InsTIL™
Confidence in IT

User Manual

Table of Contents

1.0 General Information

1.0.1 System Overview

InsTIL is developed using Microsoft .Net. InsTIL runs on Microsoft Desktop Engine Database or Microsoft SQL Server. Since the front end is browser based, this provides the user flexibility to access the application from multiple locations.

1.0.2 Authorized User permission

This is a trademarked product from Precision Group. InsTIL, a licensed product, comes to the user with remote support, with the flexibility of scaling up based on the complexity and the requirements of the organization. InsTIL comes with an option of Annual Support Contract (ASC) after the first year of usage. The ASC helps the organization to get continuous support, special pricing on upgrades and much more even after a year's usage.

Being a licensed product, InsTIL warns against unauthorized usage of the system and making unauthorized copies of data, software, reports and documents. Unauthorized tampering would affect the performance and the stability of the application and the user is warned that a fresh license is required to be procured to reinstate the existing condition.

2.0 System Summary

InsTIL provides to the user six roles in terms of functionality. InsTIL also supports multi roles i.e. a Service Desk can be a Technician, Administrator and an IT Manager. The roles are defined as follows:

1. Site Manager
2. Administrator
3. Service desk
4. User
5. Technician
6. IT Manager

2.0.1 System Configuration

InsTIL can be deployed on a system that runs on Windows XP or above. As the application come to the user with a bundled MSDE database, investment on an exclusive database is minimized. However depending on the volume of internal transactions the user is provided the flexibility of using Microsoft SQL server also. InsTIL is developed using Microsoft .NET and therefore it can be accessed from most popular browsers

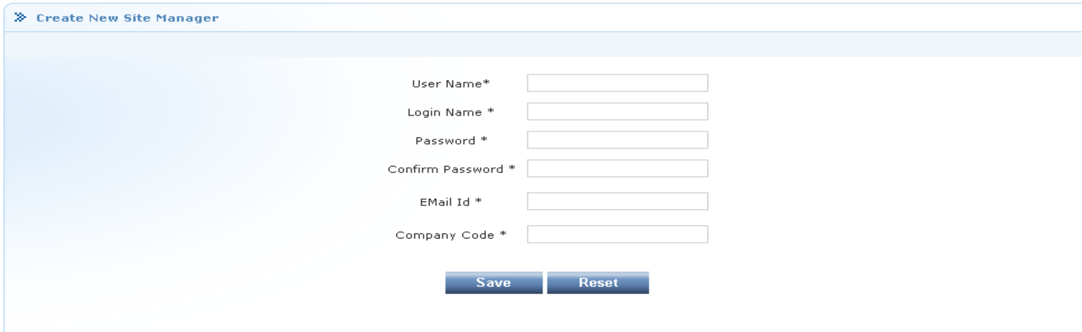
2.0.2 User Access Levels

The functionalities of various roles of InsTIL are listed in the table below

ROLE	FUNCTIONALITY
Site Manager	Managing and creation of companies and maintaining their licenses. Creation of Administrators for each company
Administrator	Network scan User synchronization through ADS Auto Service desk functionality Customizable E-mail alerts Incident Template creator Knowledge base and FAQ Report generation
User	Incident intimation, Call Classification, Call closure
Service Desk	Call logging on user absence, call classification, calls assigning / re-assigning. Remote Desktop Call Analysis report
Technician	Call updating upon actual investigation & Diagnosis Call Re-classification Call Logging on User absence
IT Manager	Overall management and reporting

3.0 Getting Started

After generation of license, a new window appears where the Site Manager account is created as shown below.



Creation of Site Manager

1. Enter the user name of Site Manager
2. Enter the login name
3. Enter the password and mail id of the Site Manager
4. Enter the company code
5. Click Save button to save the Site Manager created

3.1 Site Manager

The role of Site Manager is to create the companies and to control and allocate the license for the various companies in the organization. The Site Manager can also create the administrator for these companies. In this section we will go through how to add company and the various type of licensing.

Company creation

Operation:

To add a new company, Click New Button

Company Details:

1. Enter company code – The company code is necessary at the time of logging into the application for different companies
2. Enter company name and other details

Database Credentials:

1. Enter database server IP – The database can be in unique system or individual systems for various companies
2. The database name is automatically generated

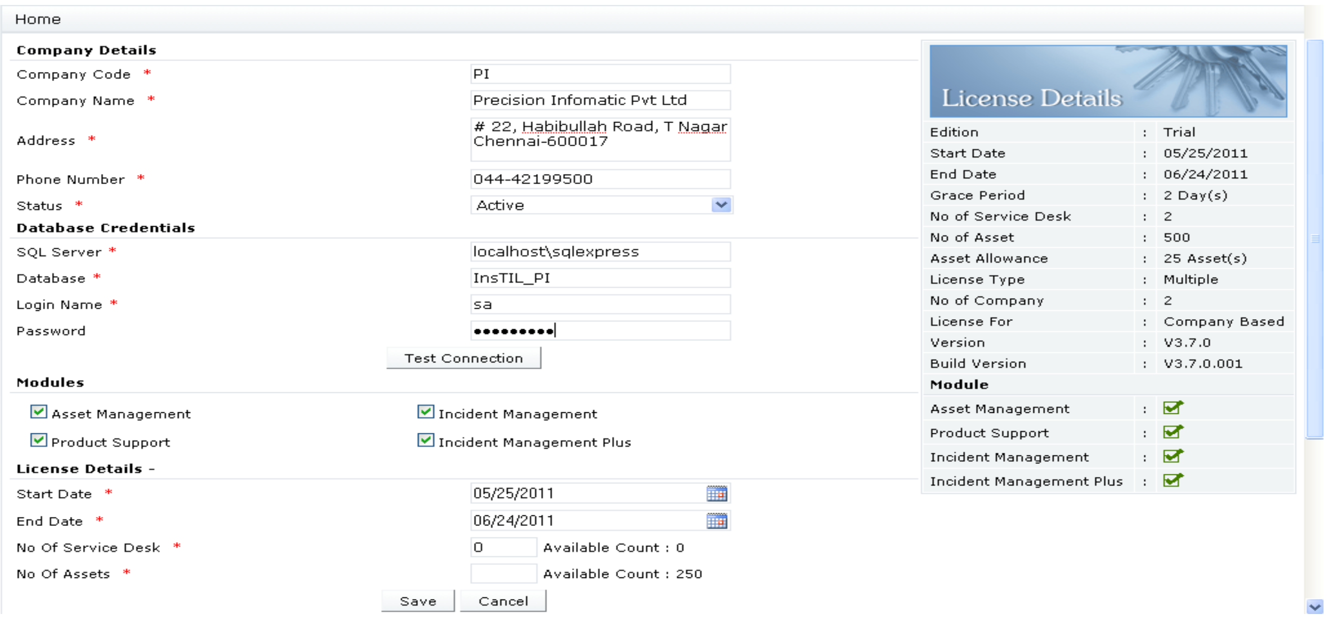
3. Enter the database user id and password
4. Click Test connection to connect the database.

Modules:

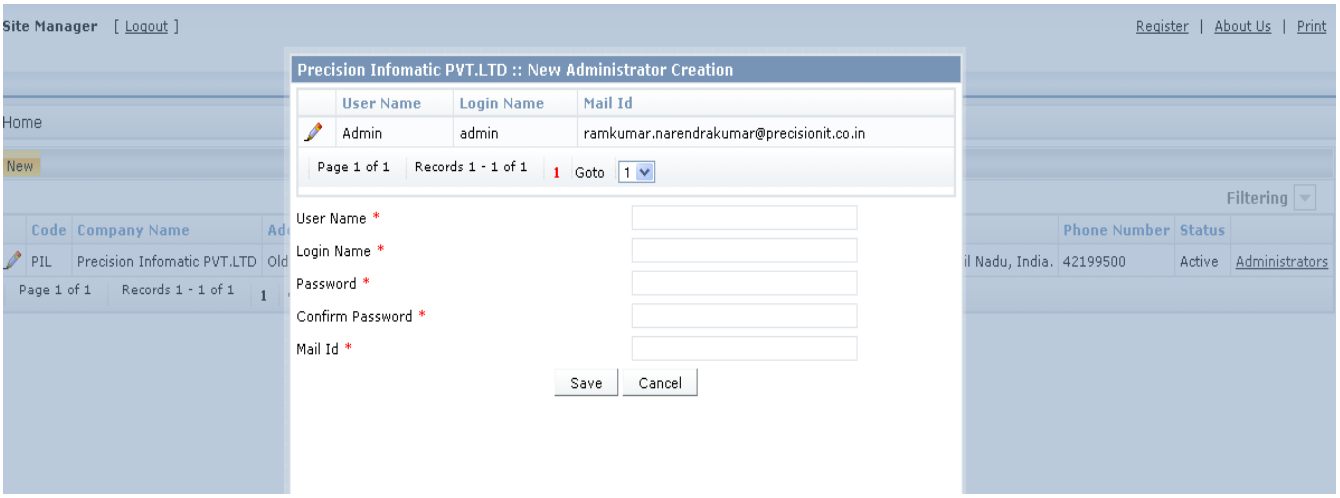
Select the modules that has to be available for the particular company

License Details:

For multi company: (Company based)
1. Choose start date – The period when the license begins
2. Choose end date – The period when the license ends
3. Enter the no of service desk and no of assets
4. Click Save button



Managing Administrator



Operation

1. Select the Administrator link from the respective Company name
2. Provide the details of Administrator like User Name, Login Name, Password, Confirm Password and Mail Id
3. Click Save to save the entry created

4.0 Logging in as Administrator

Just like any application, InsTIL also require master information related to the assets, users, complaints, service desk detail that needs to be created before the user or service desk or technician or IT Manager starts using this tool from their functional perspective. The Site manager creates the company and relevant information. The Site manager creates the InsTIL administrator who has the privilege of creating the master records related to the assets. Similarly master records related to user, service desk, organization are created by the administrator.

InsTIL Wizard

InsTIL wizard is the new feature enabled with the latest version of InsTILXpress. This wizard helps the administrator to ease the process of configuring the major functionalities covered in InsTIL like, Discovery of assets on the network, Discovery of users from Active Directory and Configuration of Service Desk etc., each from a separate wizard. For example - discovering the assets on the network, the administrator has to create the domain information, credentials for authenticating and create network name with IP ranges all in separate windows. This wizard helps the administrator to create all the above said master data information in a single process based configuration wizard.

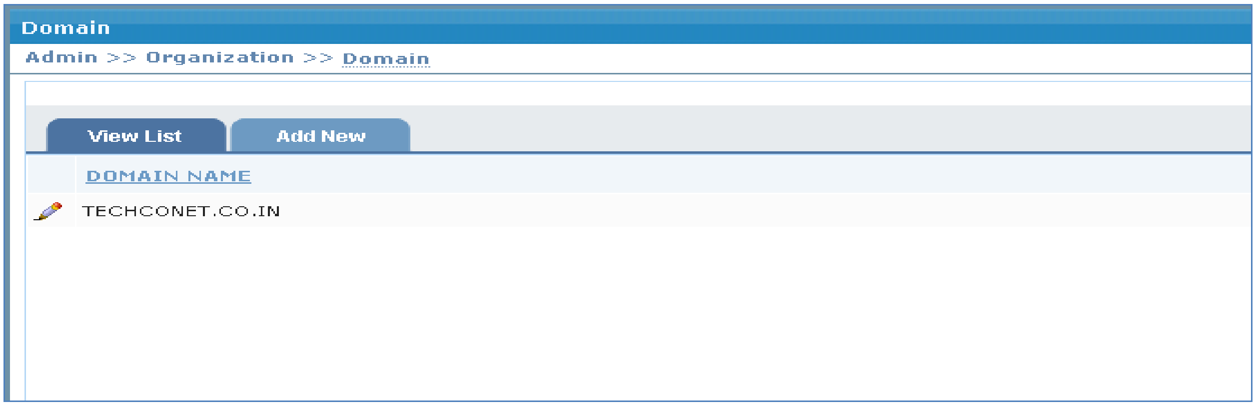
The various wizards currently available in InsTIL are;

1. Discover assets on network
2. Discover user from Active Directory
3. Configure Service desk

Discover Assets from network

By discovery we mean remotely capturing asset information for IP enabled devices such as Desktop, Laptop, Server, Router, Switch, Printer and getting vital information on their hardware and software configurations. The steps for using the wizard is given below

1. Click Wizard link from the Home Page
2. Select Discover assets on network
3. The description on what asset discovery is all about will be displayed and click Next to continue
4. The **Domain** name is captured by default, also the administrator can add additional domain on the same window by clicking Add New



5. Click Next to Continue
6. Click Add new to add a new credential. There are two types of credentials that can be added in InsTIL application a. WMI credential b. SNMP credential

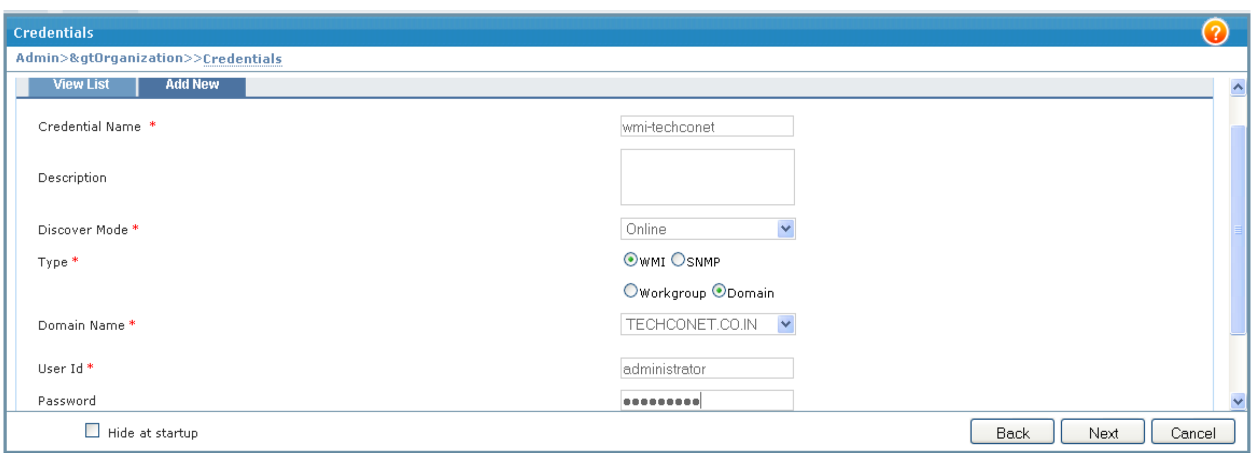
Steps to create SNMP credential

a) Click Add new credential

b) Enter an SNMP credential name
c) Select SNMP
d) Enter the community string value as public
e) Enter the timeout as 2000 (milli seconds)
f) Click Save to save the credential created

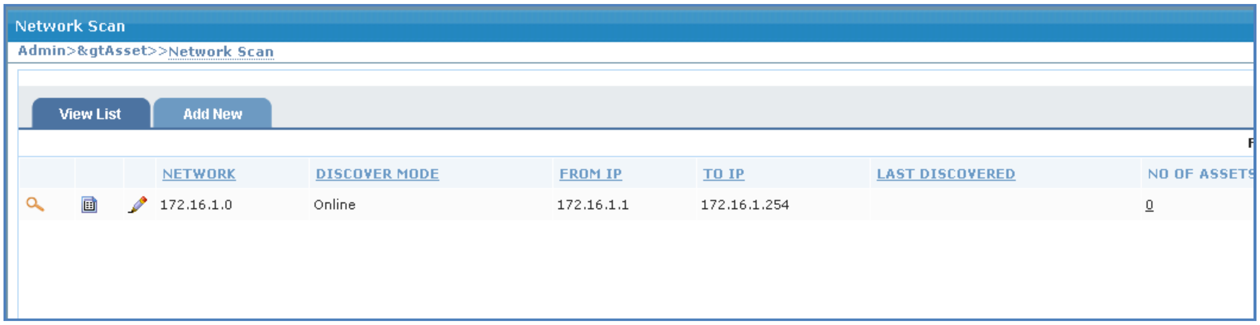
Steps to create WMI credential

a) Click Add new credential
b) Enter a WMI credential name
c) Select WMI
d) In WMI the credentials are created through workgroup or domain
e) Click on Domain as credential type and select the domain name from the dropdown list
f) The domain system name is automatically fetched from the Domain master
g) Enter the domain administrator username and password
h) Click Save to save the credential created

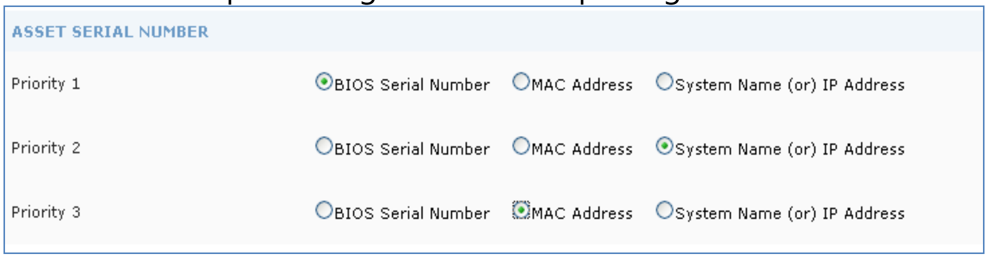


7. Click Next to create the network name along with the IP range for discovery
8. Enter a suitable network name based on various VLAN and select the discovery mode as online

9. Enter the IP range say for example 172.16.1.1 as From IP to 172.16.1.254 as To IP
10. Click save to save the entry created



11. Click Next to configure the settings for discovering the Asset serial number for each asset
12. There are three priorities given for the capturing the Asset Serial Number as shown below



13. Click submit to save the record and click Next to proceed with the next step
14. Click the Discover icon to start the asset discovery for the specified IP range
15. The assets in the specified range are automatically discovered and imported to the application
16. Click Next for scheduling a network scan
17. Select the network name, category and re-occurrence type
18. Click Save to save the entry created
19. Click next to configure the various services available in InsTIL
20. Click Finish to complete the wizard configuration

Similarly wizards can be used for configuring other two major features Active Directory Import & Service Desk configuration.

Quick Link

Quick Links is a bullet functionality, which provides short cuts to Administrators to perform a specific function. The quick links are available for the following menu in InsTIL. This helps the administrator to quickly navigate to the specified menu for the ease of operation.

1. Vendor
2. Asset Entry

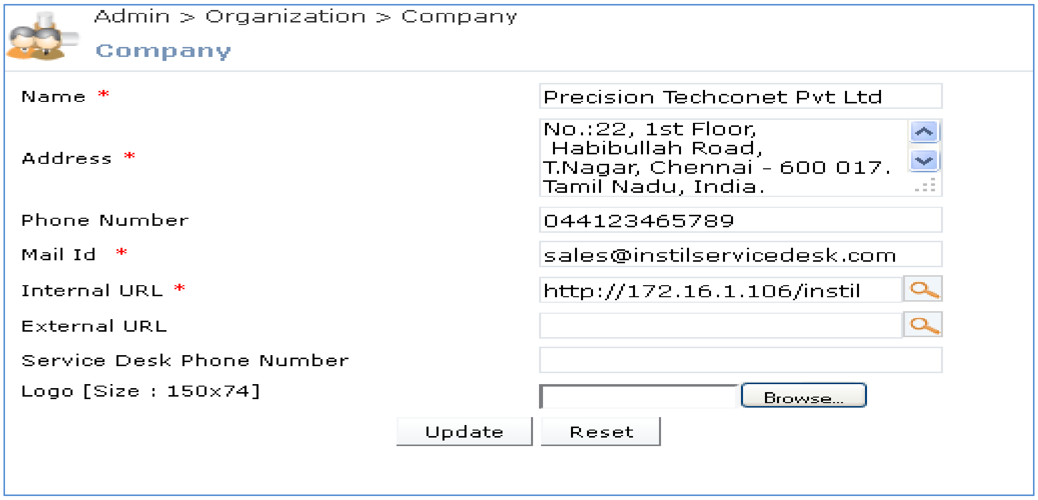
3. User Entry
4. User Asset Linking
5. FAQ
6. Knowledgebase
7. Escalation
8. Tasks
9. Settings
10. Preference

4.1 Organization

Defining Organization – Company

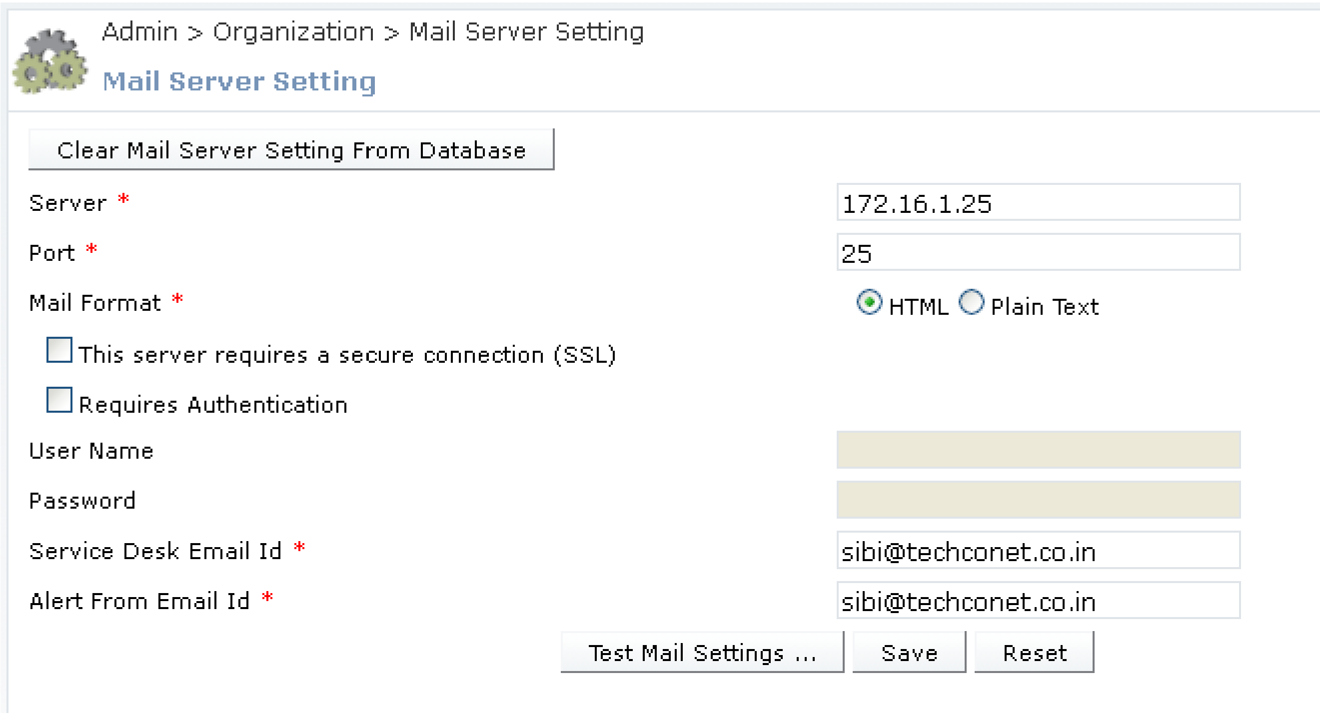
Operation

1. The company name and address is automatically generated when the license is configured for the company.
2. Enter the Company Mail Id
3. Enter the Internal URL – The Internal URL is given so that when a mail is triggered, the Internal URL is also displayed in the mail so that the user can log into the application from the URL which is displayed.
4. Enter the Service Desk Phone Number
5. Click Browse to Add the Company logo so that it appears on the screen.
6. Click Update button to update the records.



Defining Organization – Mail Server Setting

The below screen shows the Mail Server Setting. This screen enables the Administrator to provide the SMTP server settings for the mail triggering functionality in InsTIL. There is an option provided for the administrator to enter the secondary mail server information if required.



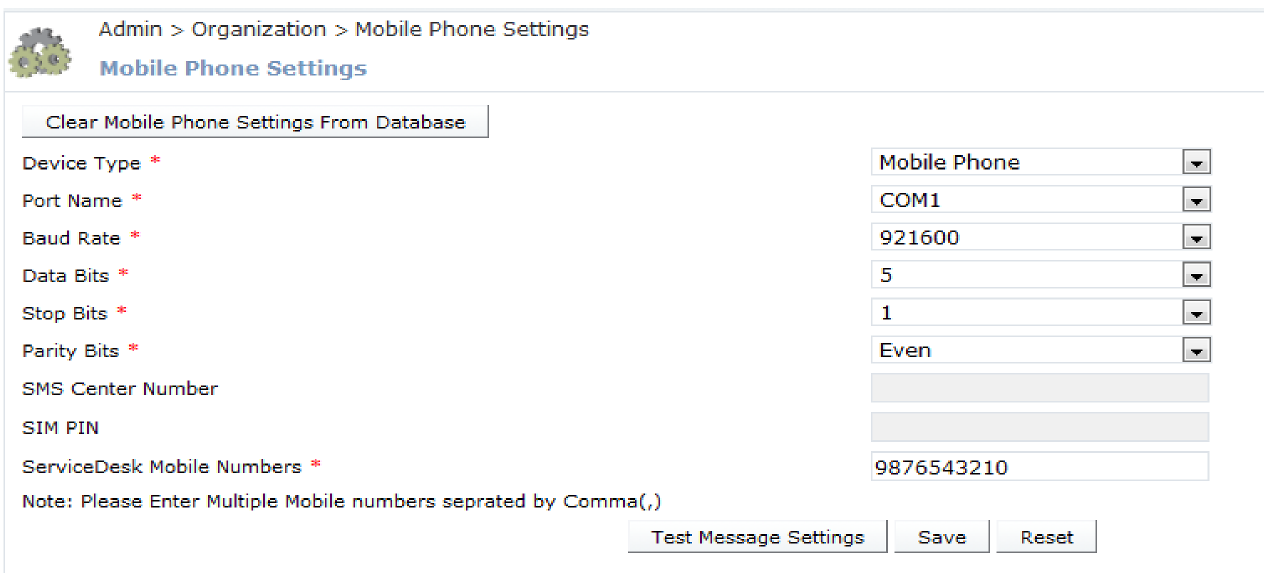
Operation

1. Enter the information of SMTP server IP and port details
2. Select the mail format as either HTML or Plain text. The email content appears based on the format selected
3. Enter the credentials required for the authentication to the mail server
4. Provide the Service Desk & Alert email id.
5. Enable Add a secondary mail server
6. Enter the information of SMTP server IP and port where the mail server is configured

7. Enable Require Authentication and provide the credential details like User name and Password.

Defining Organization – Mobile Phone Settings

InsTIL application provides SMS alerts in addition to Email alerts for various functionalities in the product like Incident handling, User creation, Escalations, AMC/Warranty/SLA Reminder and Task
This menu provides the administrator to configure the SMS settings required for the alert process. The below fig shows the SMS settings screen.



