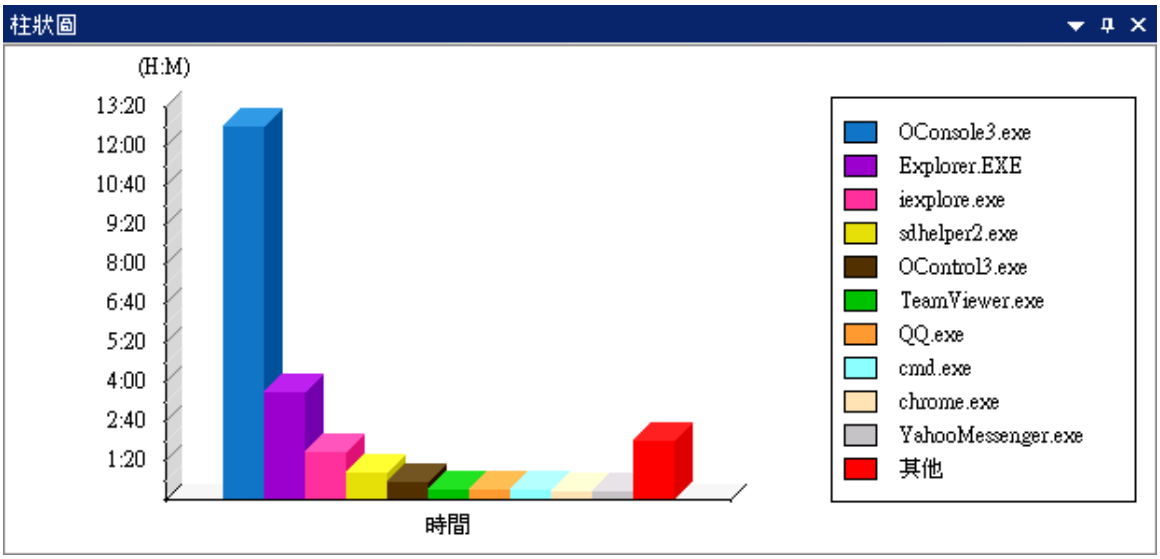
By Group is used to generate report on a computer or group of computer’s application usage within a category. Category details can be defined in categories settings.

For example to generate Instant Message Application usage report, following steps below:

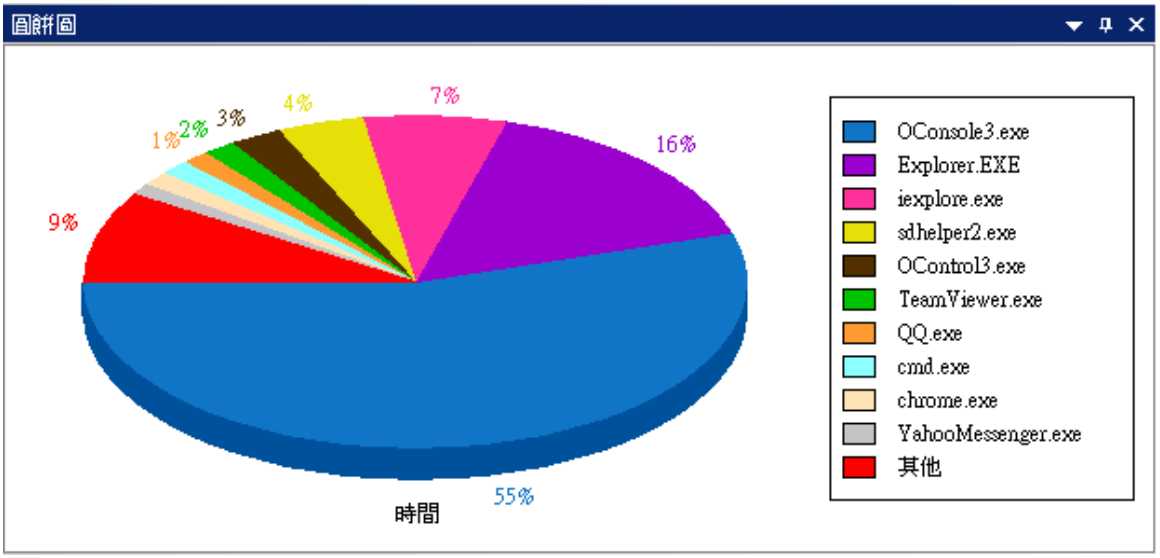
1. Create IM group in category management
2. Move all IM related applications in to IM group
3. Select computer group
4. In the search panel add categories buy click on category button
5. Click on Search to generate result
6. Click on expend button to see detail statistics for computer within a group

Charts included in statistics report

◆ Bar Chart



◆ **Pie Chart**



4.2 Website Statistics

Web statistics provide employees website browsing details. Report will help administrators identify end users browsing pattern and correct inappropriate behaviors.

Button Description

Items	Description
	Mode button: uses to search By Category, By detail or By Group
	Expend Button: only apply when mode set to By Category, its use to expand all sub-categories. The button will display in gray when the button is not applicable
	Display Button: Set to display top 10/20/self-define number of records. Button will display in gray when not applicable

There are 3 modes in Website Statistics

1. By Category

To generate website statistics report by category, administrators need to predefine a website category in category management. By default all website will be class under unclassified in descending order.

2. By Detail

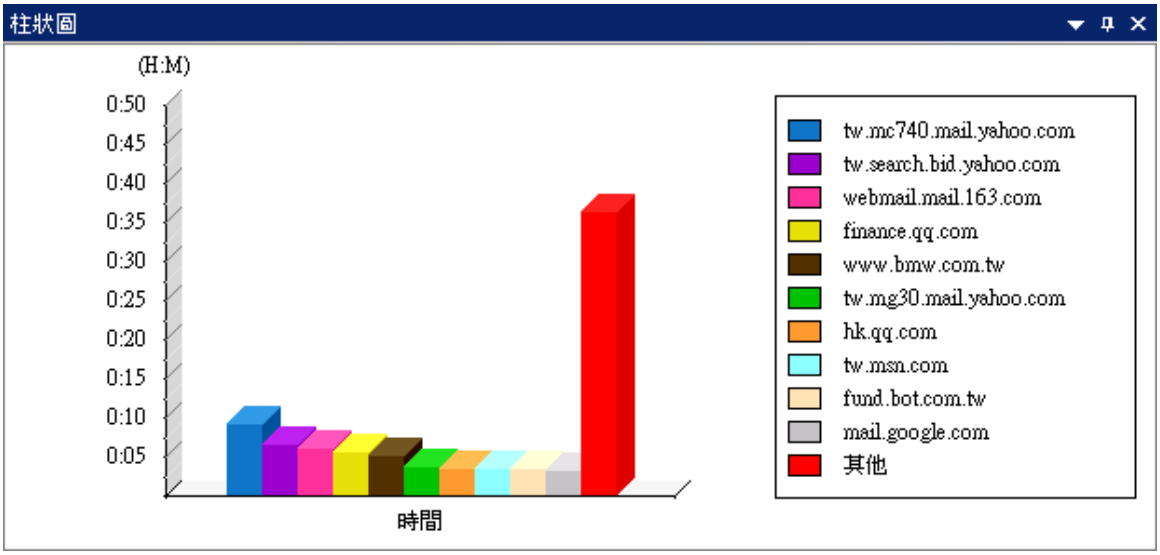
By Details will display visited website's URL along with time spend and percentage.

3. By Group

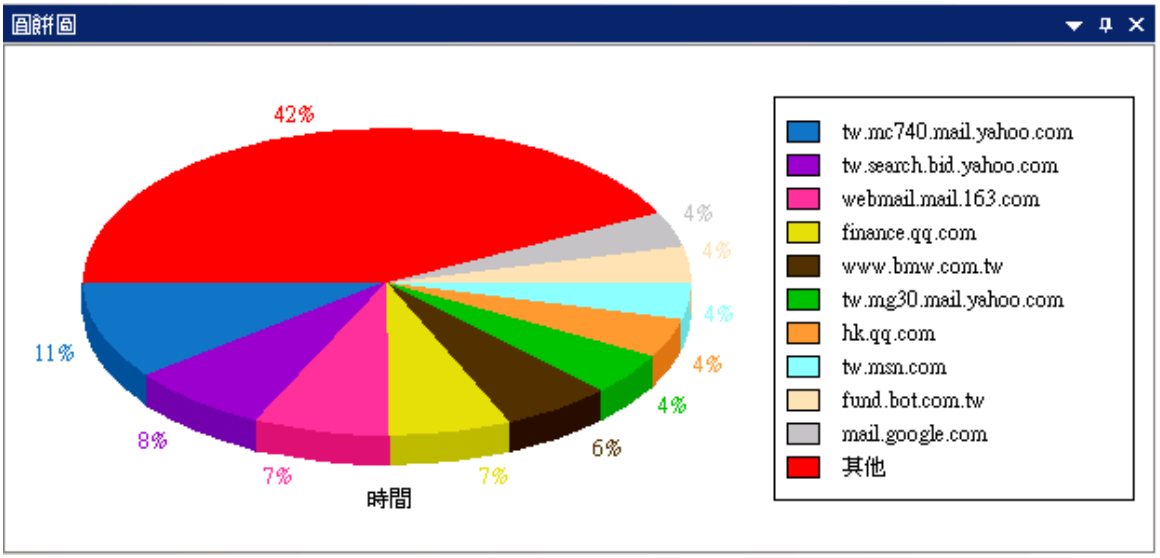
In this mode it displays browsing time of each computer on one or more categories. By default information displayed without any category (All), administrators can use search panel to list information by category.

Charts included in website report

◆ **Bar Chart**



◆ **Pie Chart**



5. Event Logs

AiD records all operation logs from agent computers include user logon, logout, application log, web log, document operation log, shared document log, print log, removable storage log, asset changes log etc.

The follow functions are available for all event logs

Item	Description
Print/Print Preview	All logs can be print or print preview
Export	Export logs according to administrators need
Delete	Delete selected, delete record of current page and delete all matched record available. To delete logs right click on the event logs and select delete.

View Screen History	In the event logs view, administrators can right click on any record and select “view screen history” to view screen history closest to the select event. Feature available to system equip with screen snapshot management module and screen recording activated

5.1 Basic Event Logs

A basic event log shows systems’ startup/shutdown, login/logoff, dialup, patch scanning and software distribution related information. Go to basic event go to Logs--> Basic Event to view basic event logs.

The following table shows the basic operation types:

Item	Description
System startup/shutdown	System referring to agent computer system and startup/shutdown referring to operating system startup/shutdown
User logon/Logout	Every occurrences of user logon and logout
Session Connected/Disconnected	Logs of remote session connection and disconnection
Dial	When dial up, agent will record dial and disconnect time logs
Patch Management	When windows patch installed, patch logs are recorded for future reference
Software Deployment	When system deployment task created, target computer will record deployment status for future reference.

Basic event log include, operation type, time, computer, group, user, and description column.

Search Panel Criteria

Item	Description
Time and Range	Common searching criteria
Type	Types are display in the above table
Description	Querying description field, it supports wild card search and keyword search

5.2 Application Logs

Application logs can be found at Event Log --> Application, it records all start and stop activities of all application on agent computer.

The following are the items in application log

Item	Description
Start/Stop	Record all agent computer's application start and stop operation
Window Change	Record window change activities when user switch window
Title change	When user change window within an application title change will be recorded.

Note Due to massive amount log created by window change and title change feature, the recording feature need to be activated at "Basic Policy --> Logging --> Window Title Change"

Application Log includes the following:

Item	Description
Operation Type	Start, stop and title change
Application	Exe file name of the application
Path	When operation type is start up or stop, path column will display path of the exe file.
Title	When operation is title change/ window change title column display title/window name of current window

By default application logs will display all logs recorded, administrators can use search panel set search criteria

Item	Description
Path/Title	Search by application path or title
Application	Search by application's exe file name, fields value can be select from category list or manual input

Application Search

1. **Manually input application name**

   In search panel --> Application input exe name such as msn.exe or *game*.exe

2. **Select from category**

   Go to search panel and click on the … button next to the application input box. To search a single category click on "Application category list" button select category on the right hand side of the "application library" window and press ok to continue. To search a single application select category on the left hand side of the "application library" window then select application process.

5.3 Website Browsing Log

Website browsing logs shows all website visited by agent computers, logs can be view by go to Event Logs --> Browsing. Website browsing logs support browsers such as IE, Google Chrome, Firefox, Netscape, Opera etc.

Website browsing logs include the following information

Item	Description
Title	Webpage title
URL	Detailed website address

Note Right click on the logs and select Open URL; it will connect to the browsed page.