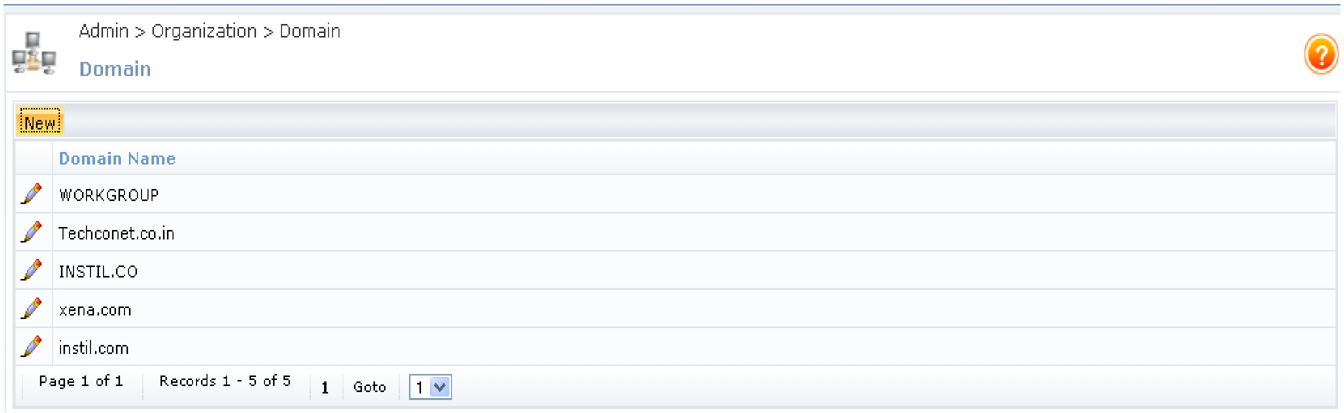
Operation

1. Select the device type as Mobile Phone or Modem
2. Select the assigned port name where the device is connected
3. Select the Baud Rate from the dropdown list provided. Baud rate is a measure for data transmission speed, which shows the number of signals transmitted per second.
4. Select the data bits from the dropdown list
5. Select the stop bits from the dropdown list
6. Select the parity bits from the dropdown list
7. Enter the SMS center number and SIM PIN if the device type is selected as Modem
8. Enter the Service Desk Mobile Numbers to whom the SMS alert is sent. An option is also provided to create multiple number
9. Click Test message settings to test whether the settings keyed in are correct.

10. To clear the information provided in the settings menu click Clear Mobile Phone settings from the database menu

Defining Organization – Domain

The below fig. shows the Domain Entry screen. The domain entry screen is to create the domains running in the organization. Discovery of the Assets and Bulk update of user can be done if the domains are created.

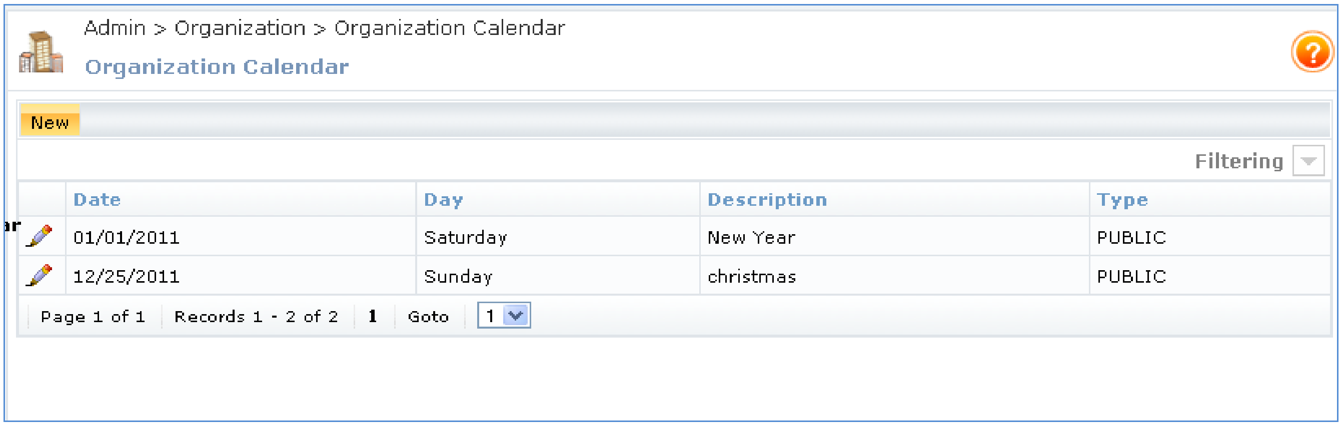


Operation

1. Click New to add a Domain.
2. Enter the domain name
3. Click Save button to save the entry created.
4. To clear the fields, click Reset button.
5. To update an existing record, select the record from the list and perform the required changes and click update.

Defining Organization – Calendar

This form is used to create the holidays of the organization. When an incident is raised by the user, the SD assigns it to the technician or vendor. By defining the holidays, the SLA will be calculated accordingly

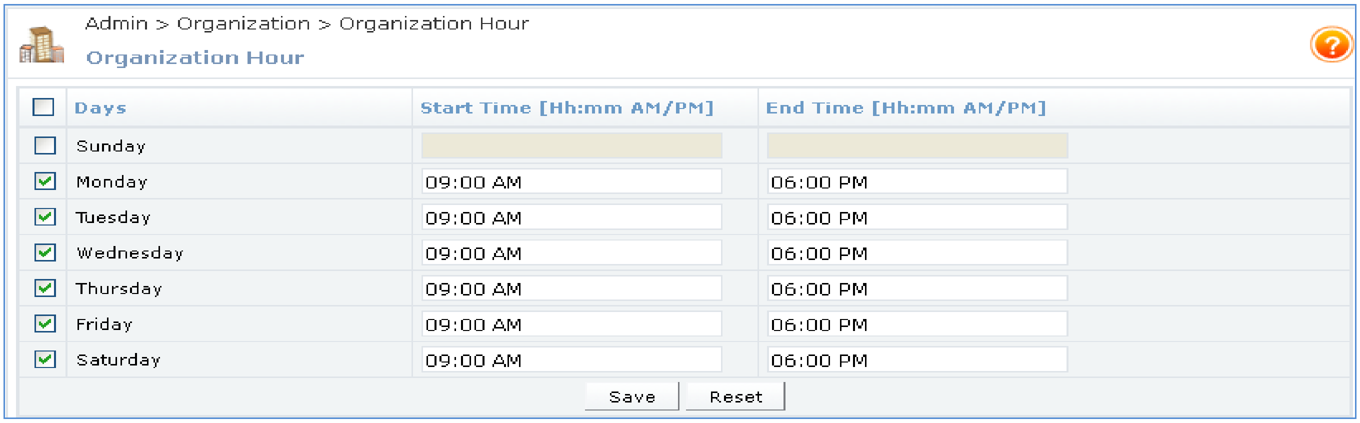


Operation

1. Click New for adding a Holiday entry.
2. Select the date from the date-time picker.
3. Enter the description of the Holiday.
4. Select the holiday type as public or private.
5. Click Save button to save the entry created.
6. To clear the fields, click Reset button.
7. To update an existing record, select the record from the list and perform the required changes and click update.
8. To delete an existing record, select the record from the list and click delete.

Defining Organization – Working Hours

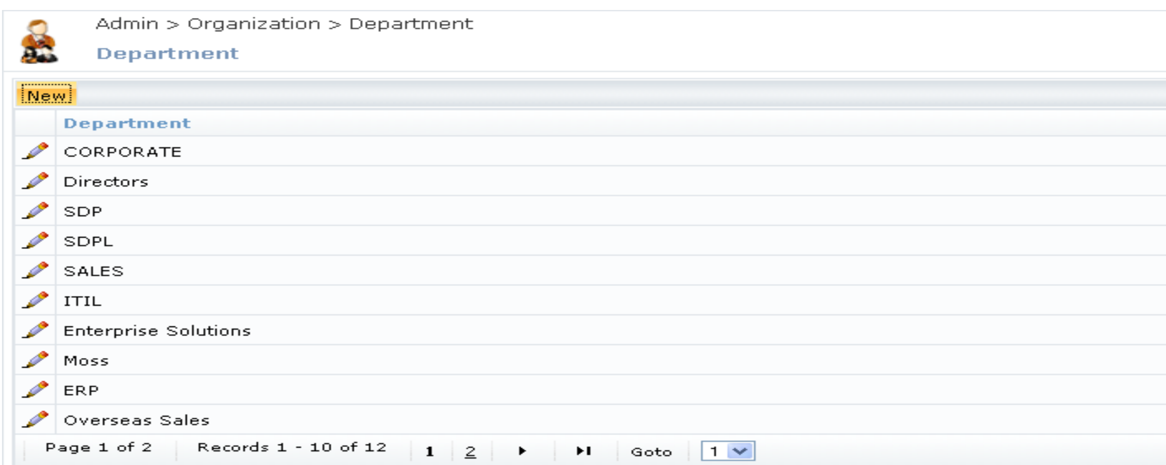
This form is used to create the working hours of the organization. When an incident is raised by the user, the SD assigns it to the technician or vendor. By defining the working hours, the SLA will be calculated accordingly



1. Enable the working days of the organization.
2. Enter the start time and end time of each working day.
3. Click Save button to save the entry created.

Defining Organization – Department

A department is an individual functional unit of any organization. For example Account, Finance, Marketing, Information Technology etc., are all considered as departments. Once InsTIL is integrated with the ADS the department details are automatically added to the department masters



Operation

1. Click New.
2. Enter the department name.

3. Click Save button to save the entry created.
4. To clear the fields, click Reset button.
5. To update an existing record, select the record from the list and perform the required changes and click update.
6. To delete an existing record, select the record from the list and click delete.

Defining Organization – Country

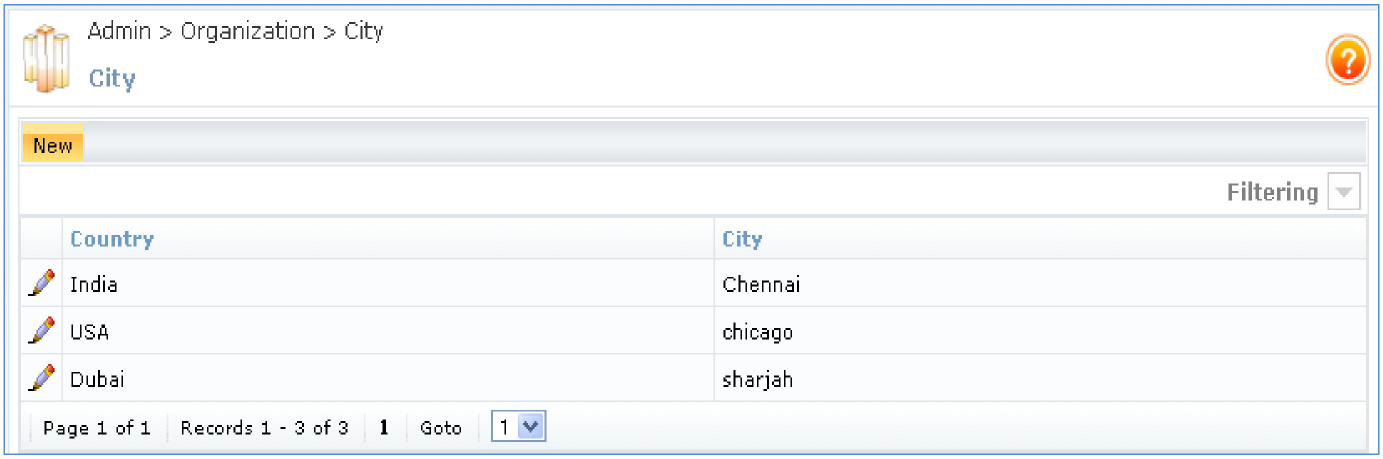
The below fig. shows the option to create the country name, where the organization is created. This will be helpful to map the Asset. Once InsTIL is integrated with the ADS the country details are automatically added to the country masters.

Operation

1. Click New
2. Enter the Country name.
3. Click Save button to save the entry created.
4. To clear the fields, click Reset button.
5. To update an existing record, select the record from the list and perform the required changes and click update.
6. To delete an existing record, select the record from the list and click delete.

Defining Organization – City

The city where the organization is located is created using this option. The below fig shows how to add a new city

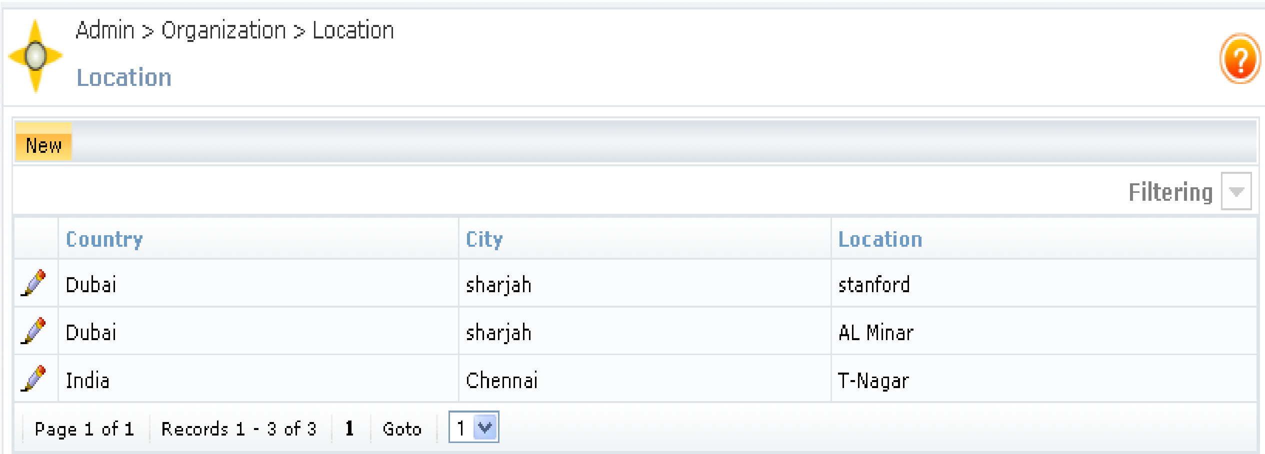


Operation

1. Click New
2. Enter the city name and select the country name from the drop down list
3. Click Save button to save the entry created.
4. To clear the fields, click Reset button.
5. To update an existing record, select the record from the list and perform the required changes and click update.
6. To delete an existing record, select the record from the list and click delete.

Defining Organization – Location

An organization may have multiple sites in the form of branches, cost Centre etc. This screen provides the user to create the location name and link it with the city where the location is situated.

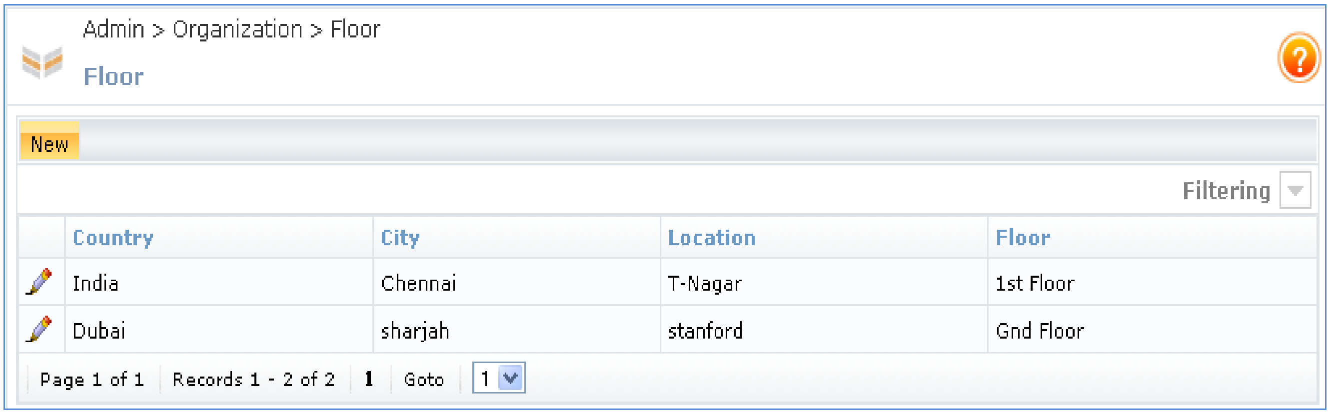


Operation

1. Click New
2. Enter the location name and select the city name from the drop down list
3. Click Save button to save the entry created.
4. To clear the fields, click Reset button.
5. To update an existing record, select the record from the list and perform the required changes and click update.
6. To delete an existing record, select the record from the list and click delete

Defining Organization – Floor & Bay

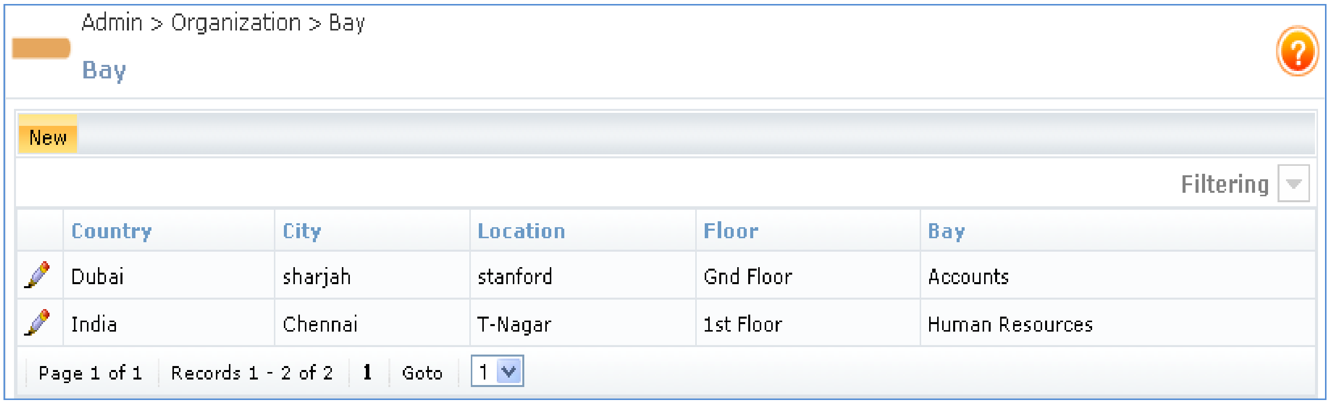
Floor and Bay master is created the same way as we created the other master records. Since, these two are self-explanatory, not much is described here. Bay represents the area within the floor of an organization.



Operation - Floor

1. Click New
2. Enter the floor name and select the location from the drop down list
3. Click Save button to save the entry created.
4. To clear the fields, click Reset button.
5. To update an existing record, select the record from the list and perform the required changes and click update.
6. To delete an existing record, select the record from the list and click delete.

Operation – Bay

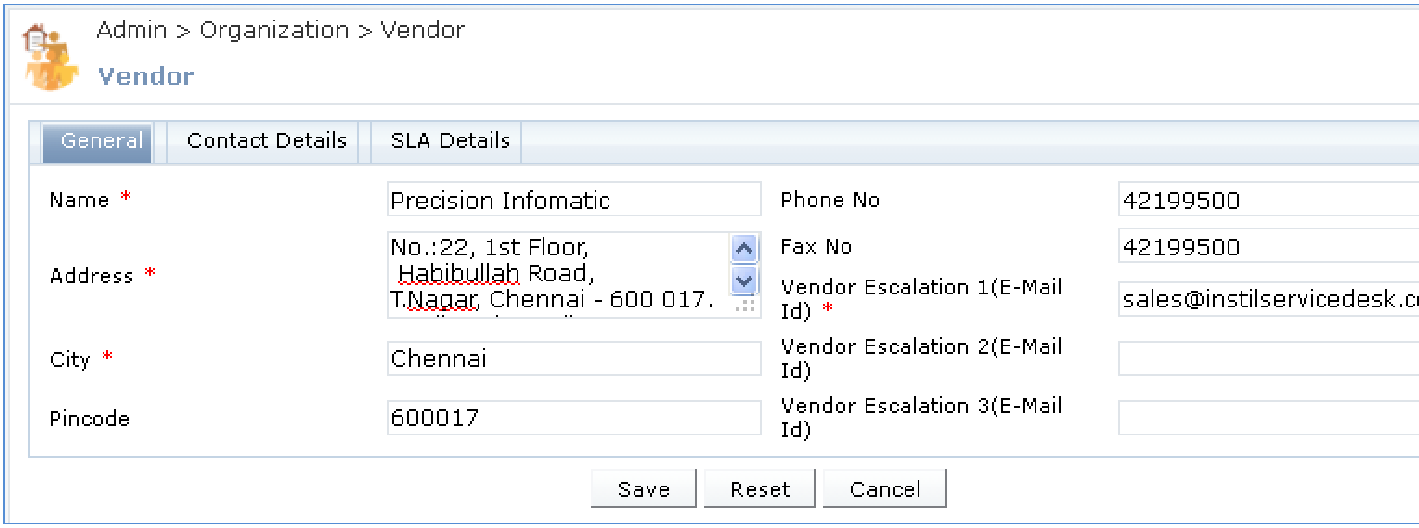


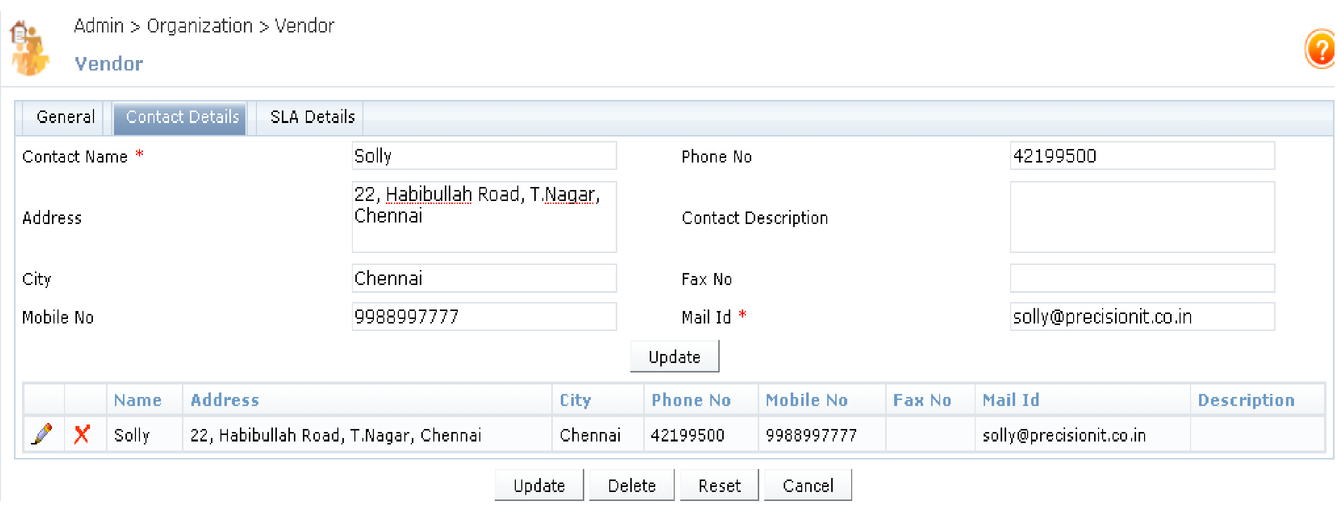
1. Click New
2. Enter the Bay name and select the location and floor from the drop down list
3. Click Save button to save the entry created.
4. To clear the fields, click Reset button.

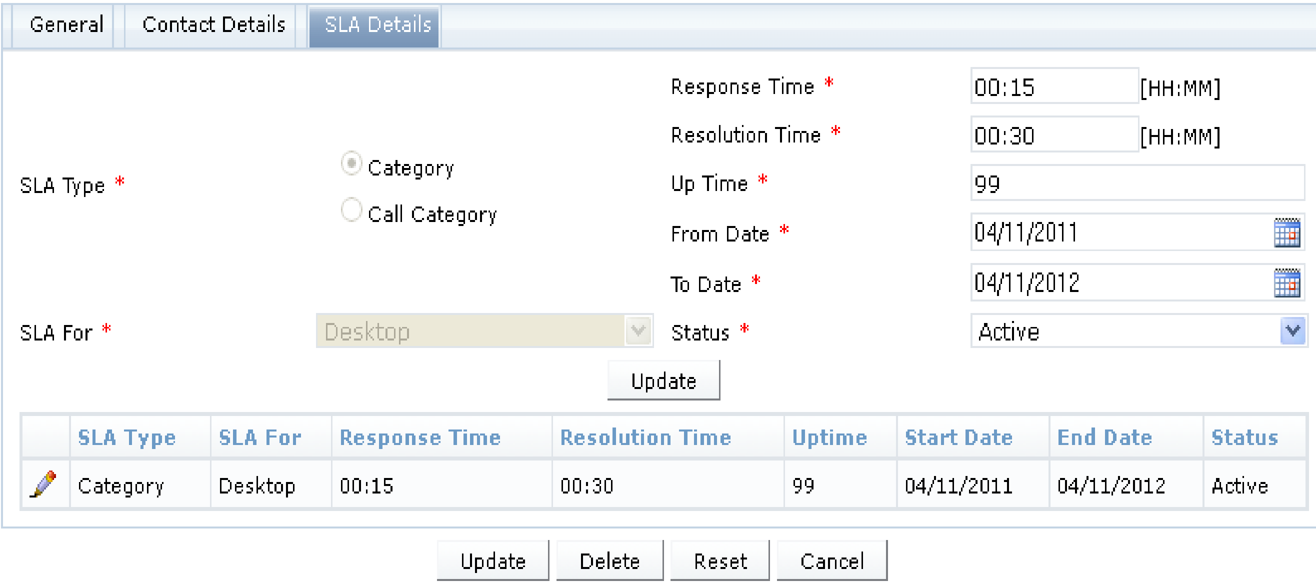
5. To update an existing record, select the record from the list and perform the required changes and click update.
6. To delete an existing record, select the record from the list and click delete.

Defining Organization – Vendor

The Vendor details of the organization are created in the Vendor master. The contact details and the SLA details of the vendor can also be added.





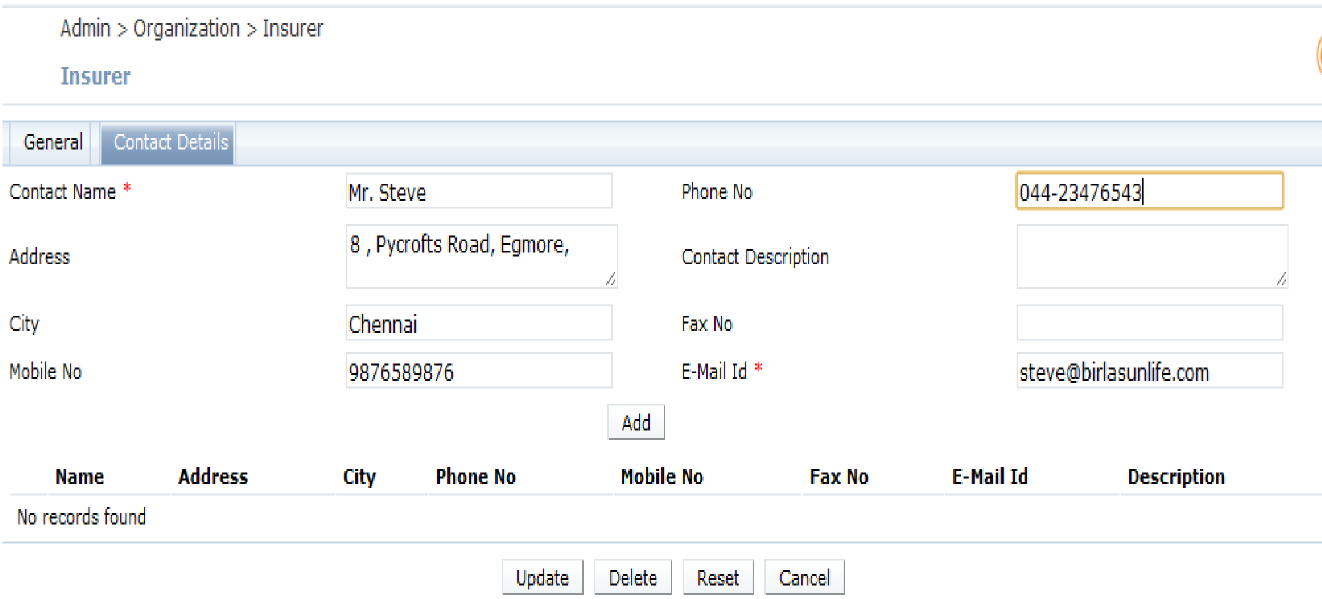


Operation

1. Click New
2. Enter the Vendor name, address and the Vendor Escalation Email Id
3. Click Contact details tab
4. Enter the contact name , mobile number and other details of the Vendor
5. Click Add to save the entry created
6. Click SLA details tab
7. Select the SLA type as Call Category or Category
8. Select the SLA for the selected SLA type
9. Enter the response time and resolution time.
10. Enter the Up Time for the SLA
11. Select the From date and To Date for the validity of the SLA with the vendor from the date time picker
12. Select the Status of the SLA
13. Click Add to save the entry created

Defining Organization – Insurer

The details of various insurers registered with the organization can be created here. The details include general and contact details of the Insurer.



Operation

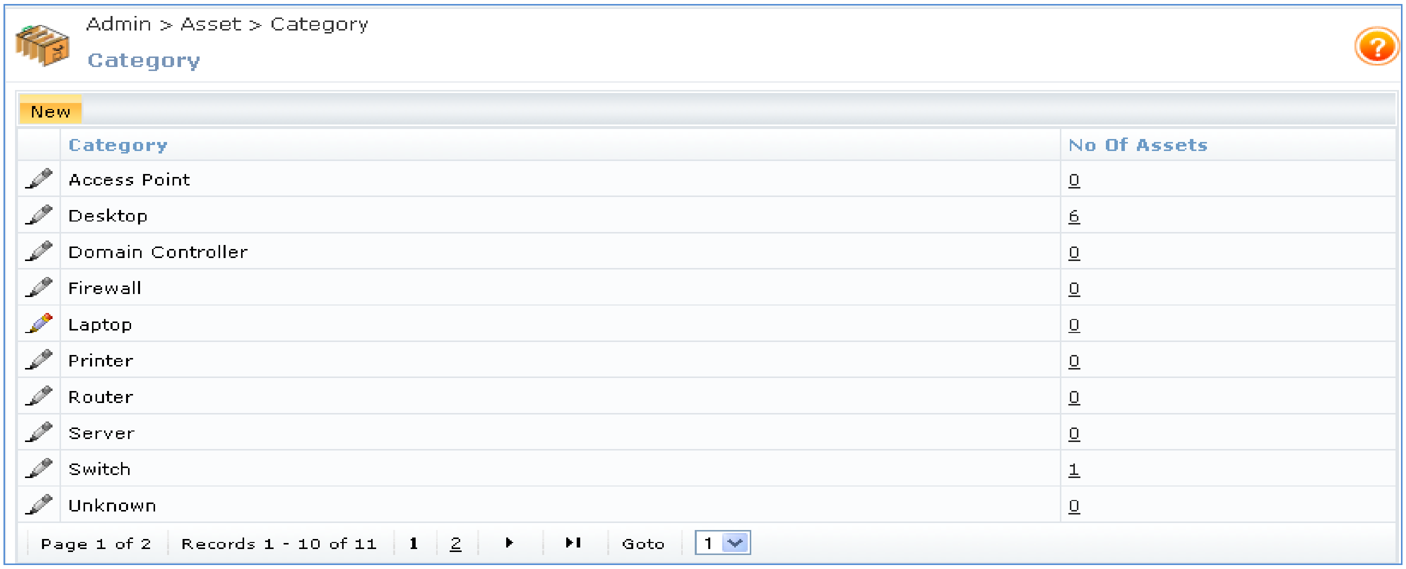
To add a new Insurer perform the following task

1. Click New
2. Enter the Insurer details like Name, Address, Email id etc.
3. Click Contacts tab to enter the contact details of Insurer.
4. Enter Contact Name, Contact Number, Email id etc.
5. Click Add to create contact information.
6. Click Save to save the entry created.

4.2 Assets

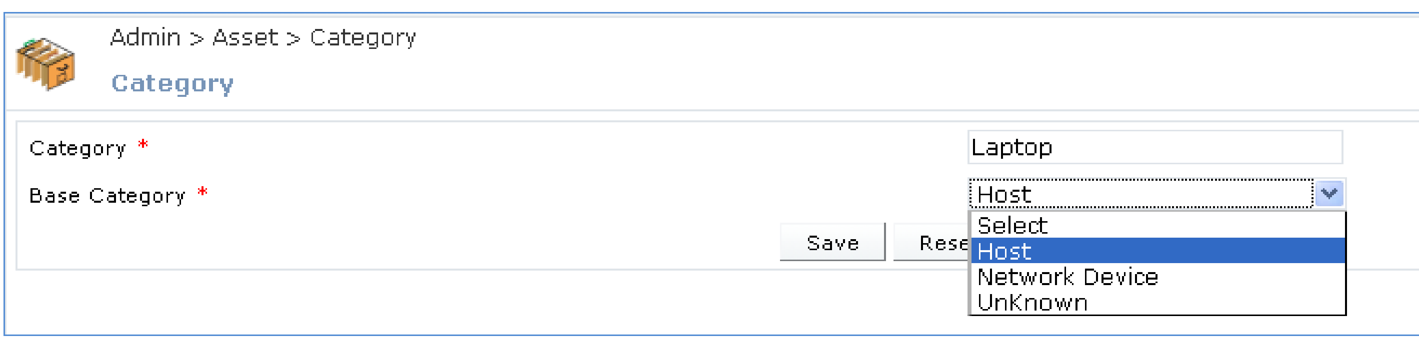
Defining Asset –Category

The administrator can define the type or category the Asset belongs to. By default the application defines a basic set of categories for an Asset. The administrator also has the option to create a list of asset categories as applicable. For each asset category the number of assets available is also shown.



Operation

The below fig. represents the create option for Asset - Category. The administrator can create the category name as shown in the top panel of the screen

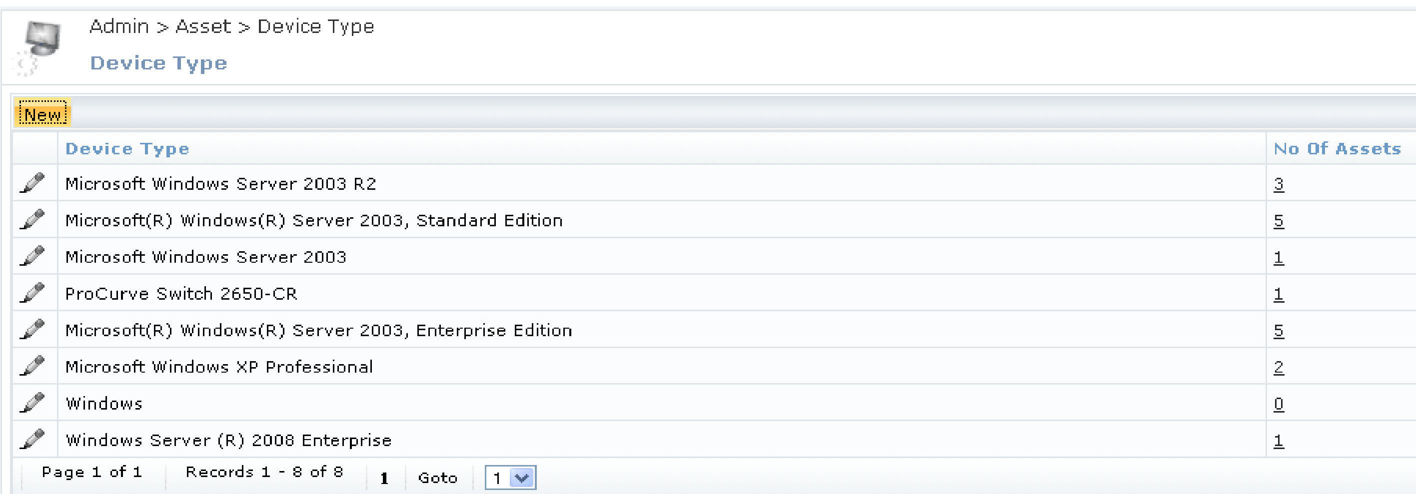


To add a new category name

1. Click New
2. Enter the category name.
3. Select the base category type from the dropdown list. The base category type defined by default are Host, Network Device and Unknown
4. Click Save button to save the record entered
5. Click Reset button if you need to reset the field entries

Defining Asset –Device Type

The device type of the assets can be added manually apart from the already discovered device type when the auto discovery process is done. For each device type the number of assets available is also shown.



Admin > Asset > Device Type

Device Type

New

Device Type	No Of Assets
Microsoft Windows Server 2003 R2	3
Microsoft(R) Windows(R) Server 2003, Standard Edition	5
Microsoft Windows Server 2003	1
ProCurve Switch 2650-CR	1
Microsoft(R) Windows(R) Server 2003, Enterprise Edition	5
Microsoft Windows XP Professional	2
Windows	0
Windows Server (R) 2008 Enterprise	1

Page 1 of 1 Records 1 - 8 of 8 1 Goto 1

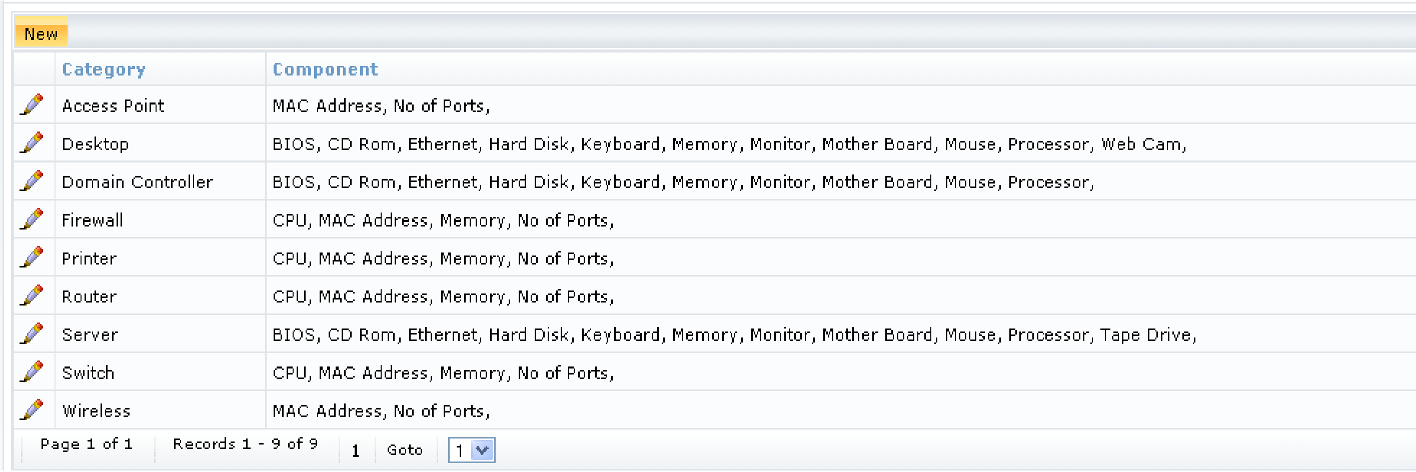
Operation

The below fig. represents the create option for Asset – Device Type. The administrator can create the Device Type as shown in the top panel of the screen

1. Click New
2. Enter the Device Type
3. Click Save to save the record
4. Click Reset button to reset the entries
5. Click Cancel button to cancel the process.

Defining Asset –Component

The below fig. represents the create option for Asset - Component. The Components that will be part of the Asset Family can be created here. The application is defined with certain component type for each Asset Category and also additional component can be added. The components created can be mapped to a particular group of assets of the same Part Description.



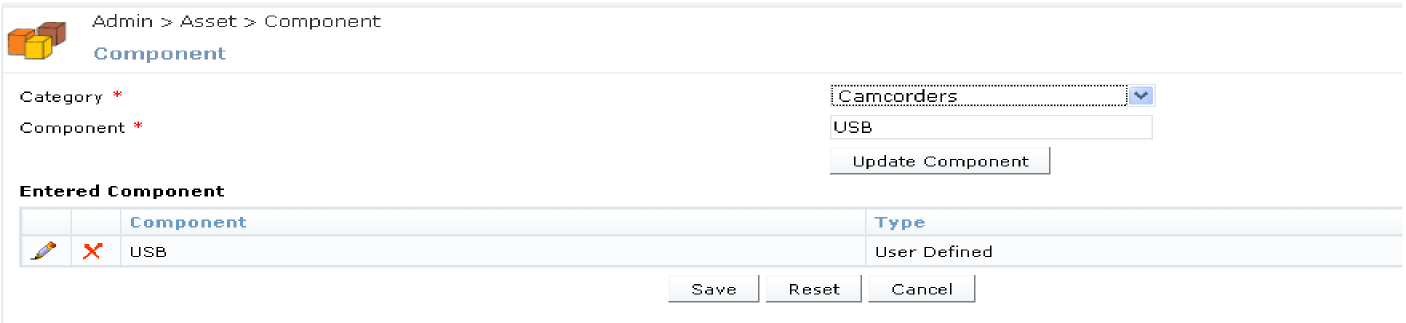
New

Category	Component
Access Point	MAC Address, No of Ports,
Desktop	BIOS, CD Rom, Ethernet, Hard Disk, Keyboard, Memory, Monitor, Mother Board, Mouse, Processor, Web Cam,
Domain Controller	BIOS, CD Rom, Ethernet, Hard Disk, Keyboard, Memory, Monitor, Mother Board, Mouse, Processor,
Firewall	CPU, MAC Address, Memory, No of Ports,
Printer	CPU, MAC Address, Memory, No of Ports,
Router	CPU, MAC Address, Memory, No of Ports,
Server	BIOS, CD Rom, Ethernet, Hard Disk, Keyboard, Memory, Monitor, Mother Board, Mouse, Processor, Tape Drive,
Switch	CPU, MAC Address, Memory, No of Ports,
Wireless	MAC Address, No of Ports,

Page 1 of 1 | Records 1 - 9 of 9 | 1 | Goto 1

Operation

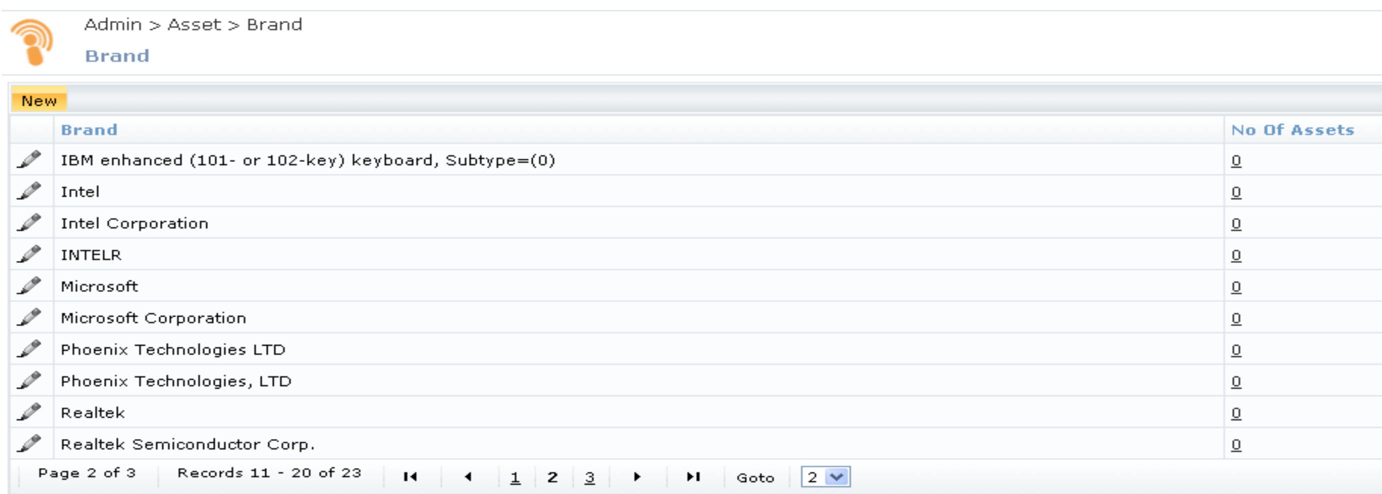
The below fig. represents the create option for Asset –Component. The administrator can create the component name as shown in the top panel of the screen



1. Click New
2. Select the Category name from the drop down list
3. Enter the component name to be linked with the Category type and click Update component
4. Click Save to save the save the record
5. Click Reset button if you need to reset the field entries

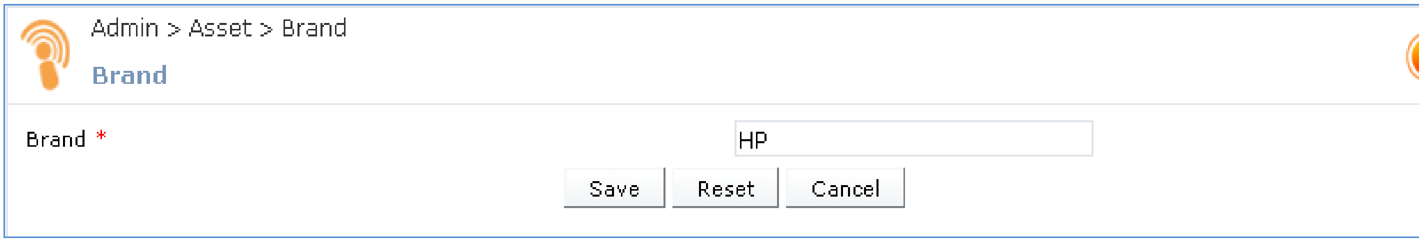
Defining Asset – Brand

The below fig. represents the create option for Asset – Brand. The brand name provides you a picture of what all brands available at your organization



Operation

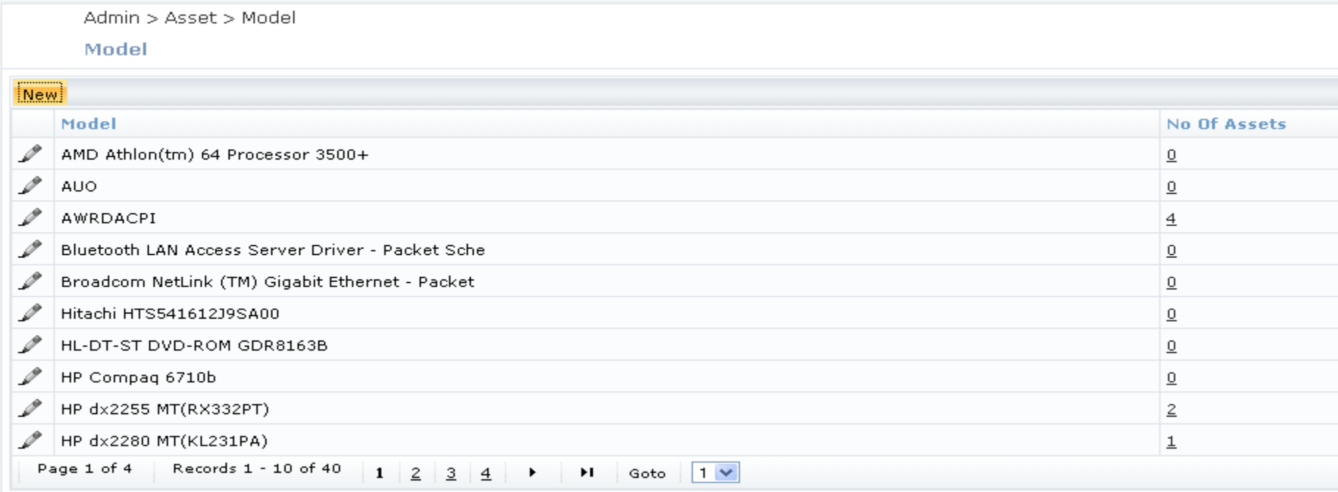
To Add a Brand name for the Asset



1. Click New
2. Mention the Brand name.
3. Click Save to save the record.
4. Click Reset button if you need to reset the field entries

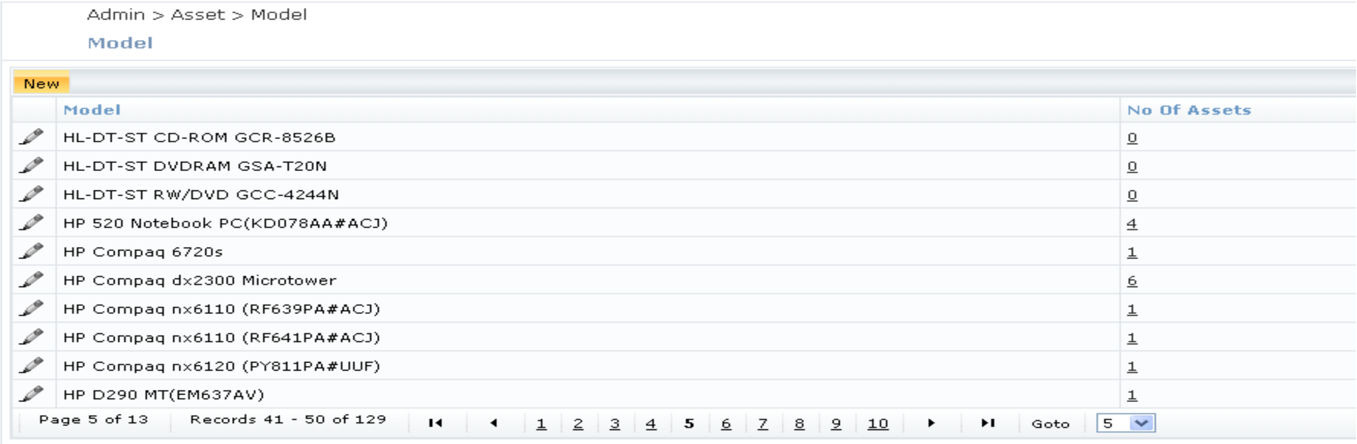
Defining Asset – Model

The below fig. represents the create option for Asset – Model. The Model name will be helpful at the time of Asset creation to classify the Assets.