Search Criteria

Item	Description
Time and Range	Common searching criteria
URL	URL field can be manually input or select from the category, this field also supports wild card.
Window Title	Search by windows title

5.4 Document Operation Log

Document operation log shows agent computer's document operation activity. Administrator can use operation log to track back information leakage. Document operation log can be view by go to Event Log --> document

Logs include the following information

Item	Description
Operation Type	Include: create, copy, move, rename, restore, delete, access, modify, upload, download, burn.
File Name	Name of operated document
Size	Size of the operated document
Path	Display detail document path when operation type shows copy, move, rename

Item	Description
Desk type	Drive location of the document such as fixed, floppy, DVD/CD Rom, Removable When operation type shows copy or move, this filed will show from path and to path disk of the document
Application	Name of the application used to access document
Title	Windows title while operating on the document

In document control and IM control, policy can be set to backup documents. When event triggered, document will be backup to AiD server and a clip will appear on the event log to indicate backup files are available.

To view backup document, double click on the event log, in the pop up window click on “Copy” button to view or save backup file.

To export multiple files right click on event log select Export backup file and choose current record, selected record or all matched records to export.

Search condition includes the following fields

Item	Description
Time and Range	Common search criteria
Operation Type	By default set to display all operation type, to narrow search result go to search panel and change setting in operation type.
Drive	By default set to display all disk type, to narrow search result change setting in disk type in search panel.
File Name	Search using file name entered, this field support wild card search.
Path	Search using document path, this field support wild card search

Item	Description
Destination	Only apply for event log with copy and move as operation type.
Drive	By default set to display all disk type, to narrow search result change setting in disk type in search panel.
File Name	Search using input file name, this field support wild card search.
Path	Search using document path, this field support wild card search
Size	Search file size between input range
Application	Search by name of the application, this field can input manually or select from the category list.
Has Backup	By default not selected, select this item will display logs with backup file in AiD server

5.5 Shared File Log

Shared file log shows document operation on the shared folder of agent computer, file access by 3rd party computers will be recorded. To view shared file log go to --> event log --> Share File.

Shared file logs include the following items:

ITEM	Description
Operation Type	Include: Create, rename, delete, modify. Access, copy and move not supported
Remote Host	Referring to computer accessing shared folder, IP address will be shown in the column
Source File	Referring to the file name been accessed
Path	Referring to the path use to access shares folder file

Search Criteria

Items	Description
Time and Range	Common search criteria
Shared File	
Operation Type	By default set to display all operation type, to narrow search result go to search panel and change setting in operation type.
Source	
File Name	Search using input file name, this field support wild card search
Path	Referring to the path use to connect to the share folder
Destination	Only apply when operation type is rename
File Name	Operated file name
Path	Operated path
Remote Host IP/Name	Computer name or IP address of the remote computer

5.6 Print Log

Print log record shows print job performed by agent computer, to view go to Event Log --> Printing

Print log include the following items

Item	Description
Printer Type	Include: local, shared, network and virtual printer
Print Task	Generally file name of the print job displayed
Printer name	Name of the printer used to print

Item	Description
Pages	Total pages printed
Title	Windows title of the print task
Application	Application use to print

View backup printed content

On activation printed content will be stored to AiD server. Clip icon “  ” in event log indicate printed content is available.

To view backup printed content, double click on the event log, in the pop up window click on “Copy” button to view or save printed content.

Click **Copy** and select to **View Printed File** to open the printed file. Viewer can be used to examine content by enlarge, shrink, and drag it. Viewer also support change page feature to allow administrators view multiple pages. Printed content can be exported to jpg format.

Batch Exports

To export multiple files right click on event log select Export printed content and choose current record, selected record or all matched records to export.

Search Criteria

Item	Description
Time and Range	Common search criteria
Printer Type	Default to list all printed records, to narrow search result select one printer in printer type field.
Printer	Search by using printer name
Computers	For local printer, computer name displayed. For network print IP-address displayed

Item	Description
Task	Search printing task field and support wild card search
Page	Search by number of pages printed, can be used to calculate total page printed
Application	Search by application used to print
Has Backup	By tick the check box search record will display event logs with printed contents

5.7 Removable Storage Logs

Removable storage logs display storage device activities on agent computer. To view removable storage logs go to Event log --> removable storage logs.

Removable Storage Logs include the following：

Item	Description
Type	Add or Delete
Disk Type	Indicate if device encrypted, blank mean non-encrypted disk
Volume ID	Unique key of storage device, ID can be used to track down actual storage device
Description	Description of the storage device, also name of the storage device
Volume Label	Volume label of the storage device
Remark	Remark can be added at removable storage category list

Search Criteria

Item	Description
Removable Storage	Query using volume ID, volume can be manually input or select from the removable storage device category
Operation Type	By default, it is set to All. Specific operation type can be selected from the drop-down menu including Plug in and Plug out
Removable Storage Type	By default is set to all. To narrow search result select encrypted or not encrypted

5.9 Policy Log

Policy logs displays event triggered by policy, policy log can be viewed by go to Event Log --> Policy

Policy log include the following item

Item	Description
Alert Level	There are three alert levels: Low, Important and Critical. The alert level settings can be done in each policy
Policy	The corresponding policy triggered by Agent
Description	Event information triggered policy

Search Criteria

Item	Description
Lowest Level	By default, it is set to All. Alert level can be selected from the drop-down menu including Low, Important and Critical

Policy	By default, it is set to All. Specific policy type can be selected from the drop-down menu
Content	Keyword can be used to search description field. This column support wildcard search.

5.10 System Logs

System logs record AiD system activities such as sever start up, shut down, illegal intrusions and agent errors. To view System Logs go to Event Log -->System

Note In the event of AiD server or agent errors, administrators can refer to system log to find out for possible cause.

6. Policy

6.1 Policy Introduction

Administrators can limit computer accessibility or network usage of agent computer by applying policies.

◆ Common policy descriptions

Item	Description
Name	Self-defined name to describe the policy. It is irrelevant to the actual function of the policy. When adding a new policy, the system will add a default name to the policy, name of the policy can be changed.
Time	Policy become effective during specified time period, time can be set in **Category -->Time Types**. If no suitable time type available, select **Custom** and set the time range from the popup time grid.
Action	3 types of action Ignore, Allow, Block,
Related Action	Policy related action include alert, warning and lock computer, detail description will be discuss in follow section.
Only take effect offline	When no active communications between server and agent for more than 3 minutes, agent will change its status to offline. Offline policy will become effective when agent in offline status. .
Expiration time	By default, the expiry date setting is **Never Expired** and policy will always be effective before expiry date. Click on "…" button to set the expiry date. Expire date cannot be earlier than the current date. Expired policy will be displayed in dark grey and **Expiring Time** displayed in red.

3 type of actions

Item	Description
Allow	Allow mode will perform defined action.
Block	Block mode will block defined action,
Ignore	Neither allows or block an operation, but it can still trigger events such as warning or alert.

When agent computer violate policies, following alert action can be triggered

Items	Description
Alert	When a policy with alert option is violated, console will receive a popup message to alert administrator. The minimum popup alert level can be set at **Tools --> Option --> Real-Time Alert -->Popup Alert Bubble**. There are three types of alert namely **Low**, **Important**, and **Critical**.
Warning	When a policy with warning option is violated, dialog box will pop up on the agent computer. The content of the warning message can be customized.
Lock Computer	When a policy with lock computer action is violated, agent computer will be locked. To unlock, go to **Control --> Unlock** or highlight the target agent from the network tree and then right click to select from the menu **Control -->Unlock**

◆ Policy Priority

Policy Hierarchy is similar to firewall, policy can consist of many rules. Policy matching rules adopting top-down mechanism and policy for group or individual computer will inherit policy from parent group.

Administrators can apply policy to Whole Network, Group, Computer and Users. Policy priority as follow (from highest to lowest): User Policy --> User Group Policy --> Computer Policy --> Computer Group Policy.

Inherited Policy will display with light green background and cannot be modified in lower tree structure. Policy can support wild cards, multiple check value can be separate by”,” or “;” sign.

Button Description

Items	Description
	Add, click this button to add a new policy
	UP, move up selected policy
	Down, move down selected policy；
	Delete, delete selected policy
	Restore, cancel new added policy or any modified settings
	Save，click this button to save all new added or modified settings
	Indicates that the policy mode is “**allow**”
	Indicates that the policy mode is “**block**”
	Indicates that the policy mode is “**ignore**”
	Indication that the policy mode is “**inaction**”
	Indicates that the policy with **alert** setting
	Indicates that the policy with **warning** setting
	Indicates that policy with **lock computer** setting
	Indicates that policy with **expiring time** setting

6.2 Basic Policy

Basic policy can be used to regulate computer operation authority and also prevent end users changing system settings and maliciously destroy system as well as strengthen end point security.

Basic policy achieve by change registry value. Basic policy and device policy are triggered by state change of the computer or device.

Basic policy controls the following: Control Panel, Computer Management, Network IP/Mac Binding, ActiveX control etc.

Control include the following

Item	Description
Control Panel	All functions on Control Panel
Modify Display Properties	Restrict users to change the theme, desktop, screen saver and appearance
Add Printer	Restrict user to add printers
Delete Printer	Restrict user to delete printers
Fast Switching Computer User in XP	Restrict to fast switch user in windows XP only

Computer Management includes

Item	Description
Device Manager	Restrict user to use Device Manager
Disk Management	Restrict user to use Disk Management
Local Users and Groups	Restrict user to use Local users and groups
Service Management	Restrict user to use Service Management
Other Computer Management	Restrict user to use: Event Viewer, Performance Logs and Alerts and Shared Folders which located in Computers Management

System include the following

Item	Description
Task Manager	Restrict user to use Task Manager
Regedit	Restrict user to use Regedit
CMD	Restrict user to use CMD. For Windows 98, it is **Command**.
Run Application in the "Run" of Registry	In **block mode**, process under "Run" will not be triggered when OS is starting up. **Log off or restart computer is required to activate policy.**
Run Application in the "RunOnce" of Registry	"RunOnce" means process will only run once when OS started up and will not run again thereafter. When mode set to block, process under "RunOnce" will not be triggered. **Log off or restart computer is required to activate policy.**

Network Include the following

Items	Description
Modify Network Properties	Restrict user to modify the network property.
Display "My Network Places"	My Network Places will be hidden when mode set to **block**. **Log off or restart computer is required to activate policy.**
Modify Internet Option	Restrict user to modify Internet Options settings
Default Netshare	When mode set to block, the default Netshare will be blocked
Netshare	When mode set to block, user cannot share folders or files
Add Netshares	When mode set to bloc, user is not allowed to add Netshares

IP/MAC Binding

Item	Description
Change IP/MAC Property	Prohibit end user change network settings Feature can be used to prevent end user change IP/MAC settings. When policy set IP/MAC will be saved and restore to saved value when change made.

ActiveX include the following

Item	Description
Chat ActiveX	Restrict user to use chat ActiveX
Media ActiveX	Restrict user to use Media ActiveX. Generally this kind of ActiveX is applied for playing music or video on Internet. Prohibit this option to stop user listening or watching online media
Game ActiveX	Some online games may require installing its ActiveX. Prohibit this option to stop user playing online game
FLASH ActiveX	This ActiveX is required for playing FLASH. Prohibit this option to make the FLASH file cannot be played properly

Others

Item	Description
Print Screen Stroke	Block PrintScreen Keystroke usage.
System Restore	Prevent user to restore system from agent to non-agent state. Using this option to prohibit the system restore function
Windows Automatic Update	Block Windows Automatic Updates

◆ Policy Example

Requirement:

IP settings cannot be changed by end-user. However, it should be allowed when the computer is out of office for business trip.

1. Add a policy to **block Change IP/MAC Property**
2. Add another policy to **allow Change IP/MAC Property** with option **Only offline** checked

Result:

According to the policy matching mechanism, the second policy has higher priority therefore second policy will be matched first – when the computer determined as offline status, the policy 2 will be invoked and the user should be able to change the IP settings. However, if the computer determined as online status, conditions specified in policy not satisfied, then policy 1 will proceed to be matched. As the condition satisfied, policy 1 is invoked, the user should not be able to change the IP settings.

Note Basic policy's IP/MAC Binding, System Recovery, Netshare only apply to computer.

6.3 Device Control Policy

Device control mainly use to control various type of external device attached to the computer system. The device control policies support the followings: Storage, Communication Device, Dial, USB Device, Network Device and other devices.