Operation

To add a new Model name



Admin > Asset > Model

Model

New

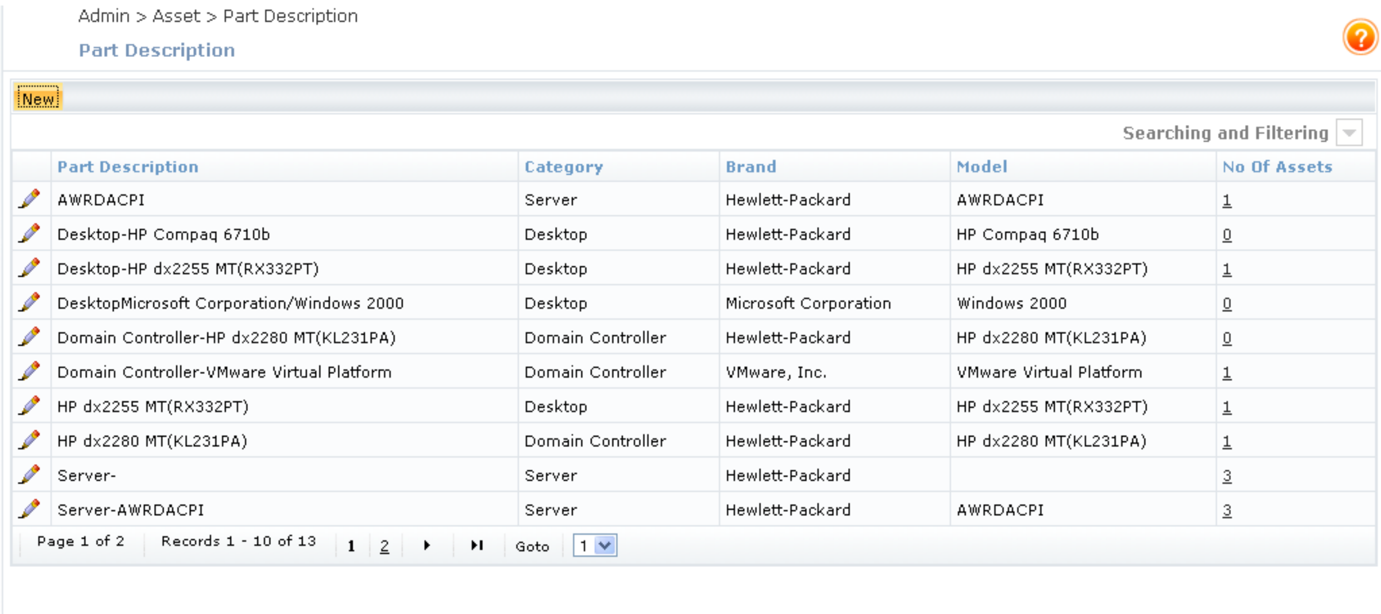
	Model	No Of Assets
	HL-DT-ST CD-ROM GCR-8526B	0
	HL-DT-ST DVDRAM GSA-T20N	0
	HL-DT-ST RW/DVD GCC-4244N	0
	HP 520 Notebook PC(KD078AA#ACJ)	4
	HP Compaq 6720s	1
	HP Compaq dx2300 Microtower	6
	HP Compaq nx6110 (RF639PA#ACJ)	1
	HP Compaq nx6110 (RF641PA#ACJ)	1
	HP Compaq nx6120 (PY811PA#UUF)	1
	HP D290 MT(EM637AV)	1

Page 5 of 13 Records 41 - 50 of 129 1 2 3 4 5 6 7 8 9 10 Goto 5

1. Click New
2. Enter the model name of the Asset – For Example Compaq 6510b
3. Click Save to save the entry created
4. Click Reset button if you need to reset the field entries
5. Click Delete button to delete that particular record

Defining Asset – Part Description

The below fig. represents the create option for Asset – Part Description. The administrator can create the Part Description for the Family, Brand and the Model of the Asset created. The Part Description will be helpful at the time of Asset creation. When the network scan is performed and assets are discovered the part description master data are automatically captured and added to the master information



Admin > Asset > Part Description

Part Description

New

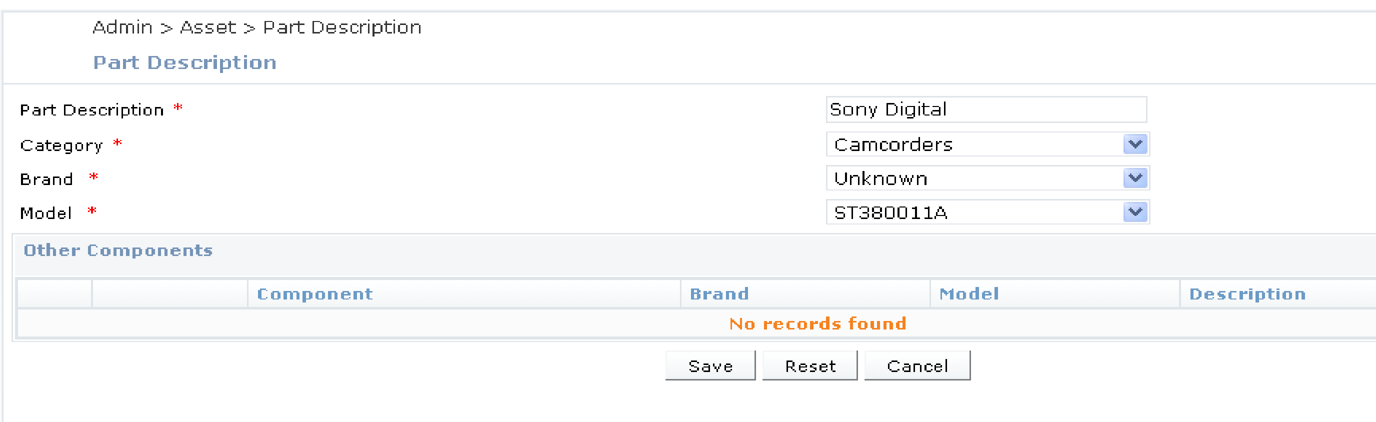
Searching and Filtering

	Part Description	Category	Brand	Model	No Of Assets
	AWRDACPI	Server	Hewlett-Packard	AWRDACPI	1
	Desktop-HP Compaq 6710b	Desktop	Hewlett-Packard	HP Compaq 6710b	0
	Desktop-HP dx2255 MT(RX332PT)	Desktop	Hewlett-Packard	HP dx2255 MT(RX332PT)	1
	DesktopMicrosoft Corporation/Windows 2000	Desktop	Microsoft Corporation	Windows 2000	0
	Domain Controller-HP dx2280 MT(KL231PA)	Domain Controller	Hewlett-Packard	HP dx2280 MT(KL231PA)	0
	Domain Controller-VMware Virtual Platform	Domain Controller	VMware, Inc.	VMware Virtual Platform	1
	HP dx2255 MT(RX332PT)	Desktop	Hewlett-Packard	HP dx2255 MT(RX332PT)	1
	HP dx2280 MT(KL231PA)	Domain Controller	Hewlett-Packard	HP dx2280 MT(KL231PA)	1
	Server-	Server	Hewlett-Packard		3
	Server-AWRDACPI	Server	Hewlett-Packard	AWRDACPI	3

Page 1 of 2 Records 1 - 10 of 13 1 2 Goto 1

Operation

To add a new part-description for the Asset performs the following tasks.



Admin > Asset > Part Description

Part Description

Part Description *	Sony Digital
Category *	Camcorders
Brand *	Unknown
Model *	ST380011A

Other Components

		Component	Brand	Model	Description
No records found					

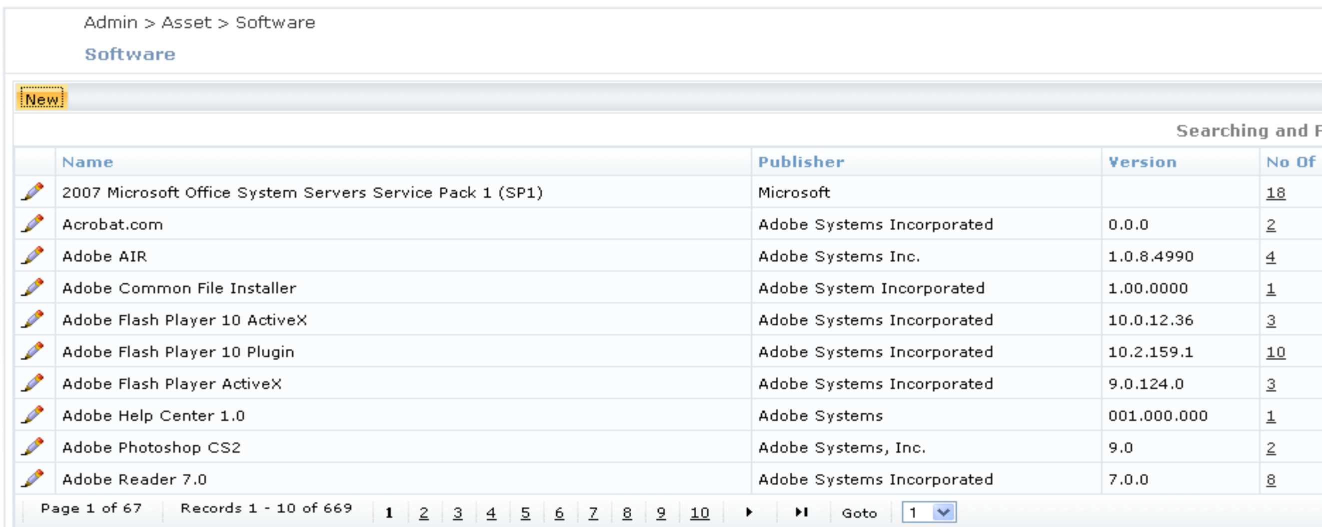
Save Reset Cancel

1. Click New
2. Enter the Part Description Name - The Part Description will be helpful at the time of Asset creation
3. Select the Category Name from Category Dropdown List box
4. The components related to the selected category will be displayed along with provision to enter the description for each component.
5. Select the Brand name.
6. Select the Model name.

7. Click the Save Button to save the record.
8. Click Reset button if you need to reset the field entries

Defining Asset - Software

The details of the software's available and their procurement details can be added to the Software master. When the network scan is performed and assets are discovered the software master data are automatically captured and added to the master information. The administrator can also find the no of assets in which particular software is installed.

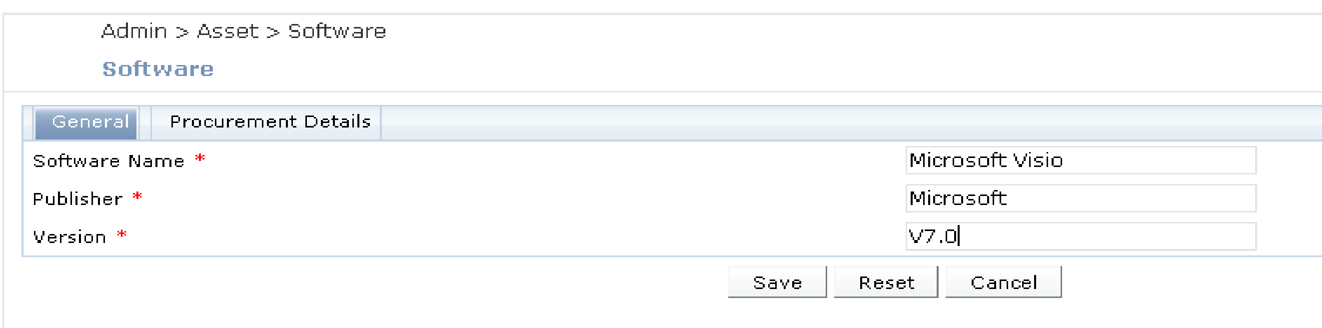

Admin > Asset > Software
Software
New
Searching and F

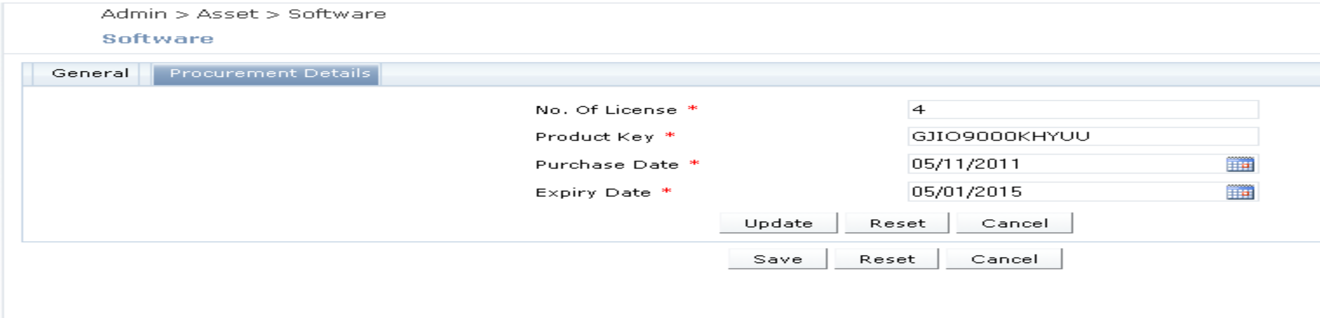
Name	Publisher	Version	No Of
2007 Microsoft Office System Servers Service Pack 1 (SP1)	Microsoft		18
Acrobat.com	Adobe Systems Incorporated	0.0.0	2
Adobe AIR	Adobe Systems Inc.	1.0.8.4990	4
Adobe Common File Installer	Adobe System Incorporated	1.00.0000	1
Adobe Flash Player 10 ActiveX	Adobe Systems Incorporated	10.0.12.36	3
Adobe Flash Player 10 Plugin	Adobe Systems Incorporated	10.2.159.1	10
Adobe Flash Player ActiveX	Adobe Systems Incorporated	9.0.124.0	3
Adobe Help Center 1.0	Adobe Systems	001.000.000	1
Adobe Photoshop CS2	Adobe Systems, Inc.	9.0	2
Adobe Reader 7.0	Adobe Systems Incorporated	7.0.0	8

Page 1 of 67 Records 1 - 10 of 669 1 2 3 4 5 6 7 8 9 10 Goto 1

Operation

To add a new software perform the following tasks





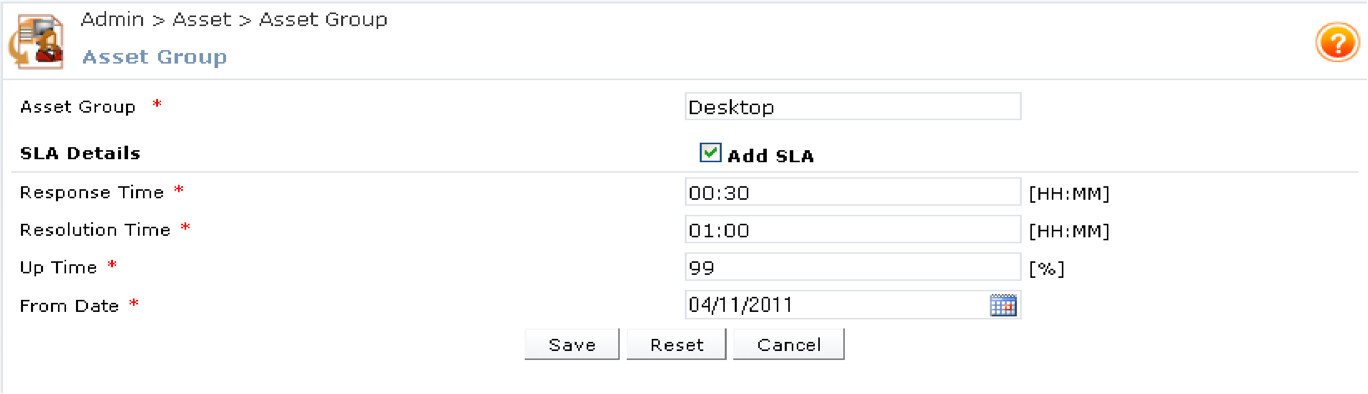
a. Click New
b. In the General tab enter the name of the software, publisher name and the software version
c. Click Procurement Details tab and enter the following information
   i. No of License
   ii. Product Key
   iii. Purchase Date
   iv. Expiry Date
d. Click Save to Save the entry created
e. Click Reset to clear the entries created.

Defining Asset - Asset Group

The below fig. represents the create option for Asset – Asset Group. The administrator can create the Asset Group for which the service level agreement (SLA) applies. Asset group can be a division or a department or a cost center of an organization for which the service level expectation can be defined. Service level is divided into response and resolution. Response is the time frame within which the service has to be attended and Resolution is the time frame within which the problem needs to be solved. Up time is percentage of time that system has to be active.

Operation

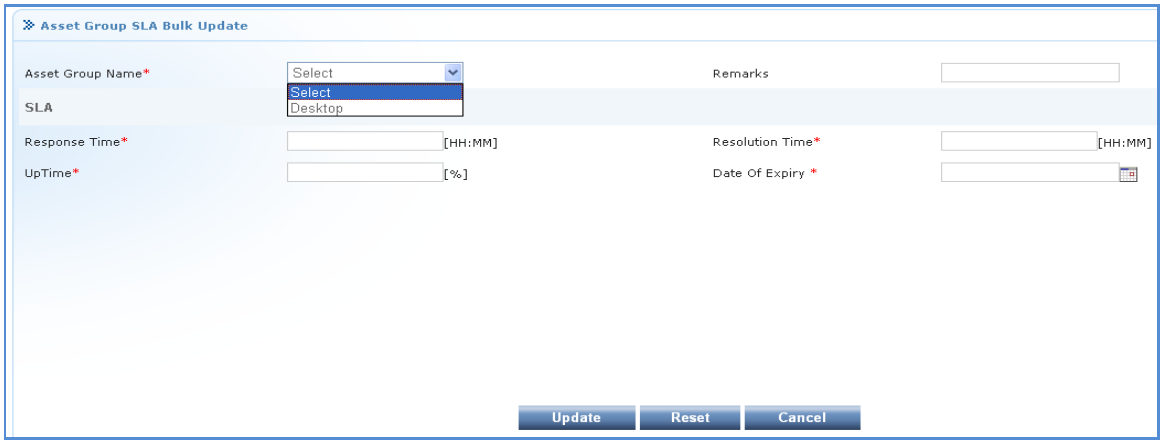
To add a new Asset Group perform the following Tasks



1. Click New
2. Enter the Asset group name for defining the SLA . Example: Server Assets
3. Enable Add SLA
4. Enter the Response Time for SLA- The time frame within which the service has to be attended
5. Enter the Resolution Time for SLA- The time frame within which the problem needs to be solved.
6. Enter the Up Time for the Asset Group
7. Enter From Date
8. Click Save Button to save the Asset group created
9. Click Reset button if you need to reset the field entries

Asset SLA Bulk Update

This option is helpful when an SLA is to be applied to a particular group of assets. All those assets can be selected and applied with a specific SLA.

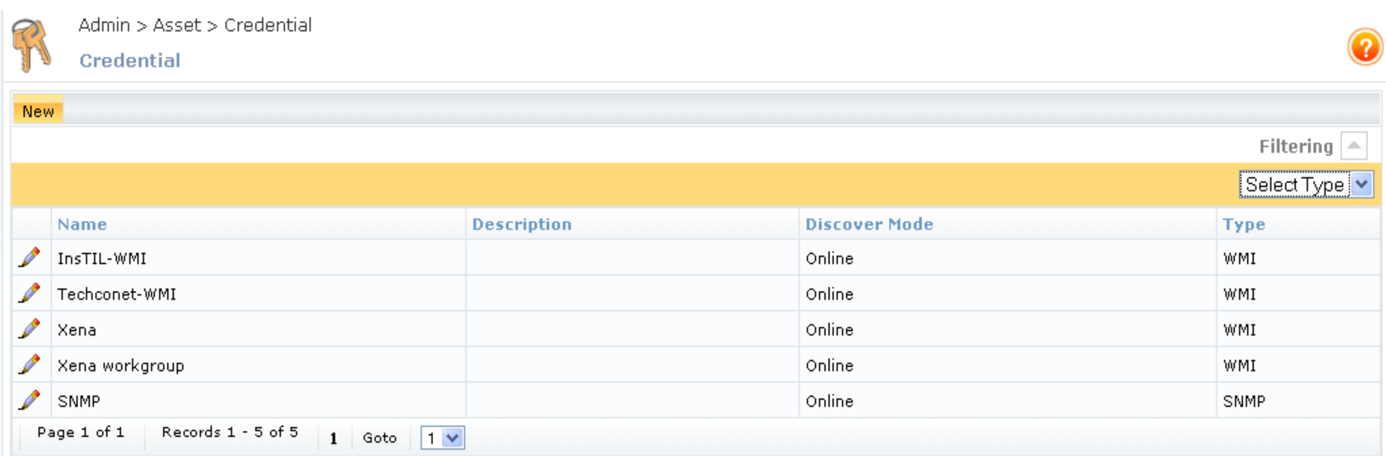


Operation

1. Click on Action and select Asset SLA Bulk update
2. Select the Asset Group name for which the SLA is to be updated
3. Enter the Response Time for SLA- The time frame within which the service has to be attended
4. Enter the Resolution Time for SLA- The time frame within which the problem needs to be solved.
5. Enter the Up Time for the Asset Group
6. Select the Date of Expiry
7. Select the assets for which the SLA applies.
8. Click Save Button to save the SLA updates
9. Click Reset button if you need to reset the field entries

Defining Asset – Credentials

This form is used to create credentials for the purpose of doing auto discovery. There are two types of credentials that are defined a. WMI credential b. SNMP credential



Steps to create SNMP credential

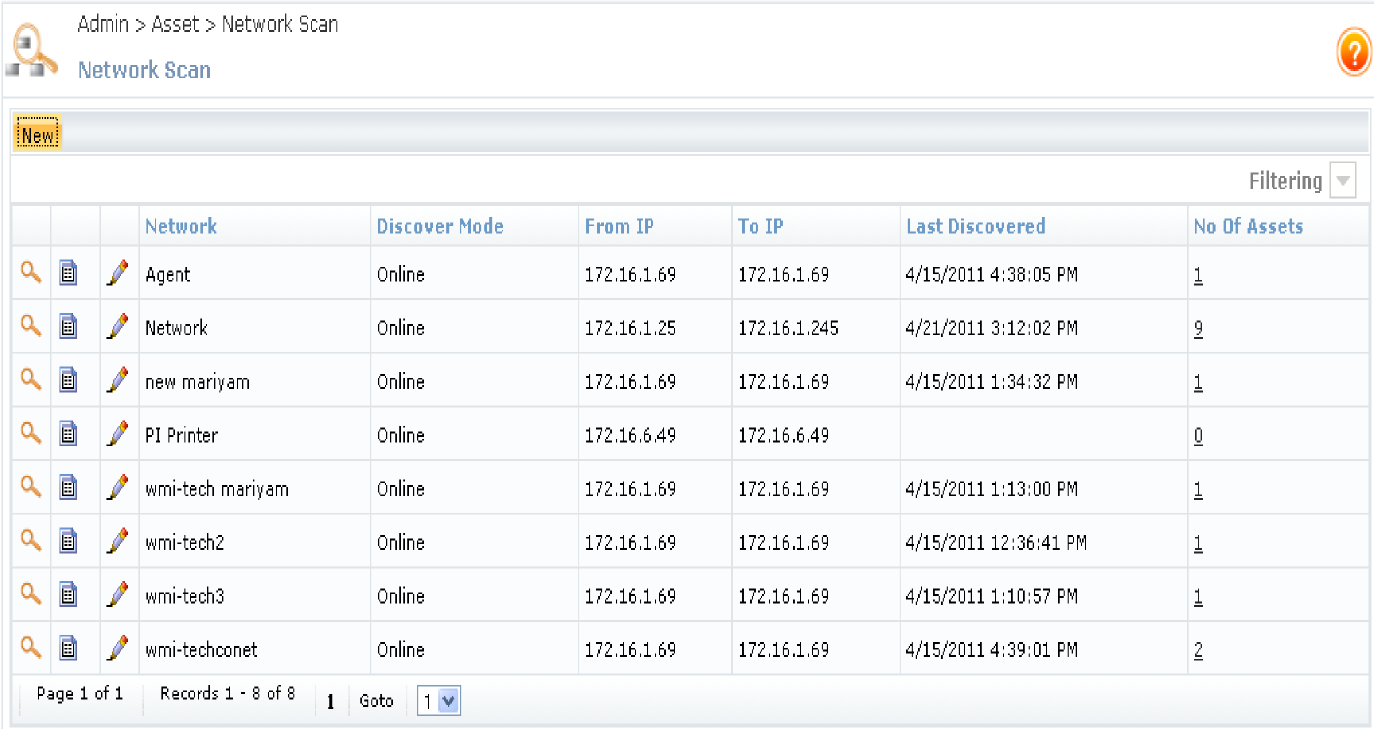
1. Click Add new credential
2. Enter an SNMP credential name
3. Select SNMP
4. Enter the community string value as public
5. Enter the timeout as 2000 (milli seconds)
6. Click Save to save the credential created

Steps to create WMI credential

1. Click Add new credential
2. Enter a WMI credential name
3. Select WMI
4. In WMI the credentials are created through workgroup or domain
5. Click on Domain as credential type and select the domain name from the dropdown list
6. Enter the domain administrator username and password
7. Click Save to save the credential created

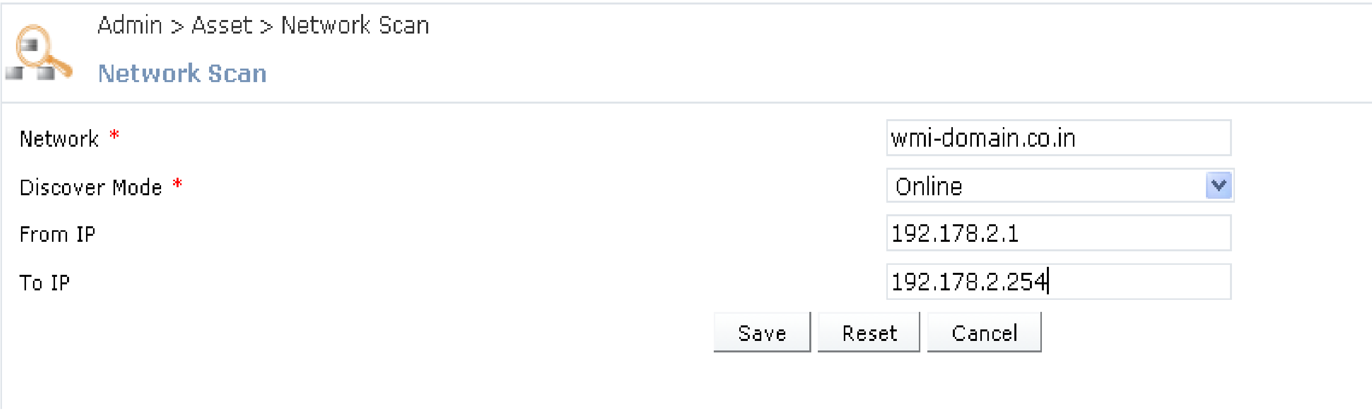
Defining Asset – Network scan

This feature enables the administrator to scan the available networks and discover all the devices with a range of IP's. Both the WMI and SNMP devices that have been discovered can be imported into the application.