Device include the following

Item	Description
Floppy	Floppy Drive Control, Cannot use floppy if it is prohibited
CD Rom	DVD/CD-ROM
Burning Device	The burning disks action, but the device still can read
Type	Tape drive Control

Movable Device	Includes USB Flash drive, removable drive, memory stick, smart card, MO and ZIP drive control But not includes the device with IDE, SCSI and SATA interface
Portable Device	Smart Phone Device

Communication Device

Item	Description
COM	COM Port
LTP	LPT Port
USB Controller	USB Controller
SCSI Controller	SCSI Controller
1394 Controller	1394 Controller；
Infrared	Infrared Device Control；
PCMCIA	PCMCIA Card；
Bluetooth	Bluetooth device
MODEM	Modem Device
Direct Line	Direct connection between computers using USB cable, COM Port or Serial Cable

Dial up

Item	Description
Dial up connection	Dial up connection control

USB device

Item	Description
USB Keyboard	Control USB Keyboard
USB Mouse	Control USB Mouse
USB Modem	Control USB Modem
USB Image Device	USB Image Device Control such as Webcam, Digital Camera and Scanner
USB DVD/CDROM	Control USB DVD/CD ROM
USB Storage	Control USB Storage
USB Hard Disk	Control Hard Disk；
USB LAN Adaptor	Control LAN Adapter
Other USB Device	Control any USB device not mentioned

Network Device

Item	Description
Wireless LAN Adapter	Control Wireless LAN adapter
PnP Adapter (USB，PCMCIA)	Control PnP adapter
Virtual LAN Adapter	Control virtual LAN adapter

Others

Item	Description

Audio Equipment	Control audio, video and game controller
Virtual DVD/CD ROM	Control virtual DVD/CD Rom device
Any New Device	Any new device unknown to the system

◆ Device Control Policy Example 1

Some companies' policies not allow staff listening music or playing online game during office hours. In this case, System administrators can set a policy to prohibit the use of Audio

Policy: Add a policy to **block Audio** in **Device Policy**

◆ Device Control Policy Example 2

To prevent important files leakage, System administrators can set a policy to prohibit the use of Burning devices, removable device

Policy:

Add a policy to **block** some **Storage** (**Floppy**, **DVD/CD-ROM** and **Moveable** Device), **Communication** (**Bluetooth** as File transfer between local computer and Mobile Phone/PDA may be done through Bluetooth) and **USB** devices (**USB Storage** and **USB Hard disk**)

◆ Device Control Policy Example 3

Per request of Sales department, all USB devices must be prohibited except a specific brand.

Policy 1: Set group policy for sales department and block all moveable devices. By set up the policy USB cannot longer be use.

Policy 2: Set group policy to sale department, in policy allow removable device and add *Kingston* in description field to allow all device brand is

Kingston.

6.4 Application Policy

Many enterprises prohibit staff install own application or software such as BT, chatting and online games software. Application policy control can limit the use of unwanted applications.

To block an application, administrators requires specify which application needs to be blocked. The follow are 2 methods used to block applications.

1. Block by Directly Input Application Name

Administrators can block an application by adding name of the application such spider.exe. However when application name changed from spider.exe to spider123.exe policy will not be able to block changed name application. The above mentioned issue can be resolve by using following method.

2. Block by Select Application from Application Category

Administrators select an application from application category management. By doing so, block will be effective even executable name of application been changed.

3. Block by Path

Administrators can block application by path. For example, APPDIR：e：*.exe can be used to block any exe file with in E drive. $UDISK$, $CRROM$ can be used to represent USB device and CD ROM drive.

⚠ **Warning:** Block by path may effect end user daily routine

6.5 Website Policy

Web policy effectively controls user website access. Web policies can be used to restrict access to prohibited websites. Website URL can be directly input or select from Website category. Wild cards can be used in the URL for example “*.Yahoo.com”，“*mail*”，“*game*”，“*.com/mail/*”

◆ Web Policy Example

To prevent user access prohibited websites, web policy can be set to prohibit websites access or to allow specified websites. The following example is used to allow access to specified websites.

1. Block All website simply use “*”
2. Set another policy to allow specific website

By set up policies above only authorized website can be access.

6.6 Screen Snapshot Policy

Screen snapshot function can record all operations behavior in agent computers. By default, screen recording is off; it required administrators’ activation to record end point computer screens.

Policy Items

Item	Description
Application	By default application set to “ALL”, Administrators can change setting according to its need.
Interval(Sec)	By default screen interval set to 15 seconds. Valid interval range is between 1 and 999 seconds

Note Shorter the interval larger HDD space required please set interval accordingly.

6.7 Logging Policy

By default, system has a preset policy to log all events except windows title

change. Policy can be used to add or remove recording items according to corporate need.

Policy Items

Items	Description
Startup/Shutdown	System startup/shutdown logs (found in basic event logs)
Logon/Logoff	Logon/Logoff log (found in Basic Event log)
Dial	Dial log (found in Basic Event log)
Policy Control	Policy alert log
Hardware Change	Hardware changes log
Software Change	Software changes log
Application	Application usage log. not record application usage log
Visible Window	It means the application with windows
Application	Application can be manually input or select from application category
Window Title Change	By default, windows title change not recorded. Policy can be add to record the changes based on different applications (optional)
Application	Administrators can monitor windows change on specified applications. Wild card supported.
Browsing	Website browsing
Website	URL can be select from website category or manually input
Document	Document Operation Logs

Items	Description
Disk Type	Includes: Fixed, Floppy, DVD/CDROM, Removable, Network and unknown disk types.
File Name	Set not to record filename contain specific keyword. Supports wildcard input e.g. not record *.txt ; *.log
Application	Application used to operate on files
Printing	Print Logs
Printer Type	Types of printer used to print
Application	Application used to print
Shared File Logs	Shared files log
File Name	Shared file name. Support wildcard.
IP Range	IP Range of computers remote access agents' shared files
Email	Email Logs
Email Type	Standard mail, Webmail, Exchange, Lotus
Send/Receive	Email direction send or receive
From	Sender's email address, support wild card
To	Recipient's email address, support wild card.
Just match a recipient	In the event of multiple recipients, system will only match one recipient to proceed with record/not record action
Email Size （>=KB）	Exclude email size exceeds specific KB
Email Size （<=KB）	Exclude email size less than specific KB
Do Not Log Body	This option only enabled under **Record** mode. When it's checked, email content will not be logged.

Items	Description
Do Not Record Attachment	This option only enabled under **Record** mode. When it's checked, email attachments will not be logged. Email logs will display attachments icon but attachments cannot be retrieved.
Instant Message	Instant Message Logs
Tools	Specify instant message application
Do not Log Attachment	This option only available when mode is **Record.** When activated attachment will not be recorded
Application Statistics	Application usage statistics
Web Statistics	Website usage
Traffic Statistics	Network traffic usage

6.8 Remote Control Policy

With remote control policy, agent's computers can be control remotely. There are two types of Remote Control Policy: **Remote Control** and **Remote File Transfer**

Remote control or remote files transfer option need to be check in order to set policies blow

Item	Description
Authorization is required	This option is only enabled under the mode **Allow**. If checked, all remote control access rights must be granted by agent computer user. If not checked, administrator can access remote computer without authorization and logon by using pre-defined password.
Manager Name	Only specified account name can perform remote control
Console IP Address	Only console from specified IP address can perform remote control

Console Name	Administrator need to use specified computer to logon to console in order to perform remote control

Separate multiple console IP address, console name and manager name by ";" or ","

6.9 Alert Policy

Alert policy is used to monitor changes from hardware, software and other system settings, AiD will alert to console when changes occur. This feature helps administrators to get a real time update on computer status on the network

Alert policy include the following

Item	Description
Hardware Change	hardware installed or removed alert；
Lock Computer	Lock computer when hardware changes
Plug in Device	Alert on plugin external devices
Unplug Device	Alert on unplug external devices
Plugin Storage Device	Alert on plugin of external storage device also record name of the plugin device
Unplug Storage Device	Alert on unplug device；
Plug in Communication Device	Alert on communication device plug in and also record name of the plugin device
Unplug Communication Device	Alert on unplug communication device

Item	Description
Software Change	Alert when software added, removed, change made
System Service Change	Alert when system service changes, include add or remove service
Startup Item Change	Alert when any startup item is added, removed and modified
System Time change	Alert when system time changed
Computer Name Change	Alert when computer name changed
Network Configuration Change	Alert on change of the network communication
Low Disk Space	Alert when agent computer do have sufficient disk space
Disk Space（MB）	Set minimum hard disk space level

System alert include detailed description that help administrators to identify location of the computer.

6.12 Email Policy

Email policy used to prevent confidential information leak via Email. Policy only applies to outgoing emails using exchange and standard email protocol. It cannot control mail sending via webmail and lotus note.

Policy includes the following:

Item	Description

Item	Description
From	Senders of the email, this field support wild card, multiple sender can be separated by “,” or “;”
To	Recipients of the email, this field support wild card, multiple recipients can be separated by “,” or “;”
Just Match a Recipient	In the event of multiple recipients, system will only match one recipient to proceed with record/not record action
Subject	Control subject of the email and this field support wild card and multiple keywords can be separated by “,” or “;”
Has Attachment	Restrict if email include attachments
Attachment	When Has attachment checked, this field can be used to restrict attachments with certain keywords, this field support wild card and multiple keywords can be separated by “,” or “;”
Email Size (>=KB)	Used to control email size, default set to 0, implies not all mails are restricted.

◆ Email Policy 1

Requirement:

Corporate request to prohibit outgoing email with certain keyword in attachment file name to prevent confidential information leakage via email,

Policy:

Add a policy with action set to “block”, “Check” has attachment and enter keyword in the attachment text box

◆ Email Policy 2

Requirement

Some enterprise only allow employees to send emails using company

email server, email sending via any other mail server will be blocked

Policy：

1. Add a policy to block all emails
2. Add a policy to specify sender by setting Action to “Allow,” Sender with domain e.g. *@acumen.com,

◆ **Email Policy 3**

Requirement:

All mail must CC to manager in order to send, else block all out going mails

Policy:

1. Add a policy to block all emails
2. Set a policy with action set to “Allow”, Recipient set to manager@acumen.com , check “Just match a recipient “

6.13 IM File Policy

IM file policy can effectively restrict computers within the organization sending confidential files via IM applications. IM File policy supports the following IM applications: QQ, MSN, SKYPE, TM, UC, RTX, Yahoo, POPO, Google Talk, ICQ, LSC, FETINO, Ali, 263EM, FeiQ.

Policy includes

Item	Description
File Control	Enable file control feature
File Name	Restrict outgoing file name contain keyword defined, wild card can be used.

Item	Description
Limited Size (>=KB)	Activated when action set to “block” and will restrict will size greater than value define. Value must in between 0 and 100000.
Backup File	Enable file backup feature, backup file can be view in Events log --> Document
Min Backup Size (>=KB) Max Backup Size (<=KB)	When backup file selected min backup size and max backup size will be used to determine when to perform backup action. Files size outside max and min value will not be backed up.
Image Restriction	Enable control on image sharing
Backup File	Enable image backup feature, backup files can be view in Events Log --> Document
Tools	Select to control specific IM Application

◆ IM Policy Example

Requirement:

Enterprises maybe allow IM application as communication tool. However, file name containing certain keyword must prohibit and outgoing files must be backed up.

Policy:

1. Set a policy to enable backup feature by “check” file control and backup file box
2. Set a policy to block out going file by keyword with action set to “block”, file control box “checked” and enter keyword in file name field.

Sending file with keyword in file name will be blocked, successful transferred can be viewed in document event logs.

6.14 Document Operation Policy

Document Operation Policy can effectively prevent unauthorized user access confidential information and reduce risk of confidential information leakage.

Document Operation Policy includes the following:

Item	Description
Operation Type	There are 3 types of operation type, Read, Modify and Delete. Allow modify will allow read. Allow Delete will allow Read and Modify.
Read	Read Files
Modify	Include create, rename, modify, copy, move and restore. Read and delete operating type not included.
Delete	Delete File
Disk Type	By default its set to all disk types. At least one disk type need to be selected else system will set disk type to All. Ctrl-A short cut key can be used on disk type field to select/unselect all disk type.
File Name	File name that require restriction. Field allow file path, input e:\work* to restrict documents within work folder
Backup Before Modify	Backup files to AiD server before modifying file
Backup When Copy/Cut To	Backup files to AiD server before copy or cut to
Backup When Copy/Cut From	Backup files to AiD server before Copy/Cut from
Backup Before Delete	Backup file before delete

Item	Description
Minimum File Size(>=KB)， Maximum File Size (<=KB)	When backup file selected min backup size and max backup size will be used to determine when to perform backup action. Files size outside max and min value will not be backed up.
Application	Specify application used to operate on the document

◆ Document Policy Example 1

Requirement:

Files/folders from shared network drive are restricted to a group of users. Restricted group will have read access and prohibit from modify and delete

Policy:

Add a policy Action set to “Block”, Operation Type select “delete and modify”, File Name set to desired path/file name.

◆ Document Policy Example 2

Requirement:

Prevent file operation error, backup files before modify or delete

Policy:

Add a policy Action set to allow, operation type select “modify and delete”, check backup before modify and backup before delete. To restrict backup action to certain folder input folder name in file name field.

Note File backup may require massive amount of storage space, please set the policy to folder level to reduce unnecessary backup file/

6.15 Print Policy

Print policy can be used to restrict employees printing confidential information and reduces print cost.

Print Policy includes the following:

Item	Description
Printer Type	There are 4 printer type local printer, shared printer, network printer and virtual printer. If printer type not selected, all 4 types of policy will be automatically included.
Printer Description	Printer description referring to name of the printer. It can be used to specify printer connected to other computers, for example \\server* implies all printers connected to "server" is prohibited.
Print Task	Print task support wild cards, multiple values can be separated by "," or ";"
Application	Specify print application
Record Mode	To record printed content change mode to record.
Max Record Page	By default, all pages of printed content are recorded. Administrators can adjust accordingly. Printed content can be view in Events Log --> document

◆ Print Policy Example

Requirement:

Restrict end user printing to prevent confidential information leakage or abusing print resource.

Policy:

Add a policy to restrict printing by set action to "Block", printer type select "local Printer, shared printer, network printer and virtual printer".

6.16 Removable Storage Policy

To prevent information leakage via removable devices, policy can be set to prohibit removable storage device usage. File encryption can be applied on files coped to removable storage device; encrypted file will be readable to authorized agent computer.

Removable Storage Policy

Item	Description
Storage Type	By default storage type set to “All”, storage type can be change to encrypted or non-encrypted. If storage type selected, policy set will only apply to selected storage type.
Readable	By enable this feature document will be access in read-only mode. Below settings are depended on activation of this feature.
Auto Decryption	Automatic decrypt, encrypted files on storage device, when file copy to local hard disk or network drive via windows explorer. Decryption will not perform is other application used to copy file from storage device.
Writeable	Allow any application copy or create files on storage device. When this feature not activated delete or modify action to storage device will be prohibited. Auto encryption feature depend on activation of this feature.
Auto Encryption	Only allow windows explorer write/copy document to the removable storage device and encrypt automatically.
Removable Storage	By default its set to all, referring to all removable storage device. The field can be used for one single device or group of device.

Item	Description
Description	Description of the removable storage such as brand name, model name. Use as keyword to identity removable storage device. When description and storage type are set, both condition must fulfill in order to pass policy condition.

Note To tightly control removable storage usage apply the following:

1. Set all storage devices to read-only mode.
2. Enable removable access right by group or by computer (for example each department only have access to a specific category of device).

As result USB storage can be use within the department and unknown USB devices will be inaccessible.

Caution In the event of both document policy and removable storage policy applied. Document policy has priority over removable storage policy. For example:

Set removable storage policy to encrypt and document policy to prohibit copy Word documents to removable storage device. Word document will be prohibits copy to removable storage device and any other documents type will be store in encrypted format.

7. Monitoring

7.1 Instant Message Monitoring

Instant Message Monitoring can be used to monitor and record IM conversations.

◆ Supported IM Applications

Instant Message monitoring support the following IM applications

QQ, TM MSN Messenger, ICQ, Yahoo! Messenger, UC, POPO, Skype, RTX, Google Talk, Lotus Sametime, Ali, Fetion, 263EM, FeiQ, OfficeIM, MSNLite and LIMC

Instant Message Logs include the following

Item	Description
Tools	IM application used
Computer	Computer used
Local User	User logon to the computer
User	User of the IM application
Participants	Nick name of the IM conversation
Start Time	Start time of the conversation
End Time	End time of the conversation
Message Type	Normal chat or group chat
Conversation	Number of chat statement
Characters	Number of characters in the conversation

◆ Save IM Content

Content can be view in console, conversation content can be exported for further reference.

To export stored content, right click and select export IM conversation. Contents can be export to Excel or HTML format. Export multiple conversation also supported.

◆ Search Conversation

Search criteria as followed:

Item	Description
Tool	Select different type of IM application from the drop down menu. By default set as All
User ID or Nickname	Search for IM content using user id or nickname
Content	Search conversation content using keyword

7.2 Email Monitoring

Email monitoring supports following email types: Standard mail, Exchange mail, Web mail and Lotus mail. Emails send and received via standard email protocol and exchange mail will be recorded. Mail sent via Webmail and Lotus mail will not be recorded.

◆ Email Logs

Email Logs include the following

Item	Description
Send/Receive	Represent send mail Represent received mail
Subject	Subject of the mail
From	Sender's mail address
To	Receivers email address, CC and BCC also recorded
Attachment	" " represent attachments available, Email logs will automatically record attachments. Click "" in content panel to view attachments
Size	Size of the mail
Content	Click on email record and view its content in content panel。

◆ Save emails

Recorded emails can export by following steps below:

Right click on email record and select export EML file, email will be export as outlook elm file format which is readable by using outlook. Multiple file export also supported.

◆ Search Email

Search conditions:

Item	Description
Type	To specify which email type to search from, email type include SMTP/POP3 Mail, Webmail, Exchange, Lotus Note
Send/Receive	To search send or received mails

Item	Description
From	Search by using sender email address
To	Search by using receiver email address, administrators can specify receiver email in To, CC or BCC.
Subject	Search email subject with specific keyword
Content	Search email content with specific keyword
Attachment	Check to list emails with attachment and enter keyword to list emails with attachment include specific keyword in attachment name.
Size	Search by size of email

7.3 Real-time screen snapshot

Administrators can monitor agent computer screen or users screen by go to Monitoring --> Screen Snapshot

Item	Description
	Save current screen to image format
	If a computer logged on with two or more users or a user logged into two or more computers, administrators can select which screen to display by clicking this button
	Fit screen to window size
	Display screen in original size
	Track button, Screen snapshot will automatically refresh. To change refresh interval go to Tools --> Options --> Real-time info and change value in Time interval to track

Item	Description
	frame
	Stop tracking, screen snapshot will be refresh

To track a computer, select target computer on the computer tree, click **Track** button to start the real-time tracking feature. Screen snapshot will update when the target computer's screen changed. The track mode can be stopped by clicking the **Track** button again.

7.4 Multi-Screen Monitoring

Multi-screen monitoring can monitor multiple screens at same time. Multiple screen view can monitor from 2x2 (4 screens) to 4x (16 screens) at ones

After select desire view, system will automatically refresh and rotate screens with in a specific time period. Refresh time and interval can be modified in Tools --> Options --> Real-time info.

Administrators can use function button to navigate through multi-screen monitoring window.

 Used to select different computer or computer group,

 Used to auto switch screens

 Used to view screen in full screen mode

◆ Lock Screen

Lock Screen can be applied to any computer on the screen monitoring view. When screen lock applied, screen will be excluded from the rotation and highlighted with yellow frame. To lock/unlock right click on the screen and

select lock/unlock.

◆ Screen Information

Computer information such as computer name, IP address, and online status will be display when mouse moved over a monitoring screen.

◆ Navigate to computer tree

By right click on the monitoring screen and select navigate to computer tree, it will take the administrators to the computer's location on computer tree.

7.5 Search Screen History

Select Monitoring --> search screen to search recorded screen history

Search condition includes:

Item	Description
From/To	Search screen history with begin and end date
Name or IP Address	Search computer screen by computer name or IP address/IP range
Range	Search computer screen history by a computer or computer group

History log include the following

Item	Description

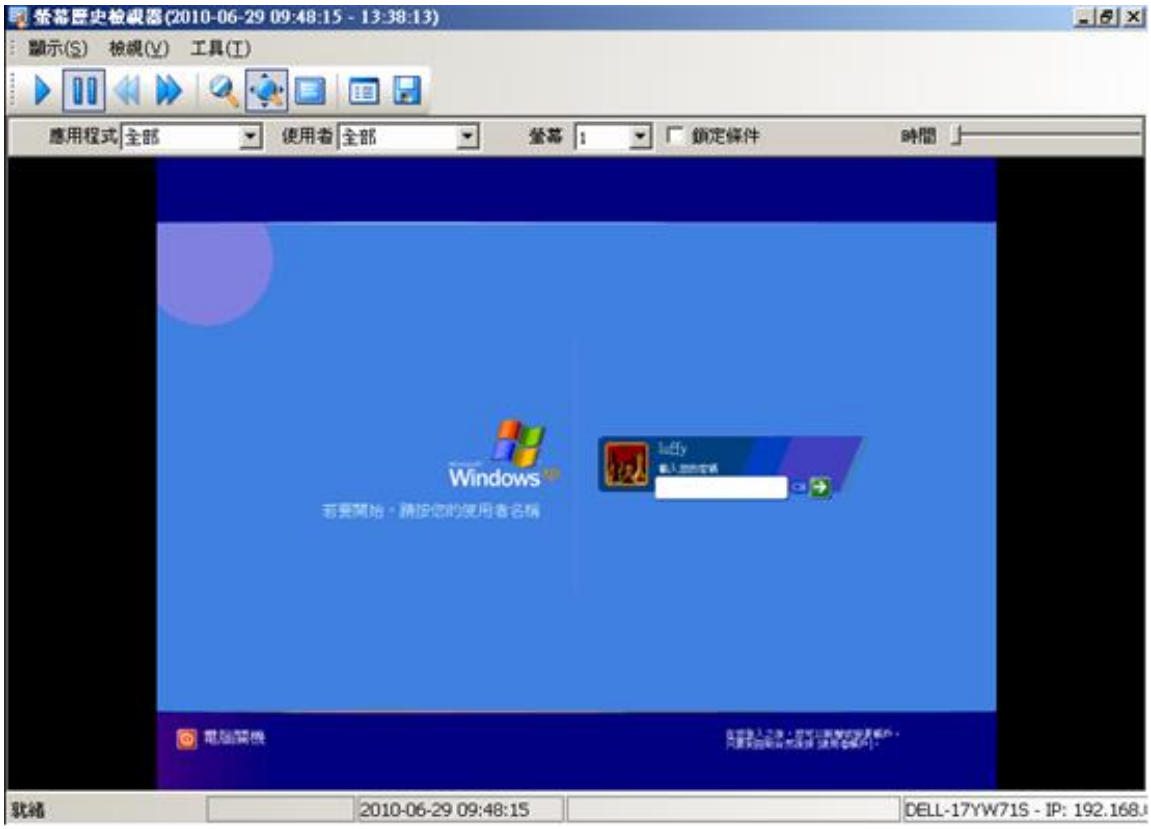
Date	Recording date of the screen history. Each new day will generate a new record.
Computer	Computer name of the computer
Session	Session ID, if one user logon session ID will be display as 0. Each session will have an own log file for snapshot history. Note For Windows Visa first session start at 1
Start Time/End Time	Start time and end time of the screen snapshot history
File Name	The file name shows as <SQL>, it represents that the screen snapshot data is stored inside the SQL Server.

7.6 Screen History Viewer

To view screen history, double click on one of the search resulting or highlight a record and click on **View**.

◆ Interface

The screen snapshot viewer include, menu bar, tool bar, search bar, time line, display panel, and the status bar



◆ Display

Administrators can use time line to navigate through the screen snapshot clips or control play status with tool bar.

◆ View

Administrators can use the view bar to perform zoom in and out and display full screen

◆ Play Speed

Play speed can be changed by go to View--> Play Speed. There are 3 type of play speed Slow, Normal and Fast

◆ Search Bar

Search Bar can be user to search screen history by application window change, user timeline and screen number.

Item	Description
Application	Name of the application, used to play screen history of selected application
User	In the event of multi-user screen recorded, User field can be used to search a specific user's screen history.
Screen	In the event of multi-screen recorded, Screen field can be used to display a specific screen history.
Lock Criteria's	By select this item, will only display screen match application, User and Screen condition.
Time Line	Display the current time frame; drag the slider to a designated location and view screen of the moment. When mouse is over the time line, information such as: **Time**, **User**, **Application** and **Caption** will appear

◆ Export

Screen can be exported by go to Tools --> Save as Video. There are 4 way to find and save screen history

Item	Description
Time From/To	Export screen history between specific start and end time
Application	Export screen history for a specific application
User	Export screen history for a specific user
All	Export all screen history

8. Remote Maintenance

IT Department engineers spend approximately 70-80% of their time on daily maintenance tasks. Remote Maintenance help IT engineers to real-time check computers' status and information. It also allow engineer to solve the technical issues with immediate effect, it also save time and resources especially to the computers in remote site.

8.1 Remote Maintenance

8.1.1 Application

Select Maintenance --> Application to check agent computer application status. The active application is highlighted in blue

Item	Description
	For concurrent sessions on terminal Server or users logon to a server/computer at the same time, click this button to view specific user's application running status.
	Track Button, to allow application list perform automatic refresh. To change refresh interval go to Tools --> Options --> Real-time info --> Maintenance

◆ **End Task**

Application task can be terminated by right click on the task list and select End Task

8.1.2 Processes

Go to **Maintenance --> Processes** can view Agent computer's processes

including: Filename, PID, time, Session, CPU, CPU Time, Memory, Virtual Memory, Priority, Handle, Thread Count and Path.