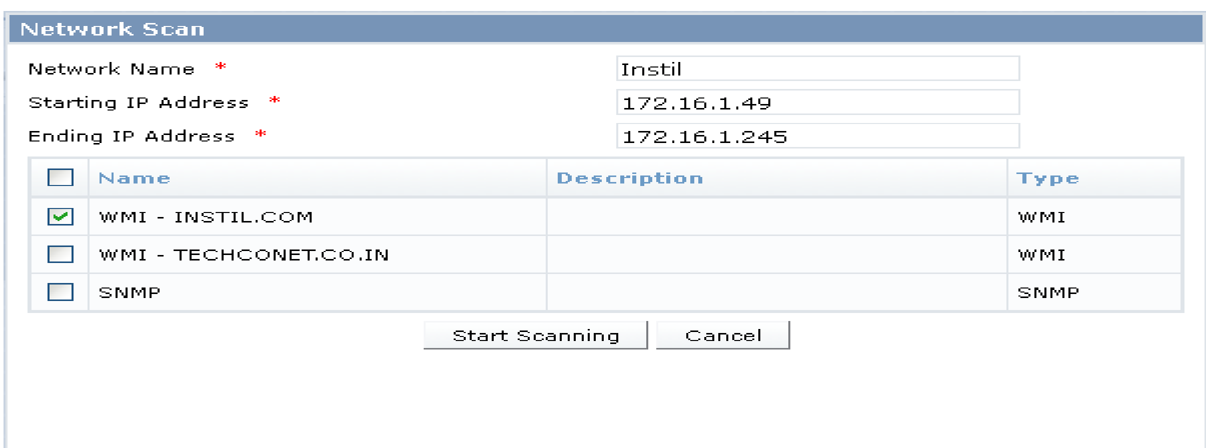


Operation

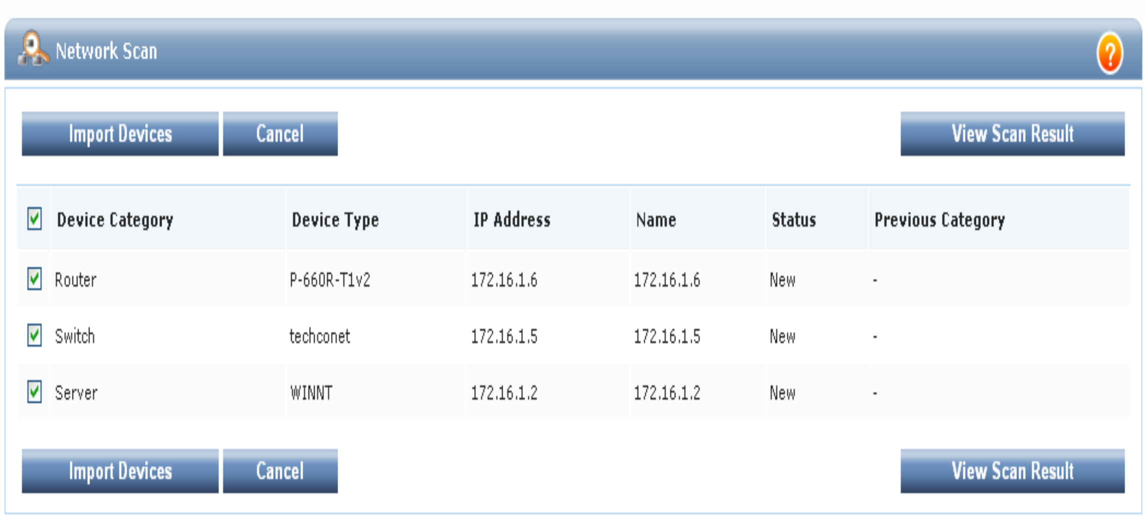
To add a new network perform the following tasks



1. Click New
2. Enter the Network name and select the Discover Mode from dropdown list
3. Enter the range of IP’s within this network.
4. Click Save button to save the record.
5. Click Delete button to delete the record.
6. Click Reset button to reset the entries.
7. Select the Domain and click the Start Scanning button in the below fig



8. Click Import Devices to import the assets into the application.
9. Click Cancel button to terminate the process
10. Click View Scan Result button to get a complete picture of the status for each system in the network.



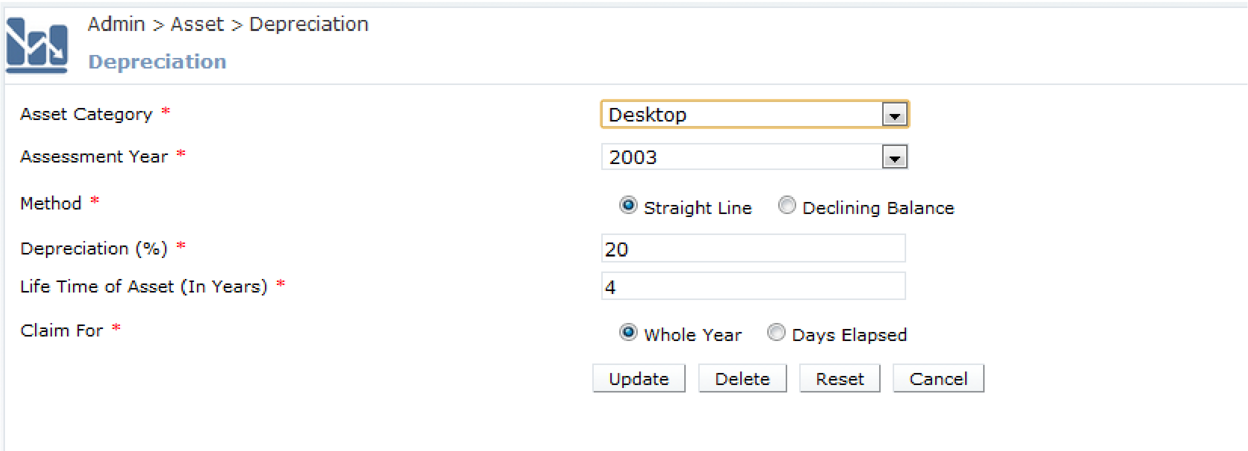
Defining Asset – Depreciation

Depreciable assets are business assets which can be depreciated. That is, the value of the asset is considered as a business expense over the life of the asset. The ability to expense an asset is useful for tax purposes. Depreciable assets include equipment and other tangible assets. Supplies cannot be depreciated because they are considered to be used within a single year and they are expensed during that year.

There are two methods by which the depreciation of an asset can be calculated 1. Straight Line Method 2. Declining Balance Method

Straight Line Method - The simplest and most commonly used depreciation method, straight line depreciation is calculated by taking the purchase or acquisition price of an asset subtracted by the salvage value divided by the total productive years the asset can be reasonably expected to benefit the company.

Declining Balance Method - The reducing balance method of depreciation provides a high annual depreciation charge in the early years of an asset's life but the annual depreciation charge reduces progressively as the asset ages.



Operation

1. Click New
2. Select the Asset category from the dropdown for which the depreciation value is to be defined
3. Select the Assessment year from which the depreciation value to be calculated
4. Select the depreciation method as either Straight line or Declining Balance method
5. Enter the depreciation percentage value
6. Enter the Life Time of Assets in years
7. Select the Claim value to be calculated in terms of Whole year or Days elapsed
8. Click Update so the depreciation value is calculated for the selected Asset Category

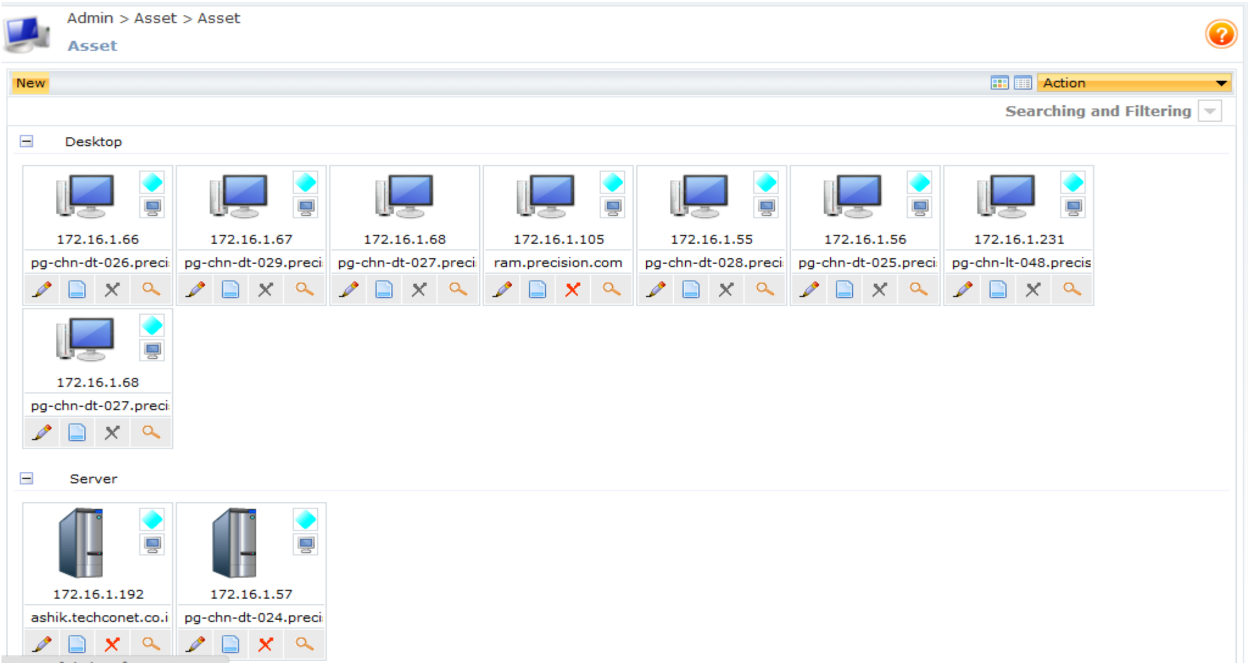
Defining Asset –Asset

The below fig. shows the create option for Asset. Asset Management is generally concerned with the identification and recording of items of corporate infrastructure for financial control purposes. The administrator has to create the Asset for the user so that the user could log in incident for his / her asset. The InsTIL system can also be used for Availability, Performance, Interface Monitoring and Alerts of critical IT Assets.

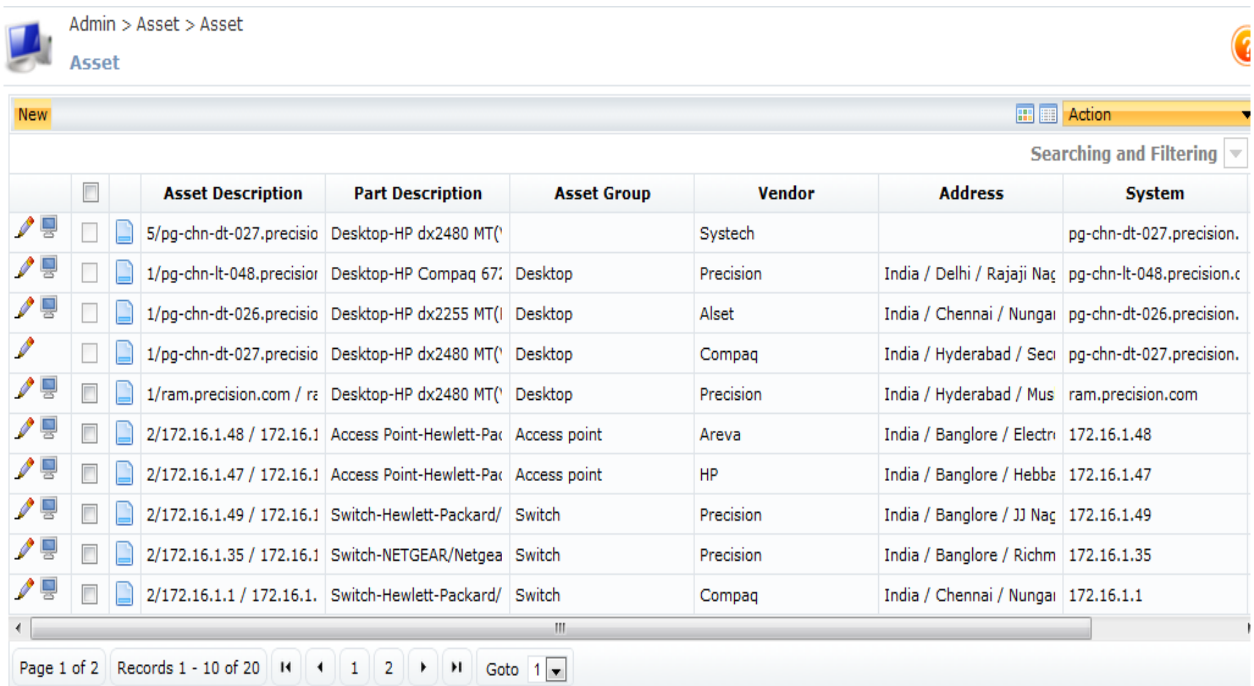
This asset entry forms the basis of all activities done at the service desk and by the technician. The assets configuration detail, location detail, purchase and support details are recorded in this form The AMC bulk update feature is provided for updating the AMC of the assets to warranty. The administrator has the provision to create custom based templates for pulling out information related to the assets. These templates can be created based on the administrator's needs. The screen shown below is self-explanatory as the admin is required to provide information related to the serial number that asset carries. Audit number is something most organization follow, it is a sequential numbering system followed within the organization and the assets are identified by their internal IT department by this number. Select the Family, Part and the Asset group which this asset belong to, from the drop down list. If the asset is a Server or a desktop, specify the OS License number. Similarly, the location where the asset is installed can also be provided as shown in the screen. All the asset entries that are mandatory are marked with an asterisk. The assets are discovered on both Windows and Linux platforms. The administrator can also track the hardware and software changes that have been affected for a particular asset in the form of baselines. The information related to the insurance and depreciation value for each assessment year can be viewed in the administrator menu. The user and assets are linked automatically based on the windows login and this feature can be enabled only for Active directory environment. The assets discovered through network scan will be available in the asset list.

The asset menu has also certain other purpose like a. AMC Bulk Update b. Custom Report c. Import from CSV d. Copy from last entry e. Delete f. Auto link Users and Assets. The Asset menu can be viewed in two forms namely Thumbnail view and Detail view

Thumbnail View



Detailed View

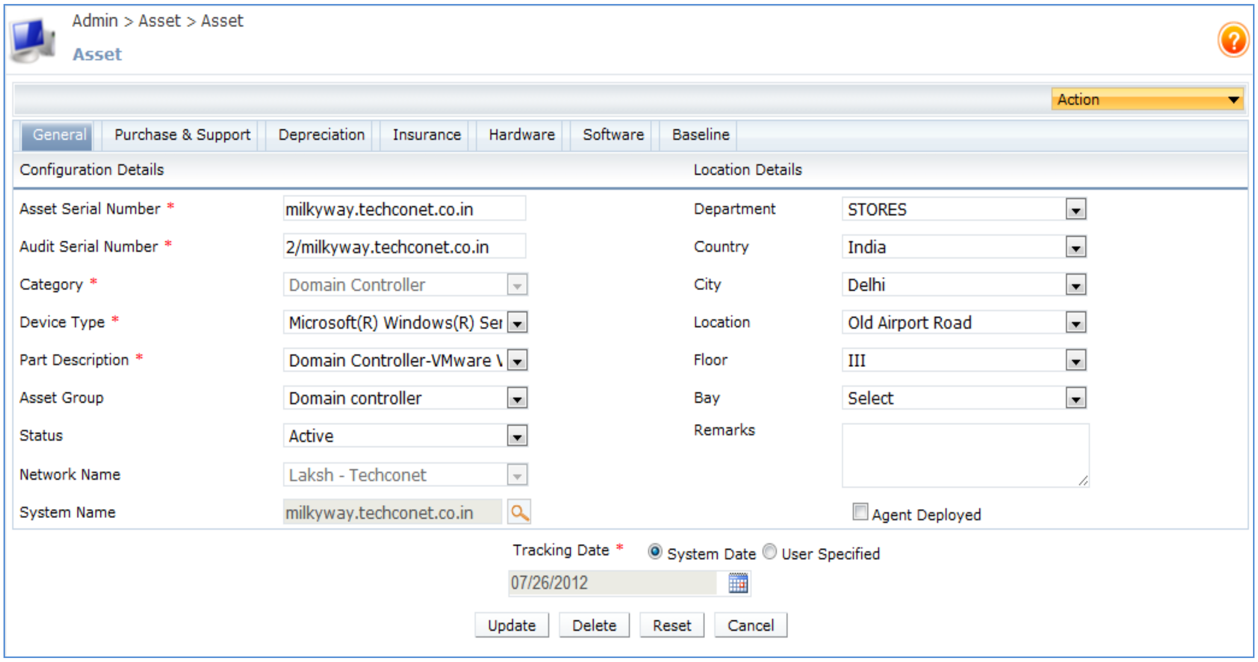


Asset Description	Part Description	Asset Group	Vendor	Address	System
5/pg-chn-dt-027.precisio	Desktop-HP dx2480 MT('		Systech		pg-chn-dt-027.precision.
1/pg-chn-lt-048.precisior	Desktop-HP Compaq 67:	Desktop	Precision	India / Delhi / Rajaji Nag	pg-chn-lt-048.precision.c
1/pg-chn-dt-026.precisio	Desktop-HP dx2255 MT(I	Desktop	Alset	India / Chennai / Nungai	pg-chn-dt-026.precision.
1/pg-chn-dt-027.precisio	Desktop-HP dx2480 MT('	Desktop	Compaq	India / Hyderabad / Seci	pg-chn-dt-027.precision.
1/ram.precision.com / ra	Desktop-HP dx2480 MT('	Desktop	Precision	India / Hyderabad / Mus	ram.precision.com
2/172.16.1.48 / 172.16.1	Access Point-Hewlett-Pac	Access point	Areva	India / Banglore / Electr	172.16.1.48
2/172.16.1.47 / 172.16.1	Access Point-Hewlett-Pac	Access point	HP	India / Banglore / Hebba	172.16.1.47
2/172.16.1.49 / 172.16.1	Switch-Hewlett-Packard/	Switch	Precision	India / Banglore / JJ Nag	172.16.1.49
2/172.16.1.35 / 172.16.1	Switch-NETGEAR/Netgea	Switch	Precision	India / Banglore / Richm	172.16.1.35
2/172.16.1.1 / 172.16.1.	Switch-Hewlett-Packard/	Switch	Compaq	India / Chennai / Nungai	172.16.1.1

Operation

To add a new asset manually perform the following task

General

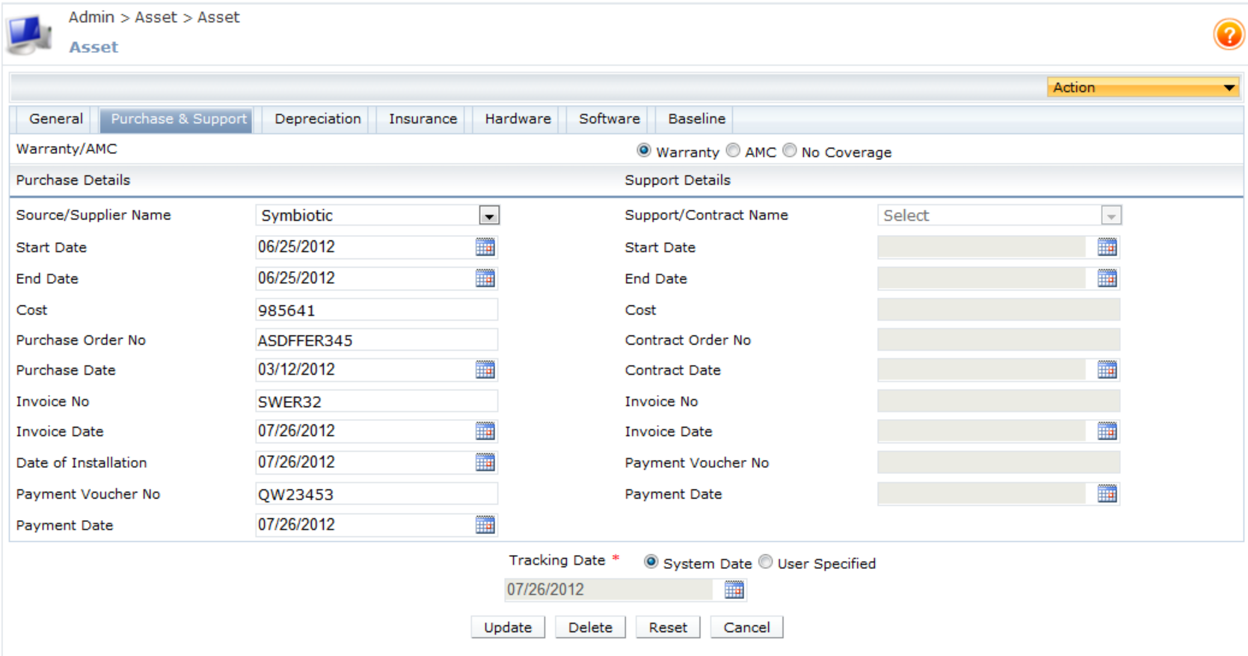


Operation

1. Click New
2. Enter the Asset Serial Number – Asset serial number is the inbuilt serial number of the assets
3. Enter Audit Serial Number.
4. Select the Category name from the dropdown list
5. Enter the Device type which the Asset belongs to.
6. Select the Part description from the dropdown list.
7. Select the Asset Group from the dropdown list
8. Select the status from the dropdown list.
9. Enter the System name –To auto discover the hardware and software components
10. Enter the Network Name from the dropdown list.
11. Enter the location detail of the asset – Country, City, Location, Floor, Bay and Department.

Purchase and Support

The assets purchase and support details are entered in this tab. If the asset is under warranty then, the user is allowed to key in the purchase detail. If the asset is under AMC, then the user is allowed to key in the vendor detail.

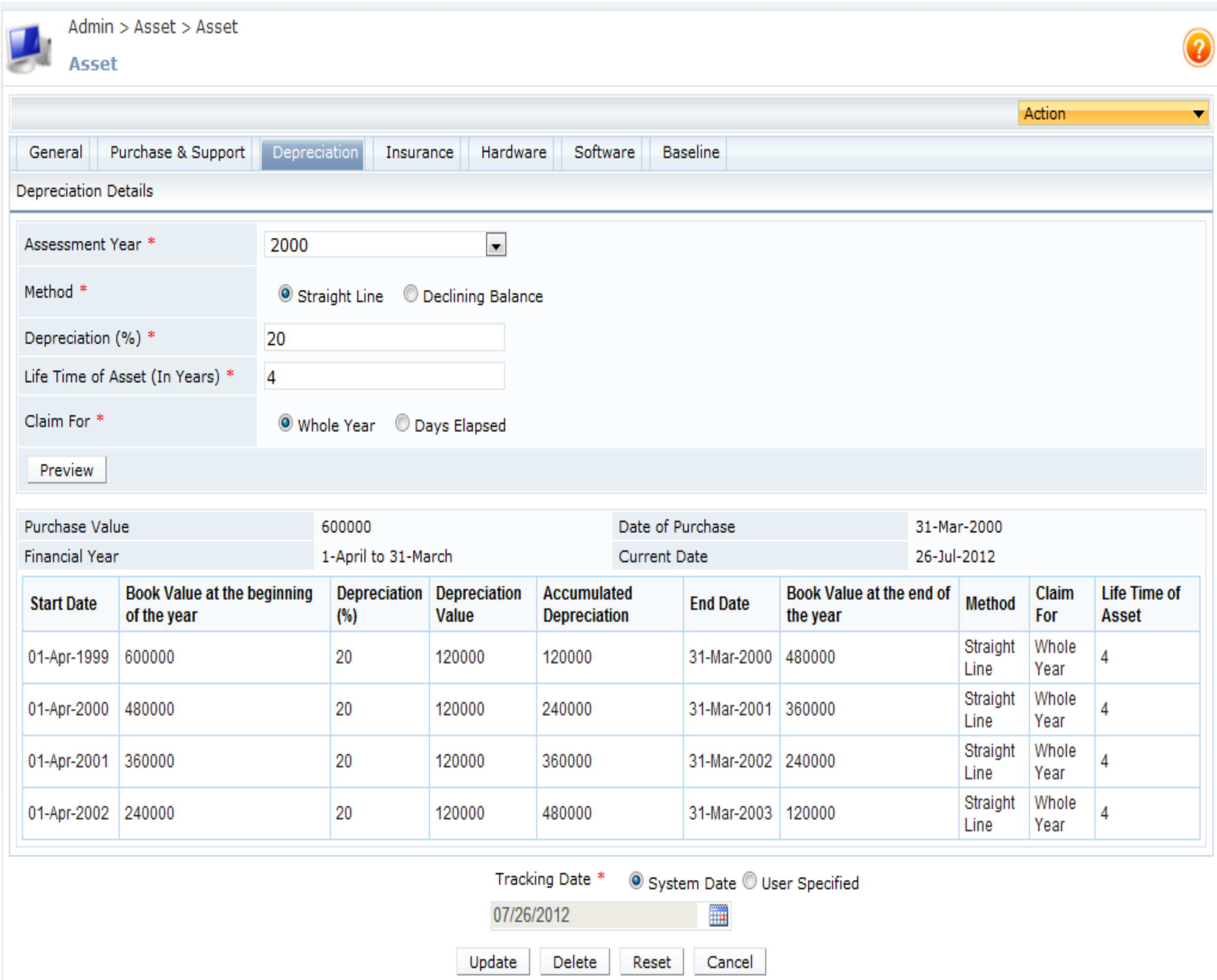


Operation

1. Select Warranty/AMC/No Coverage
2. Enter the purchase detail of the asset like the Source/Supplier name, PO Number, Start date, end date of the warranty period, etc.
3. If AMC, enter the support details like the Support/Contract name, PO number, start date, end date of the AMC period, etc.
4. If No Coverage, both the purchase and support details can be entered.