Item	Description
Time	Startup time of the process
Path	Details path of the process
Other	Other properties are like the processes running in Explorer.exe, their meanings are similar

Control Button

Item	Description
	Only active under user mode, select target process to view processes status.
	Track button, allow process list perform automatic refresh. To change refresh interval go to Tools --> Options --> Real-time info --> Maintenance

◆ **End Process**

Select any processes from Processes List, right click and select **End process** to stop the process

8.1.3 Performance

Select Maintenance --> Performance to view agent computers performance status including CPU Usage, Memory Usage, Physical Memory, Commit and Kernel Memory. These real-time data is exactly same as **Performance in Windows Task Manager.**

Item	Description
	Only active under user mode, select target performance to view performance status.
	Track button, allow Performance list perform automatic refresh. To change refresh interval go to Tools --> Options --> Real-time info --> Maintenance

8.1.4 Device Manager

Select **Maintenance --> Device Manager** to view agent computer's devices, Include Processor, DVD/CD ROM Drive, Keyboard, Mouse and Network adapters etc.

Item	Description
	Device List Checking method: **By Type**, **By Connection** and **Show Hidden Devices**
	Only active under user mode, select target device manager to view device information.

◆ **Disable/Enable Devices**

Select target device, right click to select **Disable** or **Enable** to control agent computer's devices

8.1.5 Services

Select **Maintenance --> Service** to view agent computers system services information including Name, Description, Status, Startup Type, Log on as, and Path.

Item	Description
	Only active under user mode, select target service to view the Service information.

◆ **Remote Control**

Administrators can make changes to agent computer by right click on the service name and select start/stop or change start up type to automatic/ manual/ Disable.

8.1.6 Disk

Select Maintenance --> Disk to view check the agent computer's disk usage situation including disk Volume, File System, Capacity, Free Space and % Usage

Item	Description
	Only active under user mode, select target disk to view disk information.

8.1.7 Shared Folders

Select **Maintenance -->Shared Folders** to view agent computer's network shared information including shared folders, shared Path, Agent Connections and Comments.

Item	Description
	Shared View Button
	Session View Button
	Open File View Button
	Only active under user mode, select target user to view shard folder information.

◆ **Share**

In shared folder tab, administrators can view shared folder information

and also has the ability to remotely stop sharing.

- **Session**
  Select this mode to view user access information to the share folder. Information includes User, Computer, Type, Open File, Connected Time, Idle Time and Guest.

- **Open Files**
  Select this mode to view current shared folder accessibility information, include Open File, Access By, Locked and Mode. System administrators can right click on target file and select **Close Open File** or **Close All Open Files**

8.1.8 Schedule Tasks

Select **Maintenance -->Schedule Tasks** to view agent computer's schedule list including Name, Schedule, Application, Next Run Time, Last Run Time, Status, Last Result and Creator.

Right click on the schedule and task record can delete any unauthorized schedule and tasks

Item	Description
	Only active under user mode, select target schedule task to view related information

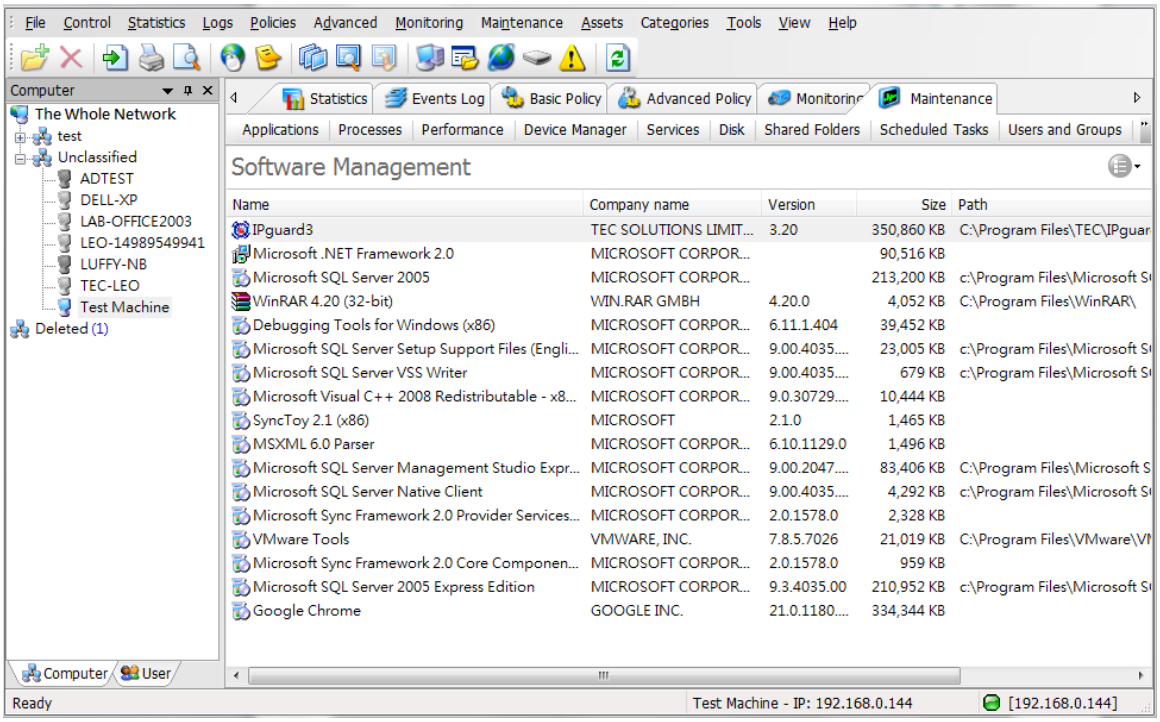
8.1.9 Users and Groups

Select maintenance --> User and Groups to view all local users and group on the agent computer. The information include name, full name and description

Items	Description
	Only active under user mode, select target user and group to view related information。

8.1.10 Software Management

Right click on Maintenance --> Software Management to view list of installed software on agent computer. Right click on list to remote uninstall software.



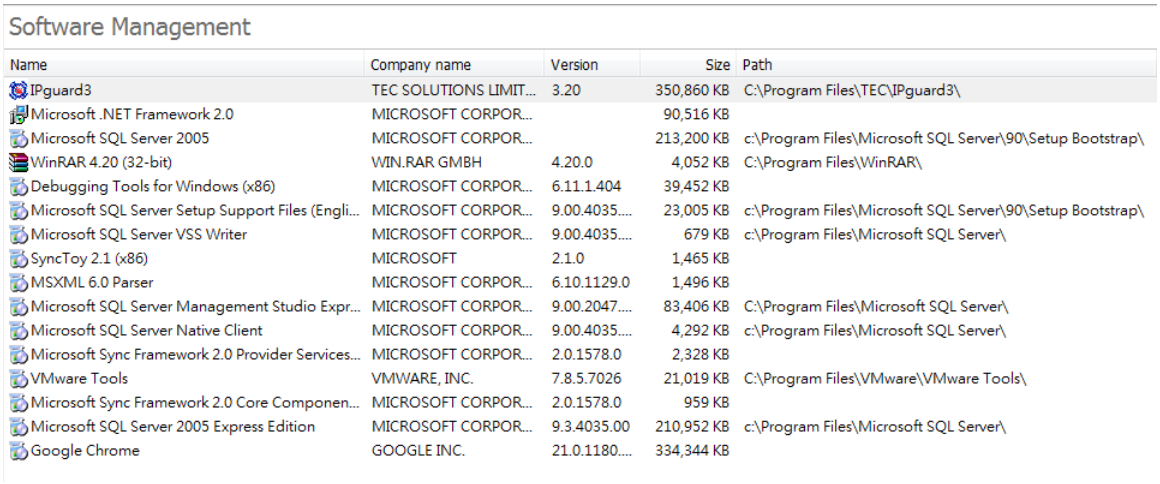
The follow are methods to uninstall software

Item	Description
Default Uninstall	Using the uninstall feature provided by software. If feature not available, the item will be gray out.

Advance Uninstall	Uninstall by using information provide by AiD agent and remove all related file.

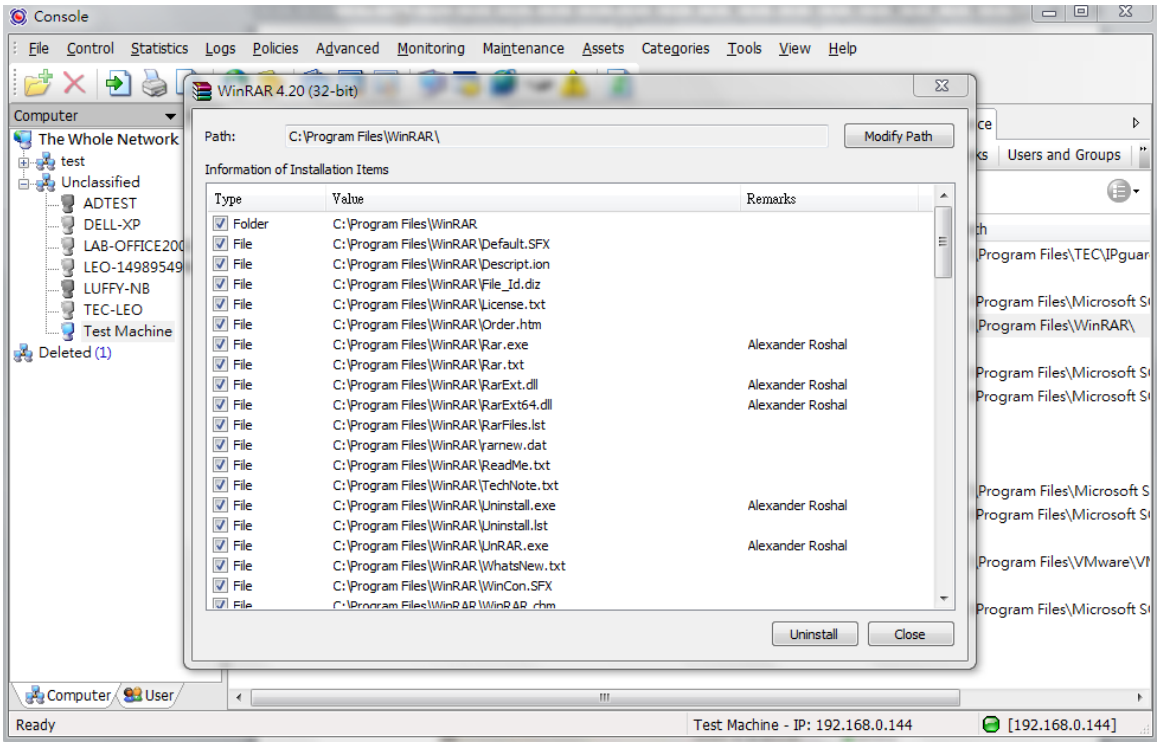
◆ Uninstall Example

Select software for example Yahoo! Messenger, since default uninstall not available, uninstall using advance install option



If software failed to obtain installation path, administrators can select correct path manually:

1. Click on the button next to path field and a window will appear with application path.
2. From the list, select an application and relative path will show in the relative path window
3. Confirm the path and system will re-analysis application information
4. Uninstall performed once click on OK button



8.2 Remote Control

8.2.1 Remote Control

Remote control is established from AiD console to control agent computers, it help administrators to resolve remote computer's problem with immediate effect.

Select an agent computer from the network tree, select **Maintenance --> Remote Control** or right click on agent computer in the network tree and select **Control --> Remote Control**.

There are 2 authentication methods to grant remote control

1. **Agent user authentication**

   Select a target computer and go to Maintenance --> Remote Control a window will appear on console to verify remote control task, by selecting "YES" an authorization window will appear in console user requires to

select “YES” to accept remote control

2. **Password Authentication**

   Select a target computer and go to Maintenance --> Remote Control, a message daillog box will appear to request for password and enter correct password to perform remote control.

   This method requires to preset password on the agent computer, to preset password: Press **ctrl + alt + shift + ocularrm** a popup window will appear in the agent computer, input the password twice to confirm.

To protect agent against preset password authentication, administrators can set a policy in Remote Control Policy to enforce all authorization must be granted from agent even agent computer password preset.

◆ Remote Control Interface

When entering remote control mode “**Remote Controlling…**” will appear on console

Item	Description
	Zoom In
	Zoom out
	Full screen or press F12
	Color mode
	Allow copy and paste between agent computer and console
	Lock agent computer mouse and keyboard
	Enable/Disable control

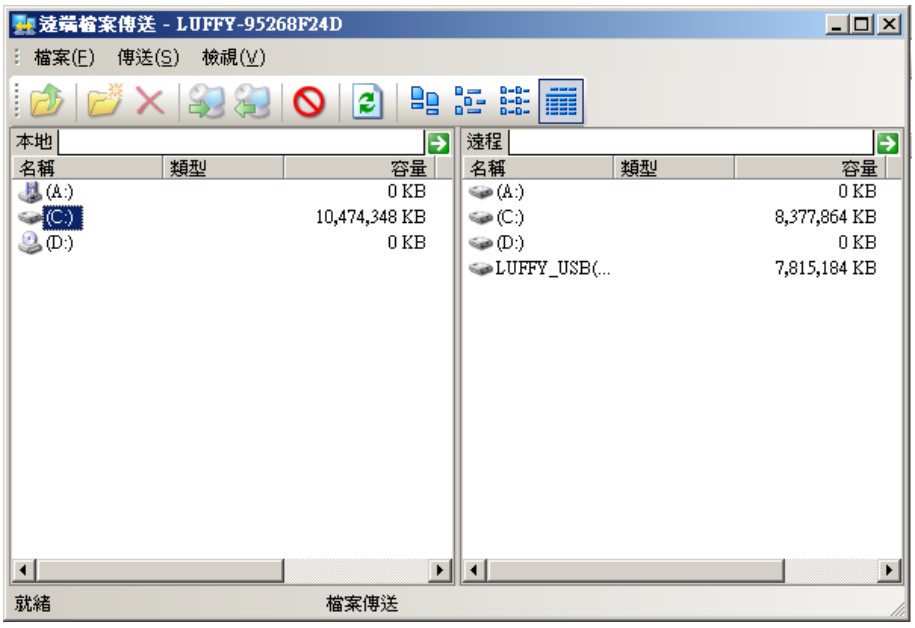
Show or hide local cursor

To send short cut keys to agent computer, right click on the remote control window and select send Ctrl-Alt-Del, Ctrl-Esc or F12

8.2.2 Remote File Transfer

Remote file transfer can be used to transfer files between console and agent computers in order to increase work efficiency

There are 2 types of remote file transfer authentication which same as remote control.



◆ **Remote File Transfer Interface**

It includes menu bar, toolbar, local and remote view panels and status bar. Refer to the screen capture above, the left-hand-side panel is local view and the right-hand-side panel is for remote computer. Double click to navigate through the folder structure or enter path in the text box above.

◆ **File Operation**

Administrators can directly click the folder and access sub-folders or select

File --> Up to move up to previous level, also folder or file path can be input in the address bar. Basic file operations such as create, rename, delete are available in this function.

◆ File Transfer

Item	Description
Local to Remote	Send file from console to agent computer
Remote to Local	Send file from agent computer to console computer
Terminate Transfer	Go to Transfer --> Stop to stop file sending process. Status will display file transfer failed

Drag and drop can be use to transfer files, however no operation can be perform during transfer.

◆ Display Mode

Both local and remote view support Large, Small, List and Details display

Note Remote transfer cannot perform when both console and agent computer are in root folder.

9. Category Management

Category management allows administrators to predefine categories and reduce effort in generating statistic report. Category includes application, website, removable device, IP, port and time type categories.

9.1 Application Category

Go to Categories --> Application to open application category window, unclassified and windows application categories are default categories.

All applications are collect from agent computers and place in unclassified group. Applications can't be added manually and shall place related application into same directory

By default windows application category is empty and it require administrators to manually sort and move windows application into this category

Application category include the following

Item	Description
Add	In category tree select Operation --> Add to add a category. Sub-category can be created with in a category.
Move To	Once category created, right click on the category and select "Move To" to perform move, or alternatively drag and drop the application to target category. Ctrl and Shift can be used to move multiple categories.
Find	Select Operation --> Find to search for an application with its category. Find can use to search on Application name, file name or description filed.

Note Delete and add sub-category cannot performed on windows application and unclassified category.

9.2 Website Category

Website category can be form according corporate's need.

Go to Categories --> Websites to open website category management window, categories and website information require manual input.

Item	Description
Add Website Category	In the root of the category tree select Operation --> Add to add a category. Sub-category can be created with in a category.
Add Website	Once category created, right click on the right panel select Add --> Website to add a new website identity, wild card supported in the website field.
Import Website	Websites can be imported from text file with Name, Website as format. For example Facebook,*facebook* Yahoo!, *yahoo* After text file created, go to Operation --> Import website to perform import. Or right click on right panel select Add--> Import website to import.
Find	Select Operation --> Find to search for a website with its category. Find can use to search on name and Website filed.

Website can be added by right click on website event logs and select add to website category

9.3 Removable Storage Category

To accommodate corporate control over its removable storage device, administrators can categorize removable storage devices into different categories and assign different access authorities.

There are two types of removable storage device, encrypted disk and non-encrypted disk, encrypted disk referring to storage device encrypted by AiD and can only be used on computers with AiD installed. Encryption can be done via AiD console.

Select categories --> Removable Storage to add new category.

◆ Removable Storage Information

Removable storage information can be obtained by following methods:

Item	Description
Agent	When removable storage device plug into the agent computer, device information will be placed under unclassified category. Administrators can further categorize removable storage information.
Console	Removable storage device information can be gathered by plug into AiD console computer. Go to Operation --> View Local Removable Storage Info to view attached device information.  icon indicated removable device information not store in category

Item	Description
	Manually refresh local removable storage disk information
	Set classes, assign device into a specific category
	Set volume ID for the device
	Save removable storage device information to category
Remark	Use to store additional removable storage device information

◆ Disk Encryption

Administrators need to plug in USB device to console computer in order to create encrypted disk. Go to Operation --> View Local Removable Storage Info to view USB information.

Click on  button to format a removable storage device into encrypted disk. All information on disk will be formatted and encrypted disk can only use on AiD agent computer.

 Indicated removable storage device is encrypted disk but information not stored in category, click  to save information.

◆ Covert Encrypted Disk to Non-encrypted Disk

Following methods can be used to restore encrypted disk to non-encrypted format

1. Format disk on computer without AiD agent

i. Encrypted disk can be used as normal disk on AiD agent computer. However, when the disk plug into computer without agents install, system will prompt to format the disk and formatted disk will be restore to its original format.

2. **Use console to convert encrypted disk to non-encrypted disk**

   i. Plug in USB device to console computer and go to Operation --> View Local Removable Storage Info to view USB information.

   ii. Select a removable storage device and press  button to convert it back to non-encrypted disk. Once encryption completed displayed icon will change back to 

   iii. To move device from console computer click on  to safely remove

 **Note** To eject device, we recommend end user click on Safely Eject Hardware icon on the system tray

◆ Removable Storage Device Description

Removable Storage Device includes USB device, Removable Hard disk, memory cards, smart cards …

Device listing has the following fields

Item	Description
Volume ID	Each removable device has a volume ID to identify that specific device.
Description	Description of the device, generally its preset by manufacturer
Remark	Administrators can input additional information for this device.
Volume Capacity	Size of the device
Type	Indicate disk encryption status, will show blank for non-encrypted disk

Item	Description
Partition Format	Partition Type：FAT、FAT32、NTFS。
Volume Label	Volume label of the device
Usage Records	Double click on the removable storage device record, Usage Records button can be found in the pop up window.

◆ Find

Go to File --> Find to open search panel and search criteria as followed:

Item	Description
Volume ID	Requires to enter full volume ID, DO NOT support wild card search
Category	By default its set to unclassified, administrators can change category accordingly.
Description	Search the description of the device, field supports wild card search
Volume Label	Field support wild card search on volume Label
Storage Type	Search for All, Encrypted or Non-encrypted devices.
Partition Format	Search by partition format such as FAT32 or NTFS …
Remark	Search on remark field support wild card.
Capacity	Search USB between specify maximum and minimum size

Search result can be drag into defined removable device categories.

◆ Change Volume ID

In certain devices volume ID is preset as 0000-0000, therefore change volume ID feature can allow administrators change volume ID to different value.

Steps to change volume ID：

1. Plugin a removable device to console computer
2. In AiD console go to Categories --> Removable Storage --> Operation --> Local Removable Storage Info
3. Click on sign to set volume ID
4. To change Removable Storage Device ID window click on “Generate” button to generate a random Volume ID
5. Select “Ok” to make change and close Change Removable Storage Device ID window.

9.4 Time Type Category

Administrators can predefine time type to facilitate search and report generation. There are 4 time types available: All Day, Working Time, Rest and Weekend.

Time type can be modified by corporate working hours click on a time type and change its range on the time grid.

Item	Description
Add Time Type	Click on button to add new time type, by default all new time type is set to all day. Administrators need to change time zone manually. Time grid cover in Blue indicates time selected.

Delete Time Type	Click on ✕ to delete time type; predefine time type cannot be deleted.

10. Database Backup

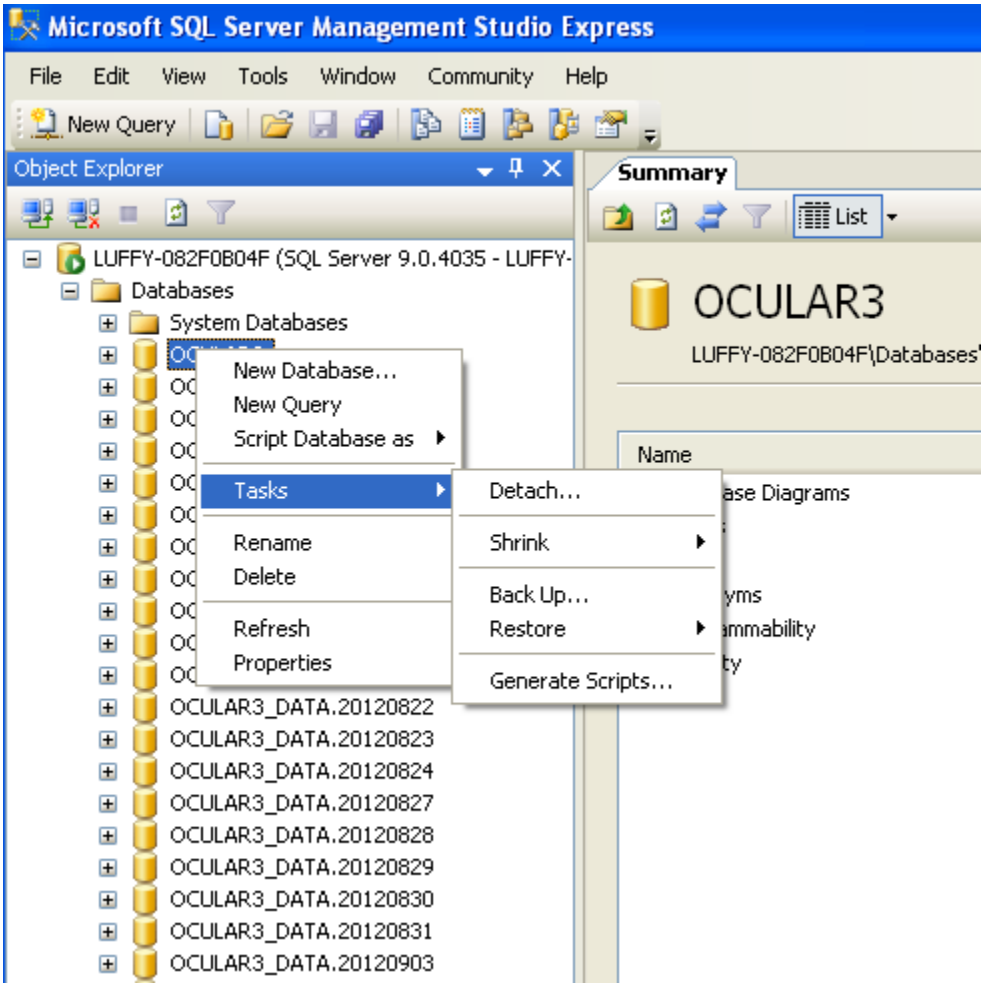
10.1 Backup using SQL Studio

◆ **Backup Main Database**

To prevent database crash from any unexpected causes, we recommend backup should be performed basic setup in completed.

Please follow steps below to backup AiD main database

1. Stop AiD server service and any other application using OCULAR3 Database
2. Start SQL Management Studio；
3. Right click on “OCULAR3” Database and select Tasks --> Detach



1. Once Database successful detached, backup OCULAR3.MDF and OCULAR3_Log.LDF.
2. Attach OCULAR3 database after backup completed and restore service

Alternatively backup can be performed by follow steps below:

1. Stop AiD server and SQL server service
2. Backup main OCULAR3.MDF and OCULAR3_LOG.LDF from AiD folder
3. Start SQL server service and AiD service respectively

◆ **Backup Log Database**

AiD logs are stored in DATA folder of the installation folder in daily format.