Depreciation

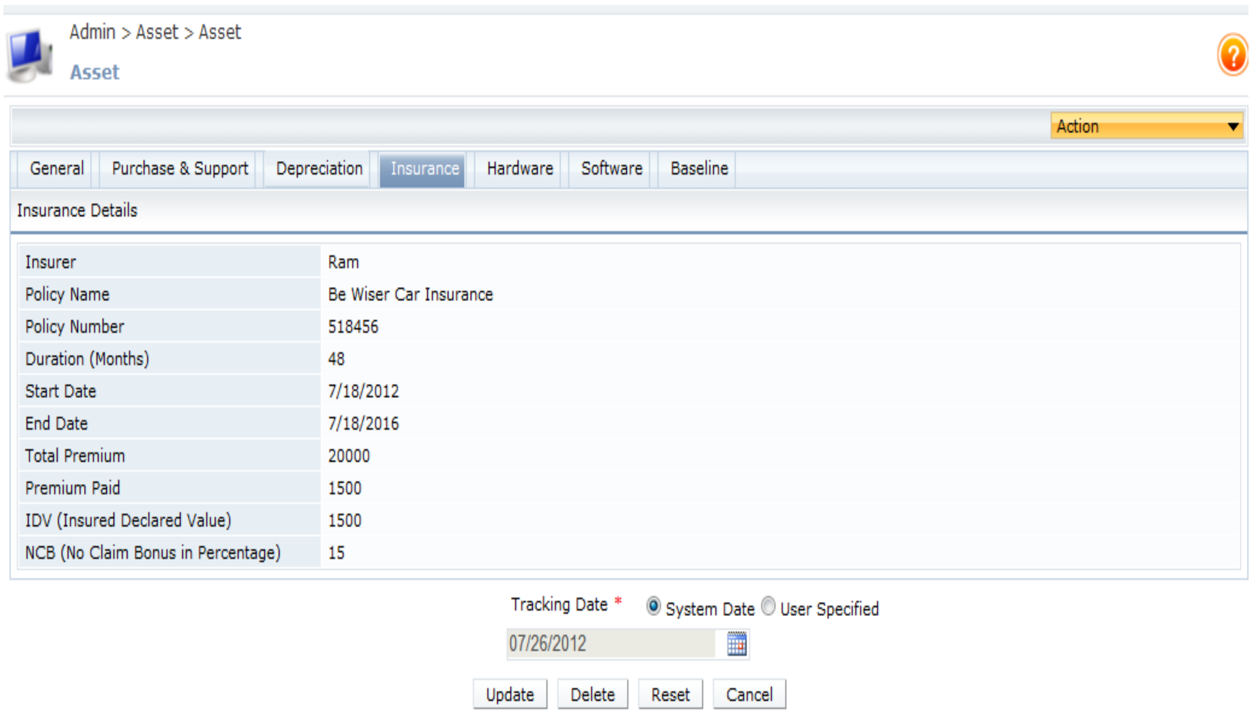
The depreciation value for the entire life time of an asset is automatically calculated and displayed here. The administrator also has the privilege to change the type of depreciation method and find the value for each asset



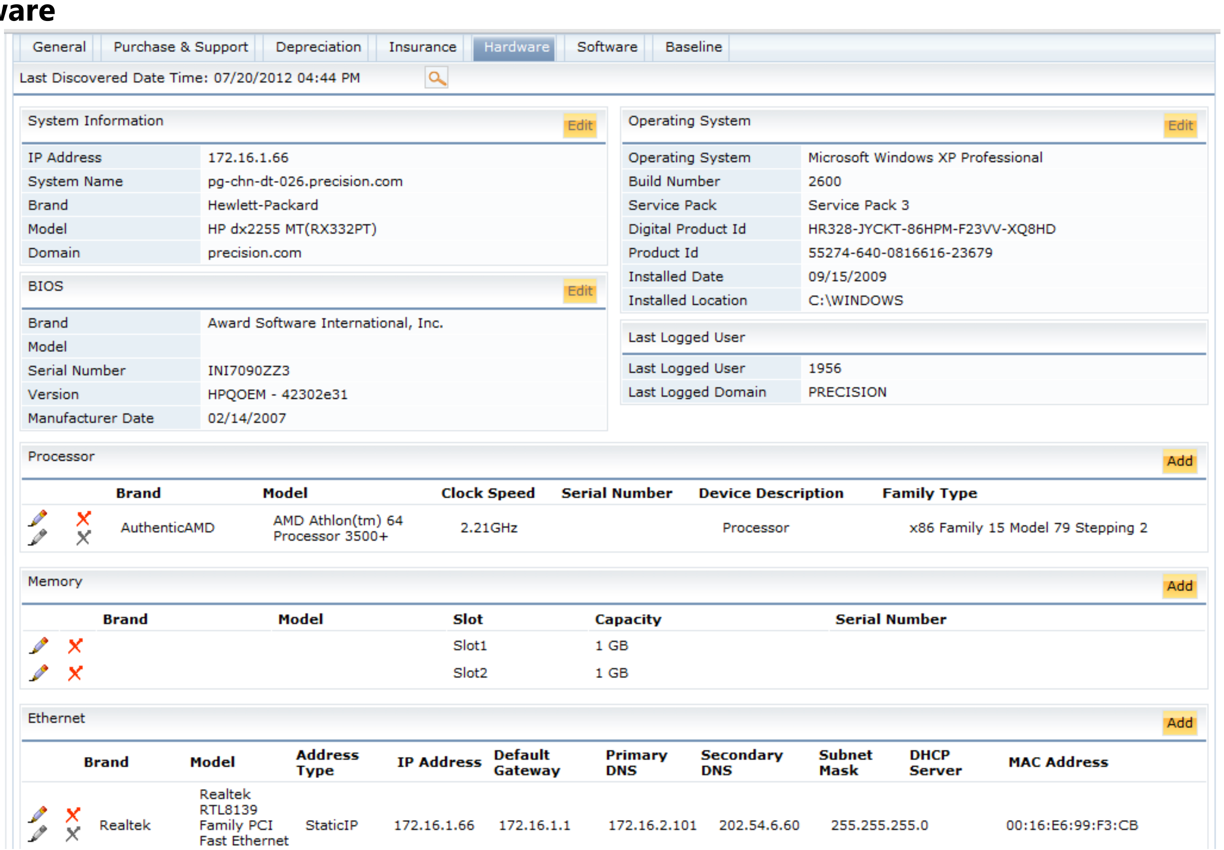
Insurance

The insurance details of each asset can be viewed in the Insurance tab.The system automatically calculates the Insured Declared value and No claim bonus in percentage for the particular asset.

Insured Declared Value (IDV) - Insured Declared Value is the maximum Sum Assured fixed by the insurer which is provided on theft or total loss of the asset.

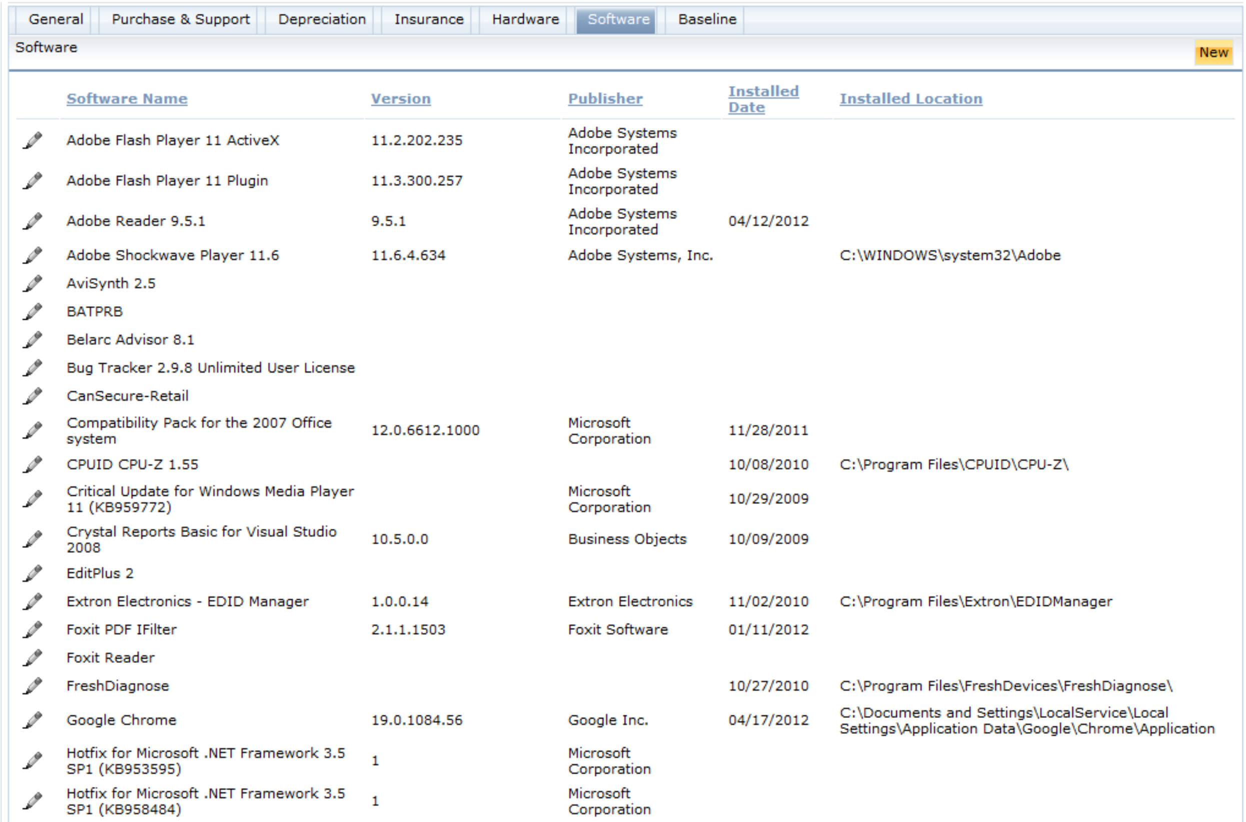

Admin > Asset > Asset
Asset
Action
General
Purchase & Support
Depreciation
Insurance
Hardware
Software
Baseline
Insurance Details
Insurer
Ram
Policy Name
Be Wiser Car Insurance
Policy Number
518456
Duration (Months)
48
Start Date
7/18/2012
End Date
7/18/2016
Total Premium
20000
Premium Paid
1500
IDV (Insured Declared Value)
1500
NCB (No Claim Bonus in Percentage)
15
Tracking Date *
System Date
User Specified
07/26/2012
Update
Delete
Reset
Cancel

Hardware


General
Purchase & Support
Depreciation
Insurance
Hardware
Software
Baseline
Last Discovered Date Time: 07/20/2012 04:44 PM
System Information
Edit
IP Address
172.16.1.66
System Name
pg-chn-dt-026.precision.com
Brand
Hewlett-Packard
Model
HP dx2255 MT(RX332PT)
Domain
precision.com
BIOS
Edit
Brand
Award Software International, Inc.
Model
Serial Number
INI7090ZZ3
Version
HPQOEM - 42302e31
Manufacturer Date
02/14/2007
Operating System
Edit
Operating System
Microsoft Windows XP Professional
Build Number
2600
Service Pack
Service Pack 3
Digital Product Id
HR328-JYCKT-86HPM-F23VV-XQ8HD
Product Id
55274-640-0816616-23679
Installed Date
09/15/2009
Installed Location
C:\WINDOWS
Last Logged User
Last Logged User
1956
Last Logged Domain
PRECISION
Processor
Add
Brand
Model
Clock Speed
Serial Number
Device Description
Family Type
AuthenticAMD
AMD Athlon(tm) 64 Processor 3500+
2.21GHz
Processor
x86 Family 15 Model 79 Stepping 2
Memory
Add
Brand
Model
Slot
Capacity
Serial Number
Slot1
1 GB
Slot2
1 GB
Ethernet
Add
Brand
Model
Address Type
IP Address
Default Gateway
Primary DNS
Secondary DNS
Subnet Mask
DHCP Server
MAC Address
Realtek
Realtek RTL8139 Family PCI Fast Ethernet
StaticIP
172.16.1.66
172.16.1.1
172.16.2.101
202.54.6.60
255.255.255.0
00:16:E6:99:F3:CB

The administrator is given the provision to add component information of the assets like Processor, Memory, Ethernet, Logical drives and Hard disk etc.

Software


General | Purchase & Support | Depreciation | Insurance | Hardware | Software | Baseline

Software

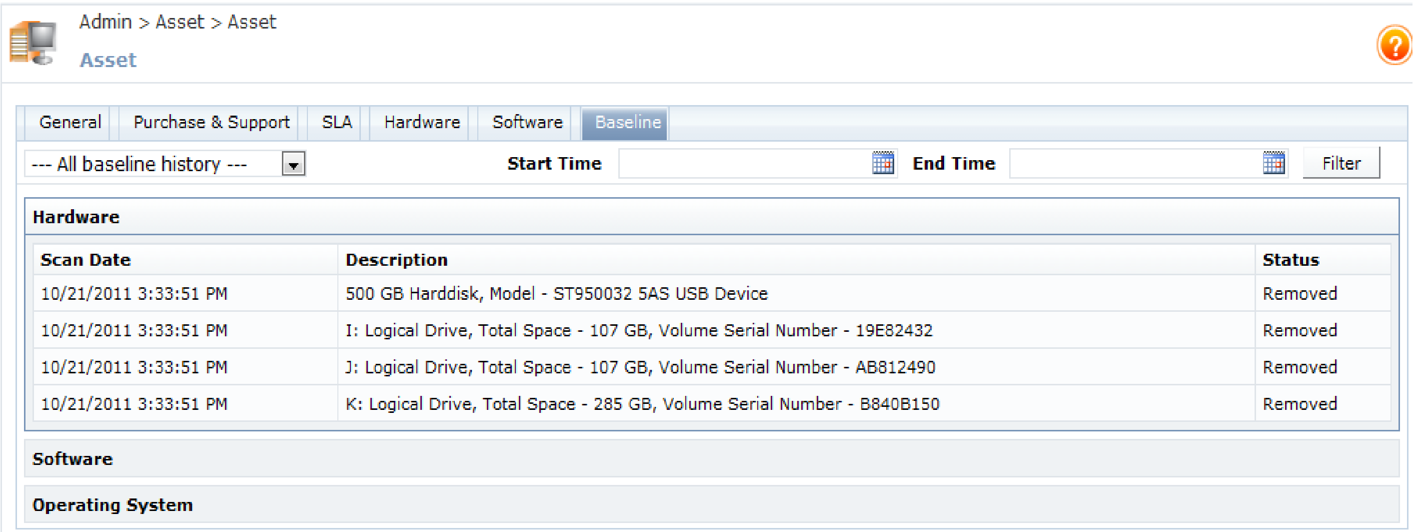
New

Software Name	Version	Publisher	Installed Date	Installed Location
Adobe Flash Player 11 ActiveX	11.2.202.235	Adobe Systems Incorporated		
Adobe Flash Player 11 Plugin	11.3.300.257	Adobe Systems Incorporated		
Adobe Reader 9.5.1	9.5.1	Adobe Systems Incorporated	04/12/2012	
Adobe Shockwave Player 11.6	11.6.4.634	Adobe Systems, Inc.		C:\WINDOWS\system32\Adobe
AviSynth 2.5				
BATPRB				
Belarc Advisor 8.1				
Bug Tracker 2.9.8 Unlimited User License				
CanSecure-Retail				
Compatibility Pack for the 2007 Office system	12.0.6612.1000	Microsoft Corporation	11/28/2011	
CPUID CPU-Z 1.55			10/08/2010	C:\Program Files\CPUID\CPU-Z\
Critical Update for Windows Media Player 11 (KB959772)		Microsoft Corporation	10/29/2009	
Crystal Reports Basic for Visual Studio 2008	10.5.0.0	Business Objects	10/09/2009	
EditPlus 2				
Extron Electronics - EDID Manager	1.0.0.14	Extron Electronics	11/02/2010	C:\Program Files\Extron\EDIDManager
Foxit PDF IFilter	2.1.1.1503	Foxit Software	01/11/2012	
Foxit Reader				
FreshDiagnose			10/27/2010	C:\Program Files\FreshDevices\FreshDiagnose\
Google Chrome	19.0.1084.56	Google Inc.	04/17/2012	C:\Documents and Settings\LocalService\Local Settings\Application Data\Google\Chrome\Application
Hotfix for Microsoft .NET Framework 3.5 SP1 (KB953595)	1	Microsoft Corporation		
Hotfix for Microsoft .NET Framework 3.5 SP1 (KB958484)	1	Microsoft Corporation		

The administrator is given the provision to add software information like Software name, Version, Publisher Name and date of installations etc.

Baseline

The baseline tab indicates information if there is any changes in the hardware and software configuration of the asset. The application sends an alert to the administrator if there are any configuration changes to the assets. This can be enabled in the settings menu of the Administrator.



Monitoring an asset

The parameters that can be monitored for Assets are

Availability Monitoring

Availability Management is a feature of monitoring the Availability status of your Critical Assets. The administrator can manage the status of a device and generate an incident if the device is down. The parameters specified for this feature is standard for all type of devices.

A green Up diamond button indicates the status UP and a red button indicates a down status.

Parameters for Availability Management:

1. Device Status
2. Monitoring Interval
3. No. Of Times to Ping
4. Time to Live
5. Packet Length
6. Time out
7. Automatic Incident Raising

Performance Monitoring

|

A process of collecting and analyzing the data of a device based on its performance. Performance Monitoring enables an administrator to monitor the performance of a device when there is a critical issue on its performance. Based on the information passed through the various parameters returned by the application, the administrator can work on a solution to solve the issues faced by the users on the device. The parameters defined, varies from device to device.

Parameters for Performance Monitoring

Hosts

1. CPU Utilization
2. Memory Utilization
3. Disk Utilization
4. Process Count

Routers

1. CPU Utilization+
2. Memory Used+
3. Memory Free+
4. Big Buffer Hits
5. Big Buffer Misses
6. Big Create Failures
7. Medium Buffer Hits
8. Medium Buffer Misses
9. Small Buffer Misses
10. Temperature+
11. Total Huge Buffer Hits
12. Total Huge Buffer Misses
13. Total Large Buffer Hits
14. Total Large Buffer Misses

Interface Monitoring

Interface monitoring is a process of collecting and analyzing the data from an interface to depict its performance. The Interface Monitoring application enables the administrator to view a list of available interfaces, status condition and access additional information about an interface, such as configuration and performance data.

Parameter's for Interface Monitoring:

The parameters specified for monitoring an interface is same across all the device types. They are;

1. Interface Description
2. Traffic Utilization Graph
3. Error Graph
4. Discard Graph

Alarms

This feature enables the administrator to view and manage the alarms raised by the application for the device selected. The alarms are generated by default if the device is down, invalid parameters defined and also based on the thresholds defined.

Asset Dashboard

Defining Availing parameters for an asset

Device Status:
The status is shown automatically by the application based on the reachability of the device. A green diamond button indicates the status UP and a red button indicates a down status

Monitoring interval:
This option can be set in minutes to enable the application to monitor the device. Based on the value set, the application would ping the device to check the availability.

No. of Times to Ping:
This option can be set to enable the application to ping the device for its availability. By default the value is set to 1.

Time to Live:
The TTL field is set by the sender of the packet, and reduced by every host on the route to its destination. If the TTL field reaches zero before the packet arrives at its destination,

then the packet is discarded and an ICMP error datagram (11 - Time Exceeded) is sent back to the sender. The purpose of the TTL field is to avoid a situation in which an undeliverable packet keeps circulating on the network. In theory, time to live is measured in seconds, although every host that passes the datagram must reduce the TTL by at least one unit. Enter the Time-to-Live value; else the default is set to 50.

Packet Length:

Enter the packet length in bytes, the default is set to 32.

Time out Milliseconds:

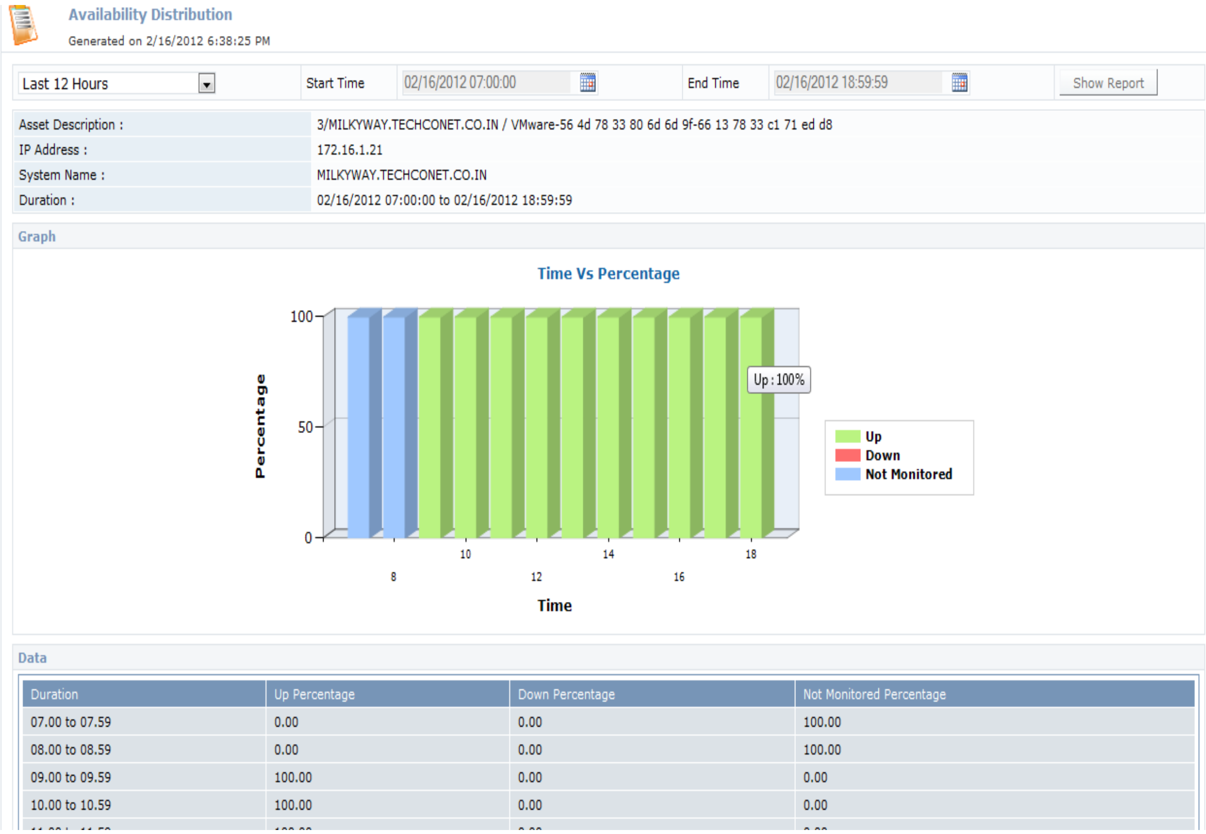
Enter the Time out value for a packet, the default is set to 200.

Action:

If any of the parameters like TTL, Packet length and time out is reached, there are options to trigger like

a. Raise an Incident – Automatically raises an Incident with the Service Desk
b. Raise an Incident & Un-Manage the device - Automatically raises an Incident with the Service Desk and device will not be monitored
c. None - No actions will be performed

Availability Graph



The Availability graph depicts the status of the Assets or devices available in the CMDB. The Availability Distribution bar graph represents 3 basic status information of Assets viz.

Not Monitored

This status indicates in blue, that the Asset is not reachable or set as Unmanaged.

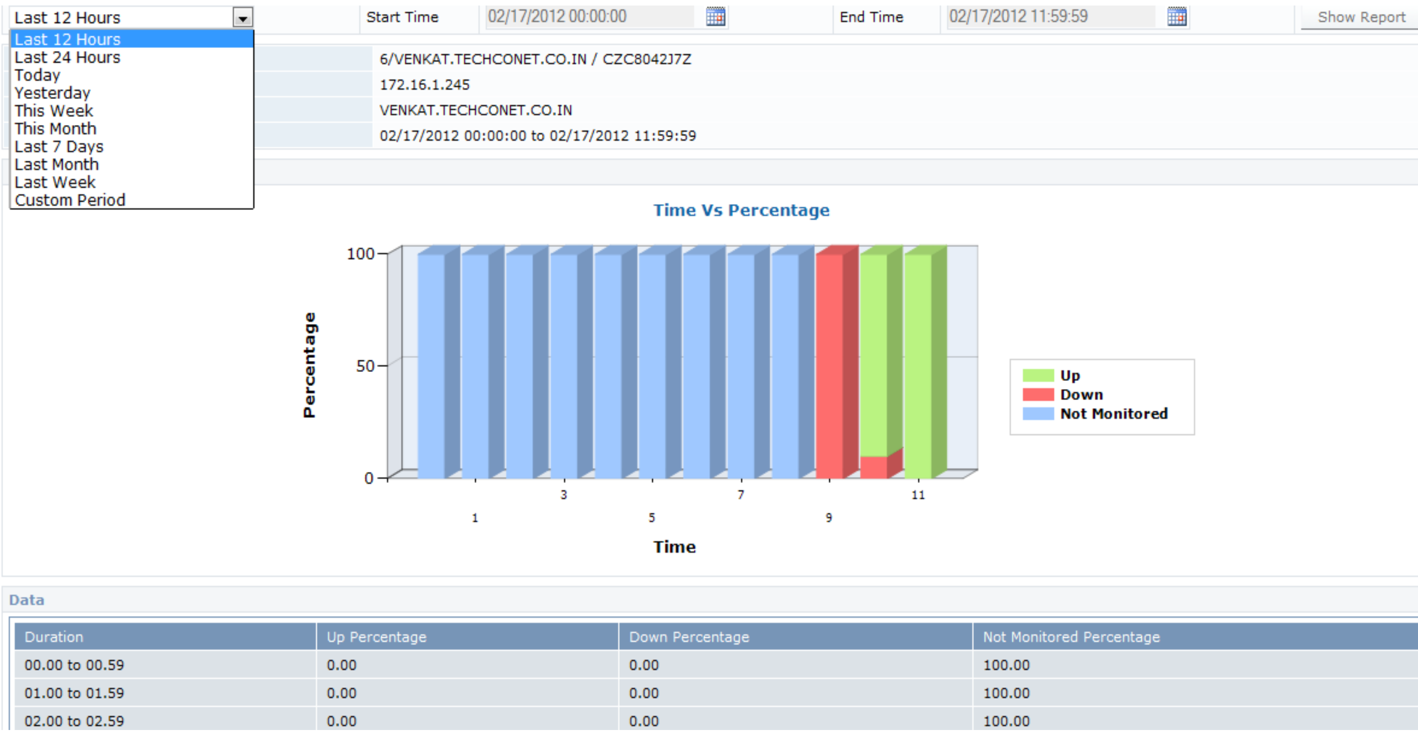
Up

This status indicates in green, that the device is monitored and UP.