For example: data for 2010-06-20 will be stored in
OCULAR3_DATA.20100620.MDF
OCULAR3_DATA.20100620_Log.LDF
OCULAR3_DATA.20100620.X.MDF
OCULAR3_DATA.20100620.X_Log …

To perform backup follow steps below;

1. Stop AiD server service and MSSQL SERVER service
2. Backup MDF and LDF files for the desire date
3. Start AiD server service and MSSQL SERVER service

10.2 Backup using AiD Console

10.2.1 Backup Data Logs

Data backup can be performed using the interface provided in the AiD consoles to prevent insufficient storage space on server computer.

Go to Tools --> Server Management --> Backup Management to open Backup Management

◆ **Add New Backup Task**

Click on new backup task button and follow steps below:

1. Select required data type include, basic event log, document operation log, browsing log, print log, screen event log etc.
2. Set backup data start date and end date
3. Select backup path

4. Check delete original data if release storage space required
5. Press Ok to begin backup

Backup data will be stored in daily formats, for example data for 2010-10-27 backup file name will be OCULAR3_DATA.20101027.MDF and OCULAR3_DATA.20101027.LDF

Note When “Delete Original Data” selected, data will be deleted after backup. Administrators will no long have access to the deleted data unless data restore to the database.

◆ Backup Task List

Backup Task List include the following information

Item	Description
Beginning Date/ End Date	Backup perform with in this period
Backup to	Backup destination folder
Delete to original data	Delete original data after backup
Start Time/ End Time	Time spend for backup task
Status	Backup status, include cancel, successful or failed

Following action can be performed in the backup task list:

Item	Description
refresh	Refresh Task List

New Backup Task	Create a new backup task
Cancel Task	Cancel current backup task
Properties	View backup task detail information

Note Backup task only allow one process at any given time. No new backup task can be added while a backup task is progress.

10.2.2 Backup and Load Data

AiD version 3.2x is downward compatible with backup logs from version 3.0 and 3.1. Administrators can go to Tools --> Server Management --> Backup Management to load or backup Logs

◆ **Load Backups**

Go to Backup Management window and click on Load Backup button to load backed up logs. System can load up to 10 logs at once; log files are displayed in date format. Loaded data can be view via console, and it will affect current data structure

◆ **Remove Backup**

When loaded data no longer required, it can be remove from the backup management window. Administrators can click on one or multiple loaded record and click on Remove backup  button to remove loaded data.

11. Tools

11.1 Account Management

Administrators account has the highest level of authority of the entire system, this account can be used to add new administrators and set its authorities.

Go to Tools --> Account to add, remove and change passwords for created account.

Item	Description
	Add an account with descriptions
	Delete account, except admin account
	Disable an account except admin account
	Enable a disabled account
	Change account password, by default account set to blank

There are 3 major areas account management

Item	Description
General	Assign administrators type and login mode
Authorities	Administrators authorities to each module, logs and tools
Range	Used to assign administrators management range (Computer Group and User Group)

◆ General

Item	Description
Super Administrator	Has full access to entire system
Only allow to logon one console at a time	No multiple logon allowed
Only allow to log on specified PC or IP	Can only log on to console via specific computer or IP

◆ Authorities

Item	Description
File	Referring to the computer group and user group operations such as add, move to delete group. Also include export and print log feature.
Control	Referring to control to agent computers, include notify, lock/unlock computer, log off, power down. Restart and uninstall agents
Statistics	Referring to authority of generating statistic report
Log	Referring to authorities to view event logs.
Policy	Referring to policy editing authorities
Monitoring	Referring to authorities to view, search and export Screen Snapshot, Email, IM Message logs

Item	Description
Maintenance	Referring to the remote maintenance rights.
Asset Management	Referring to the authority to operating on Asset Management module
Patches	Referring to authorities to patch management
Vulnerability	Referring to the authority to operate Vulnerability
Software Deployment	Referring to the authority of create package and dispatch package
Intrusion Detection	Referring to authority to set up intrusion detection policies
Category management	Referring to authority to change category settings
Delete	Referring to authority to delete logs
Backup	Referring to authority to perform backup and review
Setting	Referring to the authority to set include and exclude IP ranges.
Generate Confirmation Code for Agent	Referring to the authority to generate agent confirmation code
Manage Encrypted Disk	Referring to disk encryption policy setting and categorization

Item	Description
Format as Encrypted Disk	Referring to the authority to create encrypted disk.
Email Report	Referring to authority to set up email alert report
Agent Update Management	Referring to authority to access agent update management feature
Computer Management	Referring to the authority to access computer management. This feature will only be effective when “All Computer and Users” in Range tab is selected.

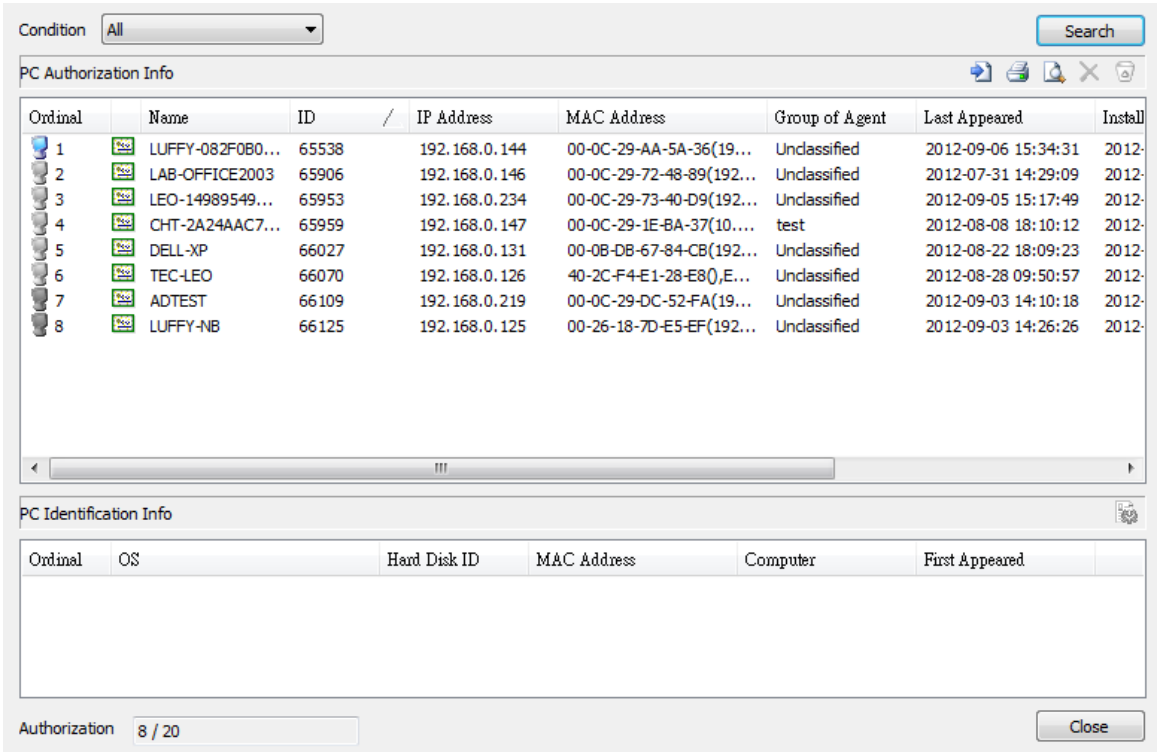
Administrators should not assign unnecessary authority to any account.

11.2 Computer Management

Computer management can be used to view the latest AiD license information. And use resolve conflicts between agents.

11.2.1 Computer Management

Go to Tools --> Computers to enter computer management feature.



Computer management includes the following:

Items	Description
	Icon represent computer has a valid license. For computer without this icon please refer to “Authorization” at bottom of the window to verify license usage.
Name	Agent computer name, if computer name been renamed on the computer tree it will be display in bracket.
ID	Unique computer ID assigned by server
IP Address	Agent computer’s IP address
MAC Address	Agent computers MAC address
Group of Agent	Group agent computer belongs to
Last Appeared	Last time agent computer appear online
Install Date	Agent installed time

Items	Description
Version	Version of AiD agent；
Days Offline	Number of days agent appear offline

Click on any record to view PC identification information in bottom panel

PC Identification Info include the following

Item	Description
	Indicate agent computer is current bind to this record
OS	Operating system of agent computer
Hard Disk ID	Hard Disk ID of agent computer
MAC Address	MAC address of agent computer
Computer	Computer Name
First Appeared	Time of agent first appear online

The following are search condition:

Item	Description
All	Search computer install with agent
By IP Address	Search computer by IP range
By Last Appear Time	Search by last appearance date
By Agent ID	Search by Agent ID assigned by server
By Name	Search by computer name and field support wild card search
Offline for >= days	Used to locate computer had been offline more than specific days

Icon Description

Item	Description
	Export information as HTML, xls or csv file format
	Print Computer Authorization Info
	Preview Print
	Delete, used to regain unused license key
	Uninstall, this action will not reduce license count

For Delete and Uninstall action a prompt window will appear to confirm action in order to reduce disoperation.

11.2.2 Re-assign Agent ID

Re-assign agent will be required under following situation

1. When two agent computers swap its hard drive or new operating system installed using image file rather than new installation.
2. Replacing faulty hard drive or network card may result new agent ID generated

Procedure to reassign：

1. Click on device information highlighted with red text
2. Click on  button in the PC Identification Info Panel

   A. Create a new agent ID for a specific PC and computer will appear under unclassified group.

   B. Move selected PC ID to a specified agent, agent ID can be manually input or select by click on “…” Button. When move computer name of the computer will be changed.

11.3 Synchronization Configuration

Active directory group structures can be imported to AiD data structure. When agent install it will automatically report to group defined in Active Directory.

11.3.1 Import Active Directory Domain

Steps as followed：

1. Login to AD Domain

   Go to Tools --> Synchronization Configuration -> Import Domain Organization, and enter required information

   If console computer is already login to the domain, click on default button to import domain name.

2. View Domain Group Structure

   Once logon to the domain computer and users can be view in the domain structure window.

3. Select Import Computers

   Select computer or groups to import into AiD server

4. Select Target group

   Click on  button to select import to computer or user group.

5. Import

   Click on Import button to perform import.

If select nodes are set to import different group structure than active directory, system will prompt to overwrite current group structure.

11.3.2 View Synchronization Configuration

To view synchronization configuration details go to Tools --> Synchronization Configuration --> View Synchronization Configuration. Imported node can be delete or modify from this window.

11.4 Alert Message

Alert message records all alerts triggered by policy, it can be view by go to Tools --> Alert. When alert occurs a pop up window will appear on console, click on the pop up window to all alerts.

By default maximum alert display set to 500 records, administrators can go to Tools--> Options --> Real-time Alert -->Number of alerts will be displayed to change maximum record display.

Alert message will be cleared when administrators re-login to console. To query alerts go to Event logs --> Policy.

11.5 Email Notification Settings

Email Notification Alert can be send via email and administrators can get a grip on the network environment in real time.

11.5.1 Email Notification Server

Emails Notification Server need to be set before administrators can receive alert via email, go to Tools --> Options --> Settings and setup of Email Notification Server to set up email server.

Item	Description

Setting List	Add, Modify and delete Email Notification Server

Button Descriptions:

Item	Description
	Add new email notification server
	Delete email notification server
	Modify email notification server
	Move up
	Move Down
	Mark as default email notification server
	Cancel default email notification server status

Mail alert sending policy adopt top-down approach, if condition match email will be send using matched setting, else no email alert will be send

Field Require for Email Notification Server

Item	Description
Configuration Name	Name of the mail server setting
Server IP	IP address or server name of the mail server
Port	SMTP port,　Port 25 set as default
SMTP Account	Account used to login to server
Password	Password of the account
Secure Connection（SSL）	Select “This server requires a secure connection” to send email via SSL protocol

Sender Address	Senders email address
Display Name	Senders display name
Mailbox Collection	Mail box used to receive email alert such as @gmail.com ; @pchome.com.tw。

◆ **Example**

Due to corporate policy, company email server can not send/receive mails from other main domains. Therefore AiD alert emails need to deliver to an additional email domain to notify offsite administrators.

1. Set an mail server configuration setting and use @companyname.com. as matched mail box
2. Set another mail server configuration setting and use @gmail.com. as matched mail box. Set this mail server setting as default

11.5.2 Email Notification Settings

Go to Tools -> Email Notification Setting to add, modify and delete mail report settings

Item	Description
	Add report setting
	Delete report setting

Email alert require the following information

Item	Description
Name	Name of the mail configuration setting
Email Subject	Subject of email

Item	Description
Max No of Alerts	Maximum alert of each email. Alerts exceed this defined number will be send in next mail
Min Alert Level	Minimum alert level, alert will be sent if policy alert level is equal or above defined level. Alert level includes Low, High and Critical.
Send Interval （Minute）	Mail setting interval, 30 minute been set as default.
To	Alert receiver email address
Send Test Email	Send test mail to verify setting
Send as Attachment	Send alert in attachment format
Unzip Password	Set password to the compressed file
Alert Type	Set email alert type, type include application alert, system alert website alert etc.
Computer Range	Alert computer range
User Range	Alert user range

NOTE Computer range and user range are in OR relationship. One of the status match email will be sent.

Mail sending status can be found in Event Logs --> System.

11.6 Policy Manager

Policy Manager can be found at Tools --> Policy Manager. From this window administrators can easily identify policy status.

11.7 Agent Tool

◆ Confirm Code Generator

Confirm code generator can be used to remove policy when end user is out of administrators condole.

Follow steps below to clear end user policy

1. On agent computer hold “Ctrl+Alt+Shift” and enter ocularat to open dialog window.
2. Select “Clear all policies” and generate OP Code.(Operation Code)
3. In popup window, take down the original OP code and send it back to administrator
4. Administrators must go to Tools --> Agent Tools --> Confirm-Code Generator to parse Operation Code Info
5. Administrator needs to confirm information submitted and click on Generate button to generate confirmation code.
6. Replay confirmation code to end user to remove all policies

◆ Agent Offline Utility

Agent offline utility can be used to temporary clear policy or uninstall agents. Steps as followed:

1. Administrators can go to Tools--> Agent Tools --> Agent Offline Utility to generate exe file to temporally remove policies or uninstall agents
2. Select available options and press next to enter effective executions, effective execution time and password. (password can be empty)
3. Once setting completed select export path and click on Next button to generate EXE file. End users can run the EXE file to remove agent or temporarily disable policies.

11.8 Server Time

Incorrect server time may affect the correctness of recorded logs, therefore system time monitoring mechanism was built to monitor and prevent server time error. System will prompt an alert message to administrators to confirm current time. Server time can be verify by go to Tools --> Server Management --> Server Time.

11.9 Category Synchronization Management

In the event of category information change server will perform synchronization to agent computers.

By go to Tools --> Server Management --> Category Sync Management administrators can glance over the category sync status.

Item	Description
	Query to locate a specific computer
	Display last synchronization time of each category

11.10 Agent Update Management

AiD upgrade includes AiD server and agent upgrade. Once server upgrade completed agent computer will receive an install upgrade file dispatched by server, system reboot required to complete upgrade process.

Automatic dispatch and install option required activation. Go to Tools --> Server Management --> Agent Update Management to set up upgrade

details.

Item	Description
Upgrade Settings	
Allow agent downgrade to lower version	Allow agent computer to downgrade agent version when server lower version than agent
Stop the upgrade when upgrade package changed	Agent shall automatically upgrade to the latest version unless this feature selected.
Distribution Period	Only dispatch upgrade file to computer within defined time period
Range	Upgrade to computers in specified range
Status	Status of the computer define in the range

11.11 Option

Go to Tools --> Option to view and modify current console and server's default value.

11.11.1 Console Setting

Console setting include the following items:

Items	Description
Basic Setting	
Login Setting	Includes remember password at login, Auto Logon and alert when password is empty.

Items	Description
Close Setting	Include minimized window to the system tray or close window and prompt when closing main window.
Sound Setting	
Enable Sound	Select this to enable play sound when alert or notify occurs.
Sound Type	Alert or Notify；
File Path	Path of the Wav file, support wav file less than 100kb
Log Viewing	
Log query Result	Number of record displayed per page
Real-time Info	
Screen Monitoring	Time interval to track frames(Sec): screen refresh interval, system default value at 2 seconds
	Time interval to jump to next PC automatically(Sec): Screen rotation period, system default set to 30 seconds
	Show visible screen only
Maintenance	Time interval to refresh application list: system default at 2 seconds
	Time interval to refresh process list: system default at 2 seconds
	Time interval to refresh performance info: system default at 2 seconds
Remote Control	Lock remote PC’s keyboard and mouse by default
	Do not control remote PC by default

Items	Description
Real-time Alert	
Alert Window	Number of alert will be display, system default at 500
Bubble Setting	Pop up alert window display on console
	Trigger level are Low, High and Critical
Agent Offline Alert	Pop up alert when agent offline over specified days, system default at 10 days.
Abnormal Agent Alert	Pop up alert when abnormal agent appear

11.11.2 Server Settings

Server setting includes the following:

Item	Description
Patches	
Install patches on new agents automatically	Select this option to install downloaded patch to new agent computers
Download patches automatically	Download new windows patches automatically
Data Cleanup	By default this feature not enabled
Global Setting	Keep all data, server will not delete any data
	Keep data within a specified number days, system default set to 30 days

Item	Description
Custom Settings	Allow to set data retention days separately Can select to inherit from global settings or define retain days
Management Range	
Search Range	Set server control IP ranges. Server will actively scan IP range for new agents
Only allow PC's within the search range to connect to server	Only allow computer included in search range to connect to connect the server
Exclusion Range	Server will not actively scan computers in listed range. And computer in listed IP-range will be prohibited from connecting to the server.
Connection	
Bandwidth setting between server and agent	Used to limited bandwidth between agent and server, range between 1-102400 kb/s. This setting may be handy for VPN network setup.
Active Polling	Server will actively scan end points 8235 port and retrieve data
Directory	
Directory Setting	List of directories storing AiD information's include data, cache, patches, backups etc. Listing are the default directory, changes will apply after restart AiD server service.
Set Directory	Press on  to select new directory

Item	Description
Restore Directory	Press on  to restore to default directory
Performance	
Fixed Mode	Maximum simultaneous connection server allows, range set between [0-100]
Dynamic Mode	Server will automatically adjust its loading. Loading refer to the loading of database process, Normal loading set at 30%, high at 50% and low at 10%. By default system set at dynamic mode server process level at Normal Real time screen monitoring and remote control are not bounded by this setting
Error Log	
Log Error messages while agent is being validated	Will record error logs when this option selected. Error logs can be view at Event Logs --> System
Lowest level of error message to log	Lowest recording level All — Report all error logs Low — Report unexpected result from agent Moderate — Exceed license key limit High — Agent serial number verification or check code error Critical — Communication error between server and agent due to range exclusion
Automatically remove agent	

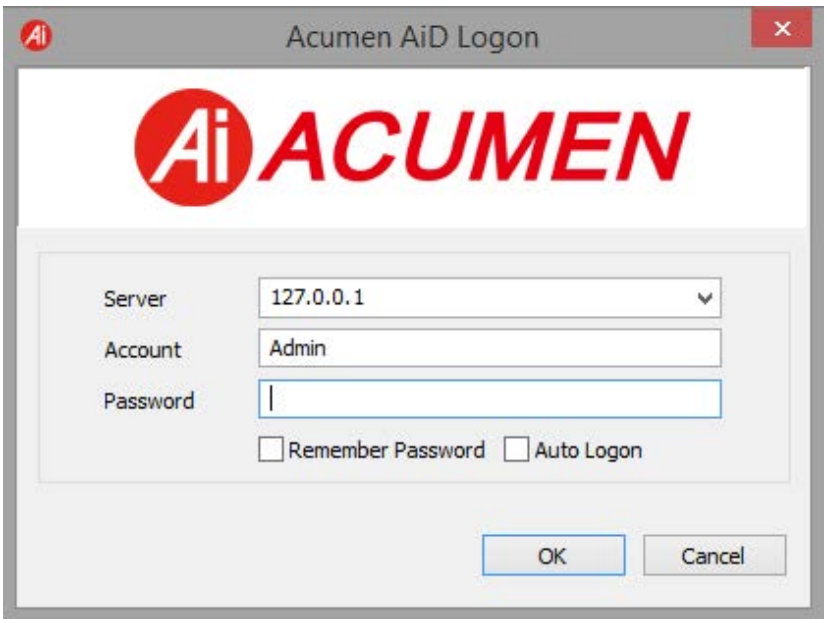
Item	Description
Automatically remove agent when it’s not logs on	Check this option to remove agent not log on for a specific day period

12. Audit Console

Like agent event logs all administrators' operation are recorded and record logs can be access from audit console.

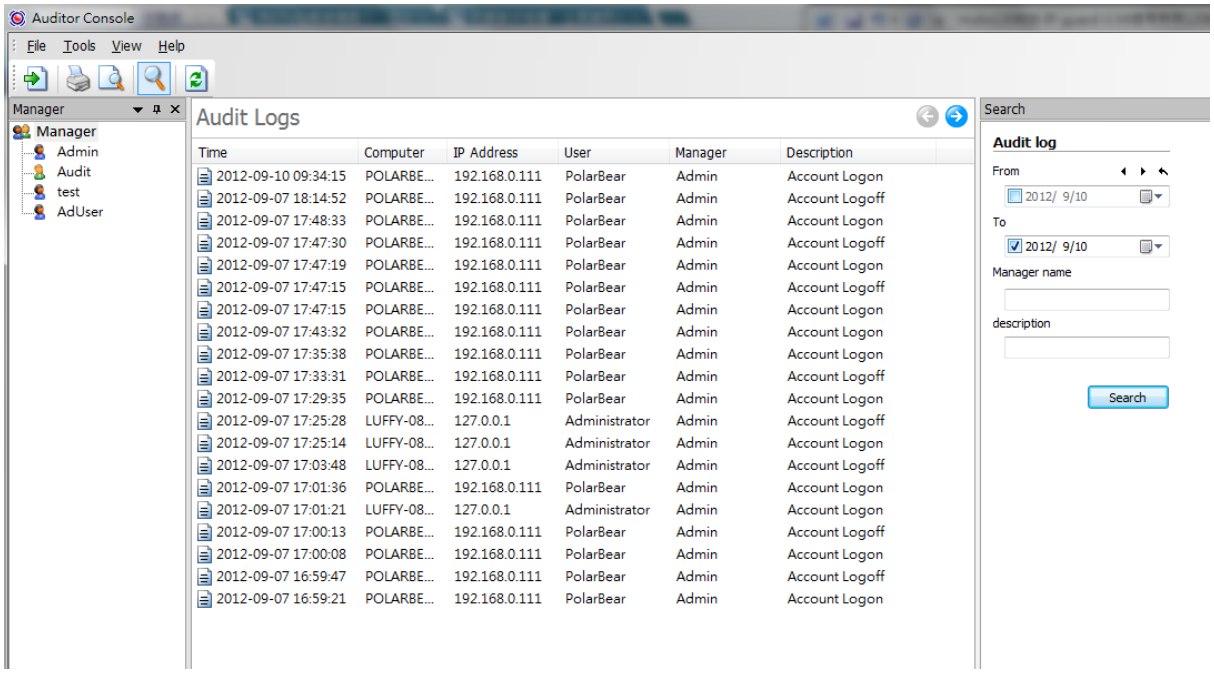
12.1 Login to Audit Console

Logon to AiD as usual, in the account field enter "audit" and leave password field as blank to logon to audit console.



12.2 Audit Console Interface

Audit console include the following, title bar, menu bar, tool bar, administrators column, data panel, search panel and status bar.



Manager column shows list of administrators, operation log per administrators can be view by selecting a specific administrator.

Audit logs provided print, export, save and delete feature.

Item	Description
Print/Print Preview	Select File --> Print/Print Preview to print or view current logs
Export	Select File --> Export or right click on data panel and select export to export logs
Delete	Delete logs by right click on data panel, select Delete and delete by “Selected” record, “Record of current page” or “All Matched Records”

12.3 Using Audit Console

◆ Audit Log

Audit logs include login info, administrator’s operation logs, policy edit/delete logs, agent screen viewing logs, remote logs and administrators account modification logs

Audit logs include the following:

Item	Description
Time	Recorded time for corresponding operation
Computer	Logon Computer Name
IP Address	Logon Computer IP Address
User	User logon to the computer
Manager	Logon administrators account name
Description	Description of the operation log

◆ Audit Log Query

Auditors can use the search panel to search for specific logs

Item	Description
From/To	Search for logs between From and To date
Manager name	Search logs by console logon account name
Description	Search log by specific keyword

◆ Create Audit Account

Audit account can be created by go to Tools --> Accounts

Items	Description
General	Used to account details similar to console administrators setup
Authorities	Control authorities such export and delete
File	Authority to export and print
Delete	Authority to print
Object	Auditing target, restrict auditors right in monitoring

13. Technical Support

Thank you for choosing our product, it’s our commitment to provide quality technical server. If there are any areas these user manual do not cover please contact with our technical support department and we will get back to you ASAP.