Down

This status indicates in Red, that the device is monitored and down.

The availability graph can be viewed for various time duration like Last 12 Hours, Last 24 Hours, Today and also for a custom period of time. Based on the selections the graph is depicted.



Performance Parameters

The performance parameter manages and monitors the performance attribute of a Device. The administrator can set the various parameters available in the application, to monitor the performance of a device. This parameter varies from device to device. The various master parameters available in the application are

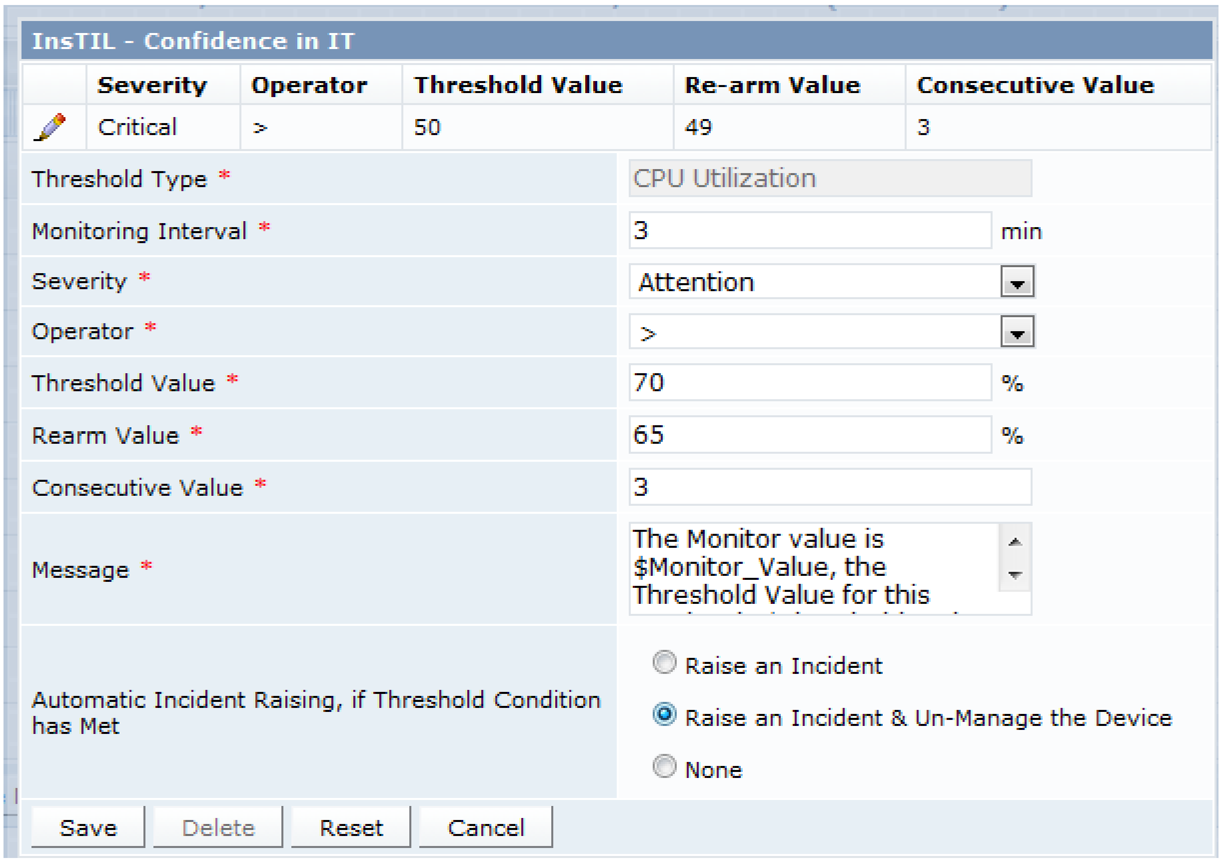
a. CPU Utilization
b. Memory Utilization
c. Processor Utilization
d. Process count
e. Logical Drives

For illustration, let us consider the CPU Utilization parameter for a desktop device.

a. CPU Utilization :

Whenever a device is performing an operation over an interface to the rest of the device, it uses some of the system's resources. One of the more critical of these resources is how much CPU time is required for the operation. This is called the **CPU utilization**. CPU utilization is important because the higher the percentage of the CPU used by the operation, the less power the CPU can devote to other tasks. When multitasking, a high CPU utilization can cause slowdowns in other tasks when doing large data transfers. By default no Threshold value is been set for any of the performance parameter. The administrator can set the threshold values for the CPU Utilization parameter and thereby monitor its performance. To set the parameters do the following;

Click on the button



1. Threshold Type - The threshold type is set automatically based on the parameters chosen. For E.g. CPU Utilization, Memory Utilization etc.

2. Monitoring interval - The monitor interval is defined in minutes and triggers the application to query the device based on the value set. The default is set to 3 minutes.

3. Severity - Select any one of the Severity parameters Attention, Trouble or Critical. This is a pre-defined value and cannot be appended or editable.

4. Operator - Select the operator value “> or <”. If the value is set as “>”, the application will raise an alarm, if the threshold value increases beyond the threshold value set.

5. Threshold - Enter the Threshold value for the CPU Utilization parameter. A threshold value can be specified for each monitored metric. It is used to determine the point at which the network operator should be alerted to a problem.

6. Rearm Value - Enter the Rearm Value. A rearm value enables the monitor to generate a cancelling event when the metric has returned to an acceptable value. This helps prevent multiple events from being generated for the same problem.

7. Consecutive Value- Enter Consecutive value between1 to 10. This value is set to enable the monitor to check for a consecutive occurrence of a threshold based on the value defined and generate an alarm.

8. Message - Enter your Message content for an Alarm message. The basic function of this feature is to trigger an alarm message whenever the application detects a override in the threshold defined. During such process, the application will raise a default alarm message containing the Monitor value detected and the threshold value defined. The administrator can rephrase the message before and after the content mentioned within the “$” symbol, as the application would replace the real-time numerical value after the “$” symbol.

9. Automatic Incident Raising, if the Threshold Condition is met - This administrator can select any one of these option to trigger an automate trouble ticket when a device crosses the threshold condition. Three options are available to be set, they are;

a. Raise an incident
b. Raise an Incident and unmanage the device
c. None, take no action

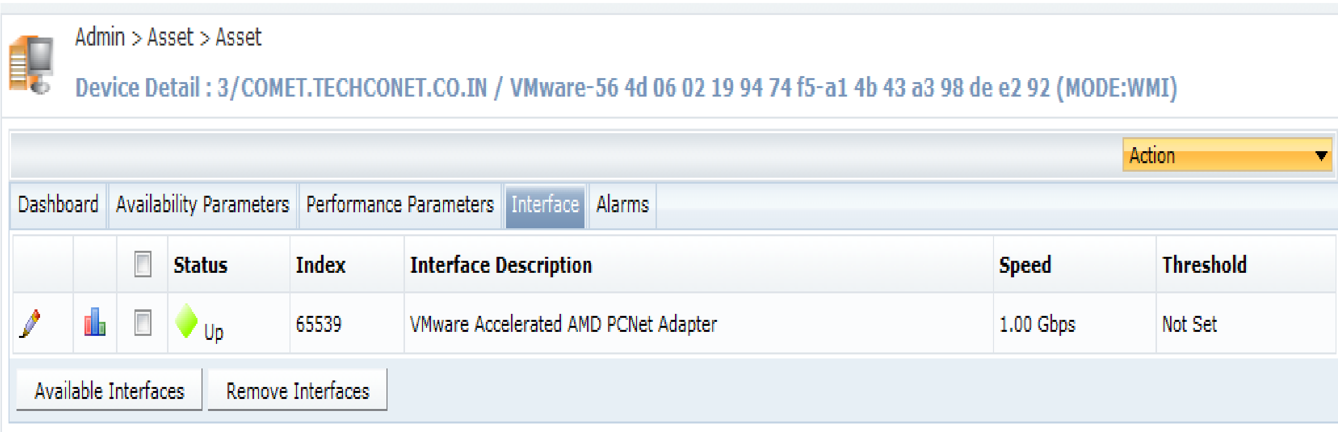
1. Click on Save to submit the changes
2. Click on Reset to clear the values defined

3. To delete a record click on  button and click on delete to remove the record

Note: The similar configuration process implies to all other parameters available for an asset

Interface Parameters

The interface feature lists all the interfaces available in the device to be monitored. For the application to import the interface details of the device, SNMP need to be installed on the device and the port has to be opened and given a read access minimum. By default, on selecting the interface menu, the application would display an empty dashboard shown as “No Records Found”. To add an interface, Click on Available Interfaces. This would list all the available interfaces in the device. Select the check box and click on “Add Interfaces” for the selected interfaces to be monitored

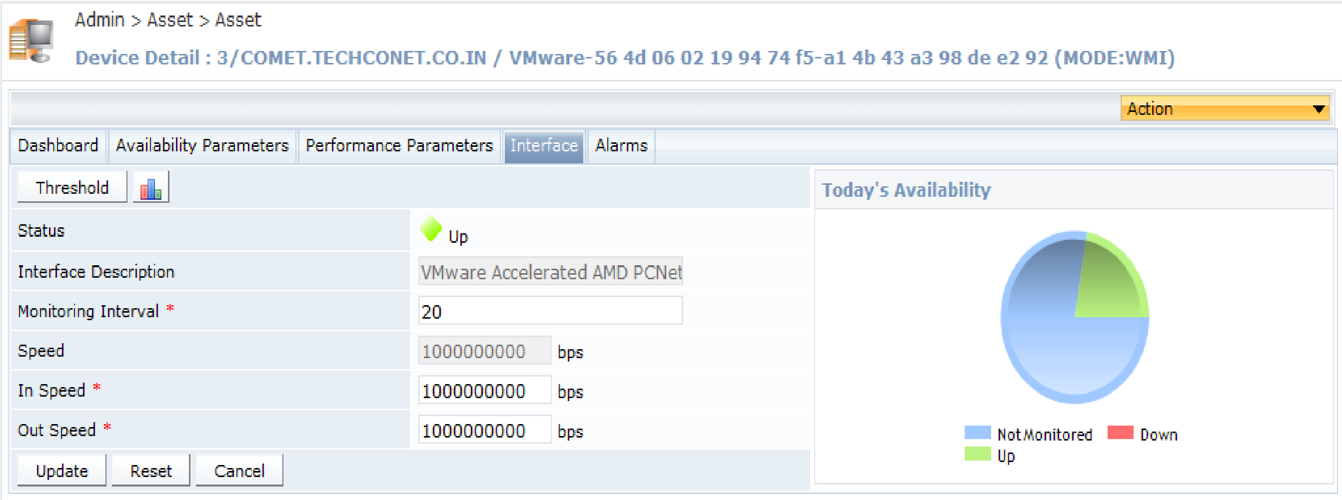


For illustration, let us configure the threshold for any one of the Interface available for a device

The parameters displayed in grey are non-editable and the administrator can re-assign the values ss for the mandatory parameters marked as “*”. They are

Monitoring Interval

This parameter enables application to monitor the device every 15 minutes, which is set as default. The administrator can change value according to his need and requirement.



In Speed

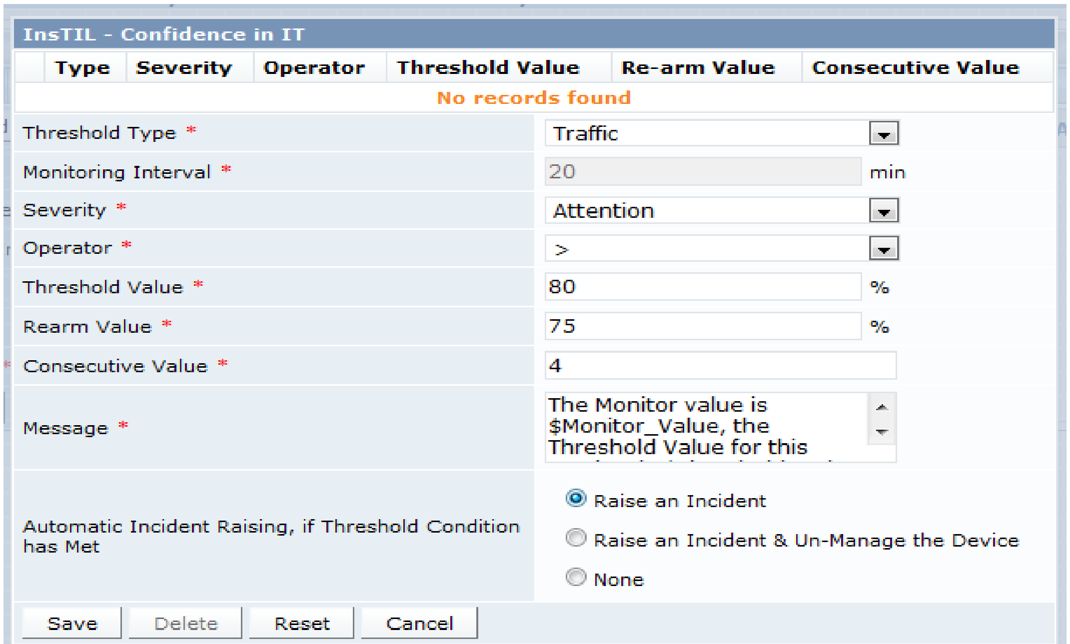
This parameter specifies the maximum inbound speed of the interface. If the value specified in the device configuration is changed, the value gets updated in the application when the device is re-discovered through a manual or a scheduled auto discovery feature. The administrator can also edit the values manually in the interface description.

Out Speed

This parameter specifies the maximum outbound transfer speed of the interface. If the value specified in the interface setting of the device is changed, the value gets updated in the application when the device is re-discovered through a manual or a scheduled auto discovery feature. The administrator can also edit the values manually in the interface description.

Defining Threshold for Interface parameter –

1. Select any one interface parameter for the device
2. Click on the Threshold tab and select  icon



3. Threshold Type - The threshold type can be defined for the following actions like Traffic, Error and Discard

4. Monitoring interval - The monitor interval is defined in minutes and triggers the application to query the device based on the value set. The default is set to 20 mins.

5. Severity - Select any one of the Severity parameters Attention, Trouble or Critical. This is a pre-defined value and cannot be appended or editable.

6. Operator - Select the operator value "> or <". If the value is set as ">", the application will raise an alarm, if the threshold value increases beyond the threshold value set.

7. Threshold - Enter the Threshold value for the CPU Utilization parameter. A threshold value can be specified for each monitored metric. It is used to determine the point at which the network operator should be alerted to a problem.

8. Rearm Value - Enter the Rearm Value. A rearm value enables the monitor to generate a cancelling event when the metric has returned to an acceptable value. This helps prevent multiple events from being generated for the same problem.

9. Consecutive Value- Enter Consecutive value between 1 to 10. This value is set to enable the monitor to check for a consecutive occurrence of a threshold based on the value defined and generate an alarm.

10. Message - Enter your Message content for an Alarm message. The basic function of this feature is to trigger an alarm message whenever the application detects a override in the threshold defined. During such process, the application will raise a default alarm message containing the Monitor value detected and the threshold value defined. The administrator can rephrase the message before and after the content mentioned within the "$" symbol, as the application would replace the real-time numerical value after the "$" symbol.

11. Automatic Incident Raising, if the Threshold Condition is met - This administrator can select any one of these option to trigger an automate trouble ticket when a device crosses the threshold condition. Three options are available to be set, they are;

   i. Raise an incident
   ii. Raise an Incident and Un-Manage the device
   iii. None, take no action

12. Click on Save to submit the changes

13. Click on Reset to clear the values defined

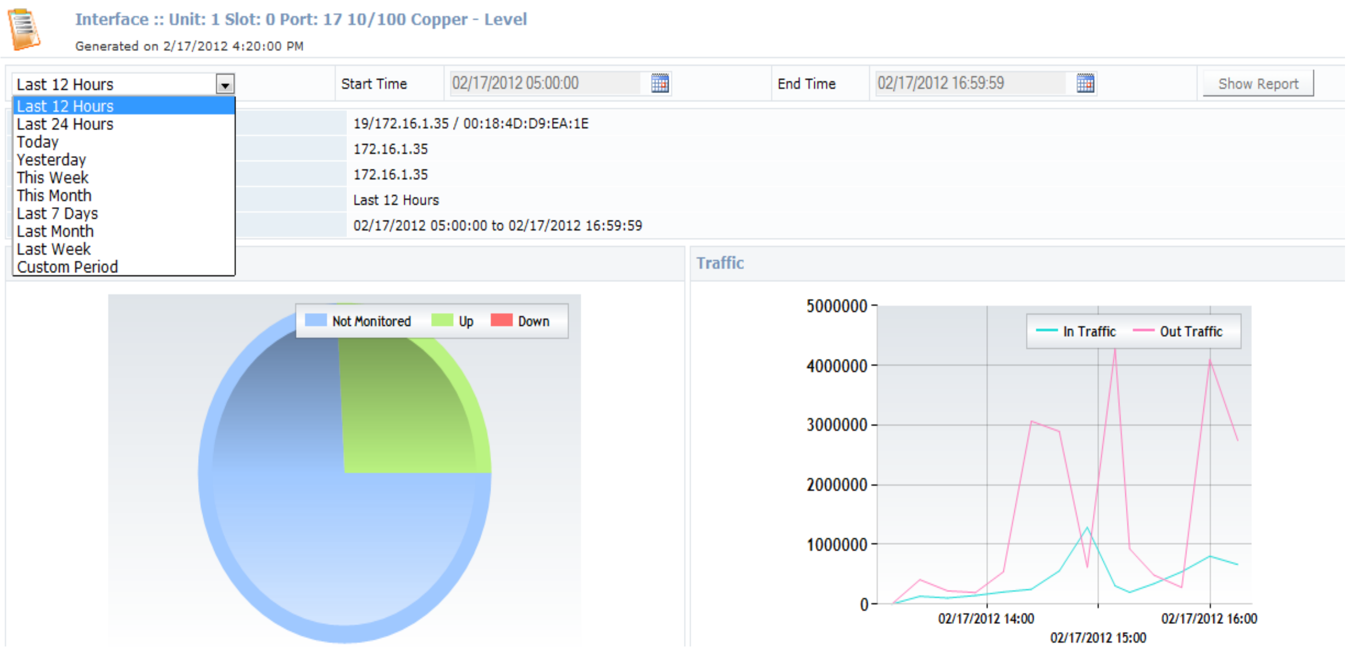
14. To delete a record click on  button and click on delete to remove the record

Note: The similar configuration process implies to all other interface parameters available for an asset

Utilization Graph –

The traffic utilization, Errors and Discards graph for an interface parameter can be viewed for a particular device

Traffic Graph - The traffic graph lets you view the graph in terms of value for inbound traffic, Outbound Traffic & Total speed. We can see traffic graphs for different time periods by choosing the appropriate values from the Filtering options Box. The default graph is for the "Last 12 Hours". The table with the graph shows the legend, along with total, maximum, minimum, and average traffic values for this interface for the selected time period.

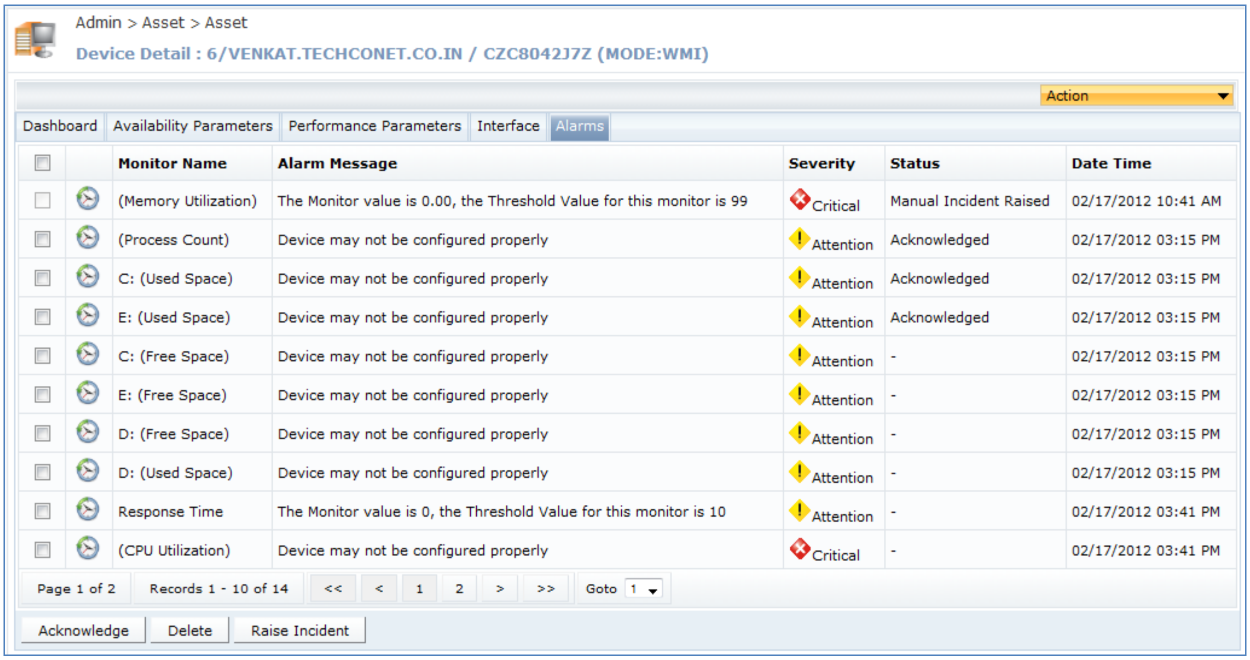


Error Graph - The Error Graph depicts the no. of errors or mishandled packets transmitted through the interface at a point of time. It's measured in packets per second. Based on the selection criteria the graph varies.

Discard Graph - During the transmission of a Packet or datagram through an interface, packets are transmitted to intended hosts after a long delay and by the time the packet reaches the destination, it would be too late to be accepted and treated as a Discard packet. The administrator is enabled to monitor such transmission errors and create a threshold alert to avoid any network choking or congestion. The Discard Graph depicts the maximum or minimum of such discard's monitored in the interface

Alarms

This feature enables the administrator to view and manage the alarms raised by the application for the device selected. The alarms are generated by default if the device is down, invalid parameters defined and also based on the thresholds defined. For example, when no threshold alarms are defined for an interface and if the device is found to be down, the thresholder would raise an alarm as shown below

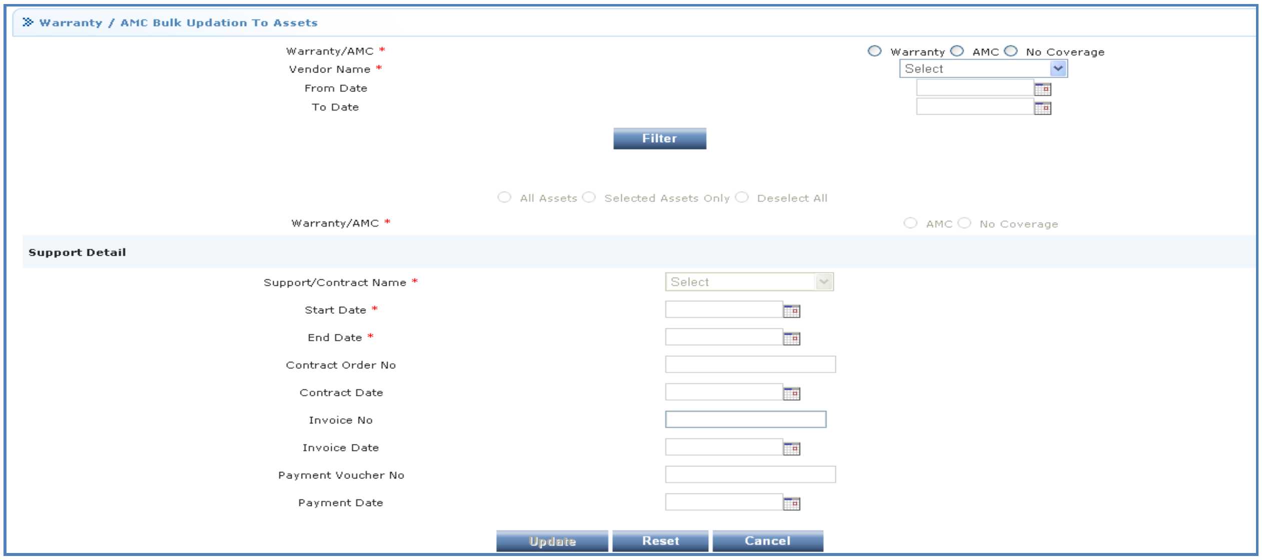


Monitor Name	Alarm Message	Severity	Status	Date Time
(Memory Utilization)	The Monitor value is 0.00, the Threshold Value for this monitor is 99	Critical	Manual Incident Raised	02/17/2012 10:41 AM
(Process Count)	Device may not be configured properly	Attention	Acknowledged	02/17/2012 03:15 PM
C: (Used Space)	Device may not be configured properly	Attention	Acknowledged	02/17/2012 03:15 PM
E: (Used Space)	Device may not be configured properly	Attention	Acknowledged	02/17/2012 03:15 PM
C: (Free Space)	Device may not be configured properly	Attention	-	02/17/2012 03:15 PM
E: (Free Space)	Device may not be configured properly	Attention	-	02/17/2012 03:15 PM
D: (Free Space)	Device may not be configured properly	Attention	-	02/17/2012 03:15 PM
D: (Used Space)	Device may not be configured properly	Attention	-	02/17/2012 03:15 PM
Response Time	The Monitor value is 0, the Threshold Value for this monitor is 10	Attention	-	02/17/2012 03:41 PM
(CPU Utilization)	Device may not be configured properly	Critical	-	02/17/2012 03:41 PM

The administrator can choose any of the alarms displayed in the grid and perform the following action a. Acknowledge b. Delete c. Raise an Incident

Action → AMC Bulk Update

InsTIL also provides the facility of updating the Annual Maintenance Contract detail of all the assets in bulk. This eliminates the work of updating the Annual Maintenance Contract detail done asset by asset in the normal course.

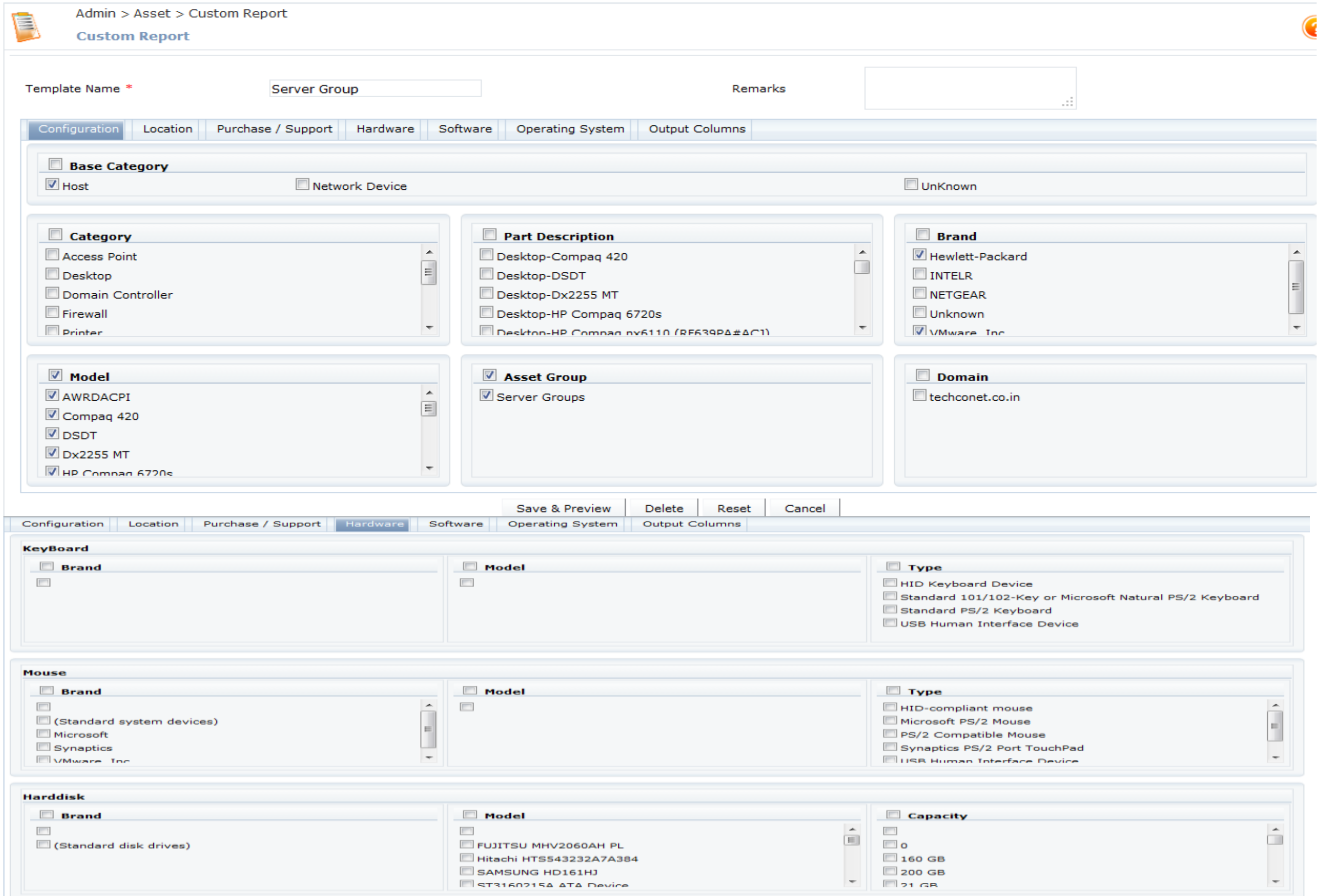


Operation

1. Click AMC Bulk update
2. If the administrator wants to update the assets from Warranty to AMC
3. Select Warranty and choose the Vendor name
4. Click Filter
5. All the Assets of the selected vendor name which is in warranty period is displayed
6. Click AMC and fill the Support details for the asset
7. Click update button to update the changes performed

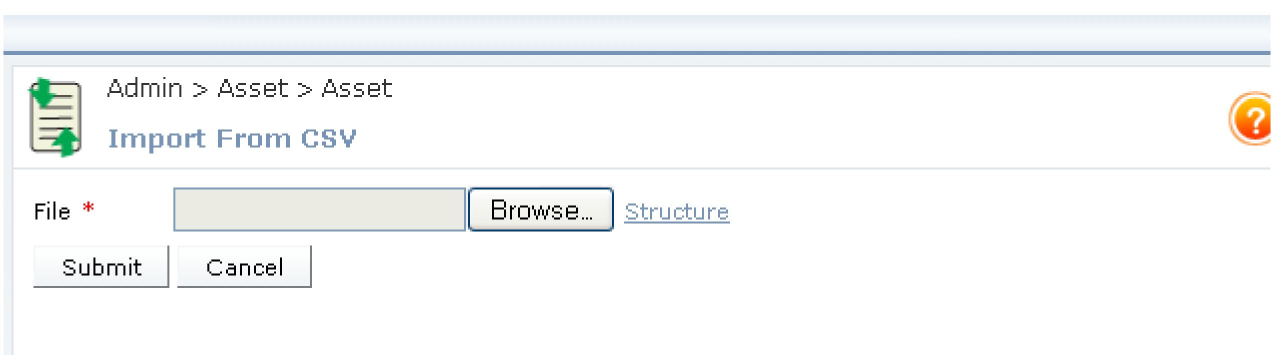
Action → Custom Report

Custom report is enabled for the administrator to generate his own reports based on various filter types like Configuration, Location, Purchase/ Support, Hardware, Software and Operating system. The output columns can also be designed by the administrator. This custom based report can be hence converted to Excel or Word format with the desired results. The snapshots of few filtering types are shown below.



Action → Import from CSV

The asset information can be keyed in a excel sheet and the file can be imported to the database so that using a single step assets can be imported in a bulk manner. The structure can be obtained by clicking the structure link which is available in the Import from CSV link. During the process of import if there is an incorrect entry in one particular field, the field is highlighted and provision is provided to correct the entry.

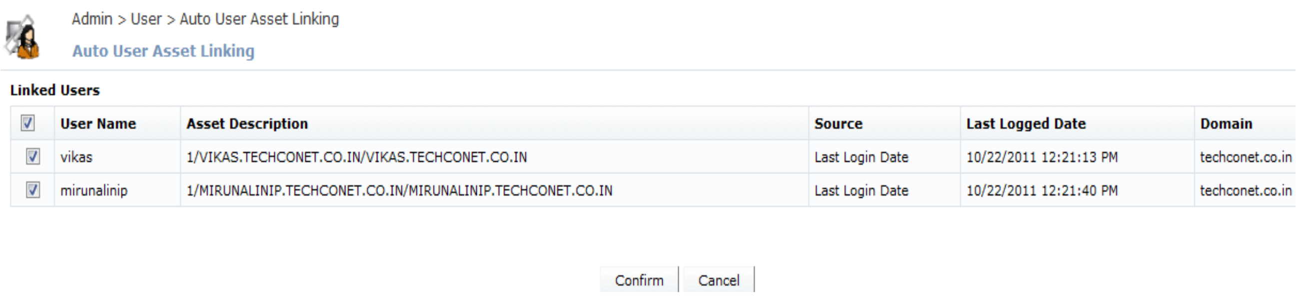


Action →Copy from last entry

This feature allows asset entries to be copied from the previous entry so it reduces the workload if assets are to be added manually instead of using Network Scan or importing from an Excel

Action → Auto link Users and Assets

This option is enabled for the administrator to link the users with their assets automatically. This process works on basis of the last windows credentials used to login to assets. The system performs a scan and brings out the users login information from the asset registry and links the user to that particular asset. The list below shows the user logged in to the assets at that discovered point of time.

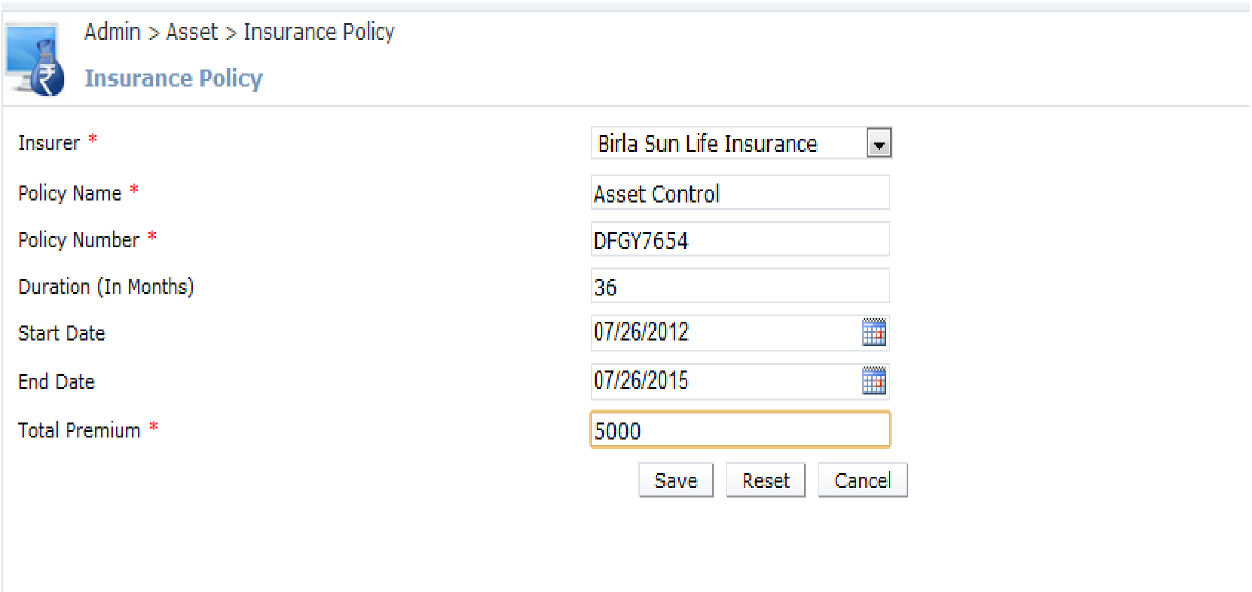


Action → Delete

This option is provided for the administrator to delete the asset entry from the asset list.

Insurance Policy

The various insurance policy registered with the Insurer can be created here. The information pertaining to the Policies are recorded in the Insurance policy master.



Operation

1. Click New
2. Select the Insurer name from the dropdown list for whom the policies are to be created
3. Enter the policy name and policy number
4. Enter the policy duration in months
5. Select the policy Start date and End date from the date time picker
6. Enter the total premium amount for the policy undertaken
7. Click Save to save the entry created

4.3 Software Distribution:

The software distribution feature automates the distribution of programs to client Pc's. These programs run on the client computers to perform tasks such as installing, uninstalling and repair the software.

Software Distribution eliminates the inefficient process of providing thousands of software CDs to users, along with programs and instructions. The automated process of program distribution eliminates user errors such as entering incorrect values in prompts, running incorrect programs, or entering incorrect arguments. By using Software Distribution, clients can successfully run programs and install software without needing to know how to run these programs or which setup options are best for them. Clients do not need to manage their own software installations. Instead, you centrally define and control how and when programs run on client computers. You can choose how little or how much users manage.

Agent

Description:

- InsTIL agent discovers assets remotely
- Distribute software to client from the server.

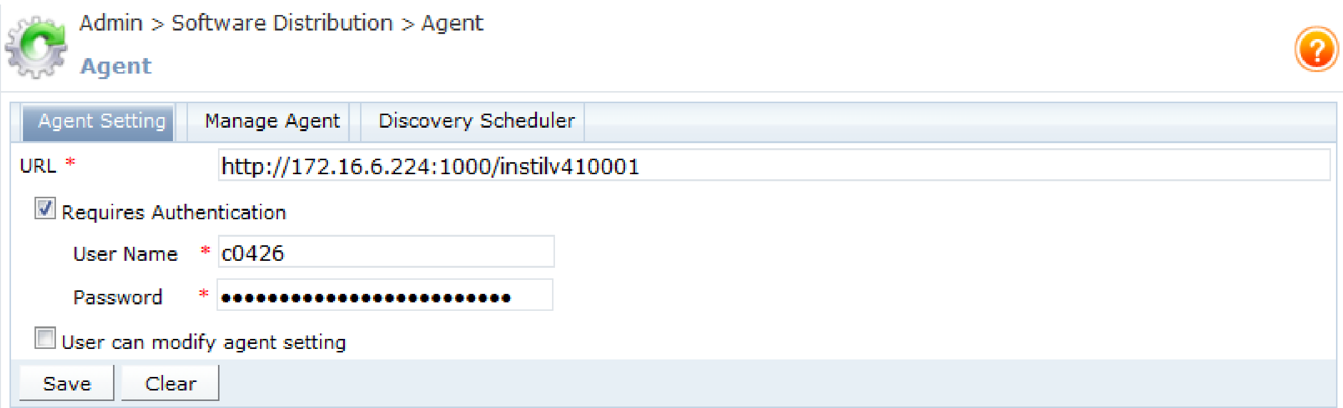
Operation:

- Agent Settings
- Manage agent
- Discovery scheduler

Agent Settings

The configuration setting for deploying an agent is defined here.

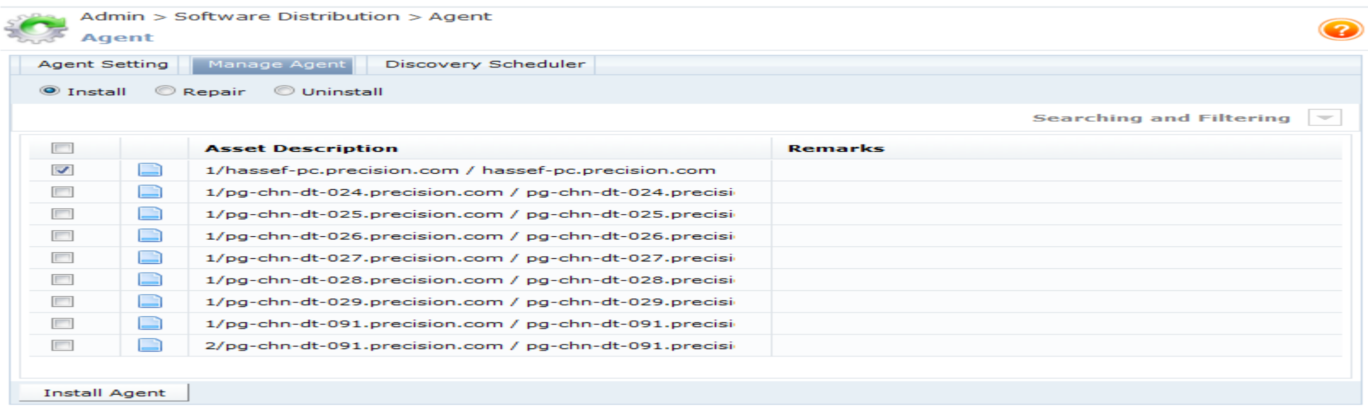
- Enter URL of server where InsTIL is configured and clicks save.
- If the end user does not have the permission to access URL specified , then enable “requires authentication” and enter valid credential to access the URL
- Enable “user can modify agent setting” for the end user to modify the agent settings



Manage Agent:

The user can install, repair and uninstall the agent.

- The asset description list contains assets which were discovered earlier.
- Enable Install and select the asset from the asset description list to install agent
- The asset in which the agent is installed is displayed under repair and uninstallation tab
- Enable Repair and select the asset from the asset description list to repair agent
- Enable Uninstall and select the asset from the asset description list to uninstall agent

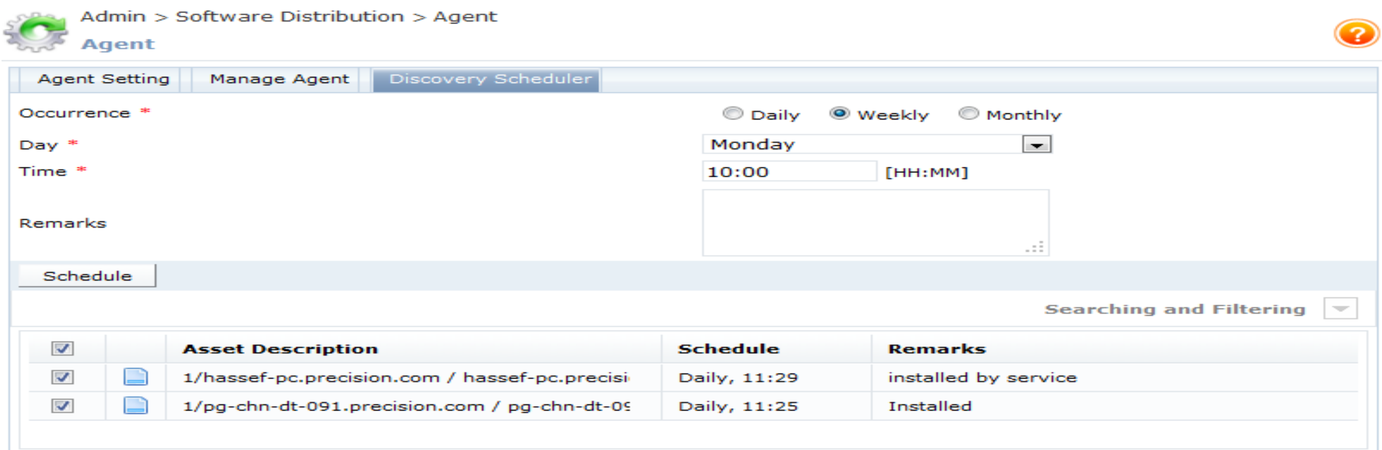


Discovery scheduler:

This feature enables the agent to run a routine scan on assets, on a specific schedule and

Updates the result to the server.

- Select occurrence, to schedule daily, weekly and monthly.
- Enter time
- Select the asset from the asset description list and click Schedule button



Template:

Description:

A predefined format for creating software packages.

Operation:

- Click **new** button to add a new template
- Enter template name
- Select software category from the given dropdown
- Select type as EXE or MSI
- Enter publisher and version of the software(optional)

Parameters:

Description:

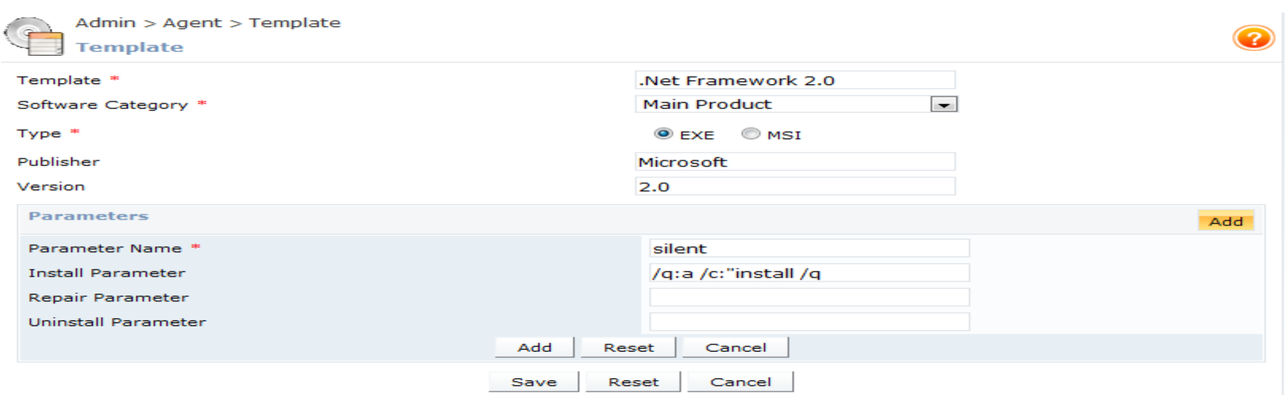
Parameters are switches used during software installation, repair and uninstallation.

Operation:

- Enter parameter to install, repair and uninstall the software
- Click add to create multiple parameters
- The parameter field can be left empty, if there is no parameter for a software package.

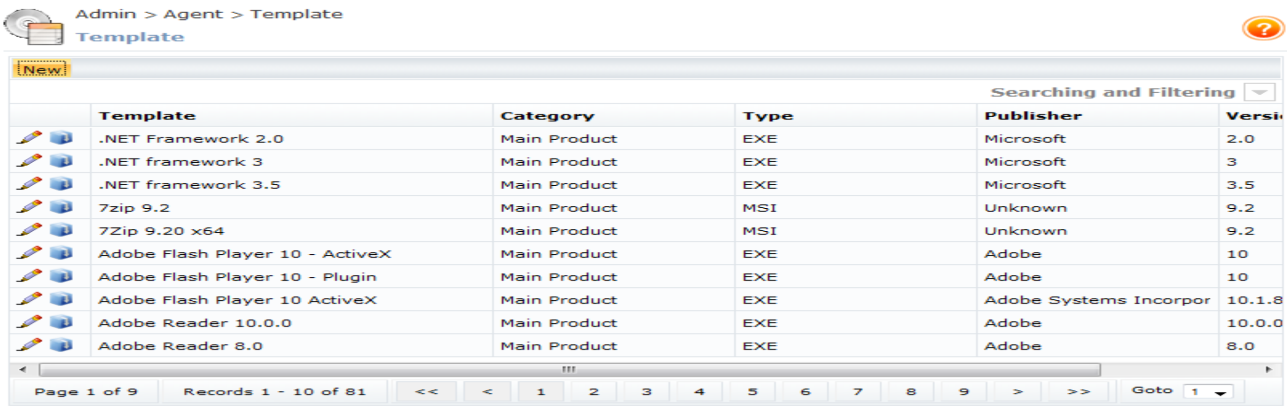
To **add** a new record:

- Click Add to enter the parameter name, install parameter, repair parameter and uninstall parameter
- Click save to save the entry



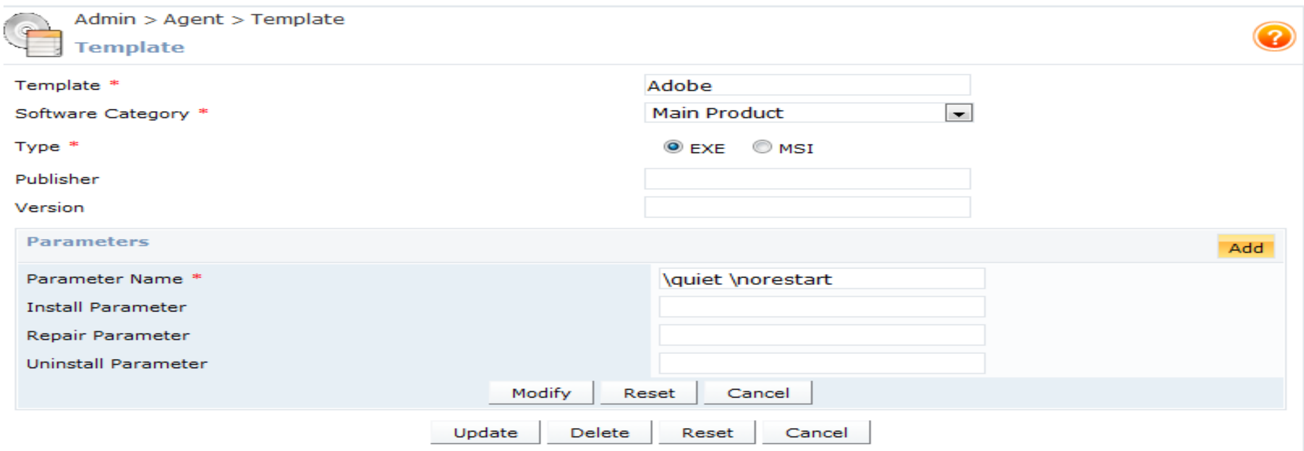
To **modify** an existing record:

- Select the existing record to be modified from the list.
- Perform the required changes.
- Click **modify** button to modify the record.



To **reset** an existing record:

- Click **reset** button to rollback to the previous state.



To **cancel** current operation:

- Click **cancel** button to discard the current action.

To **update** an existing record:

- Select the existing record to be updated from the list.
- Perform the required changes.
- Click **update** button to update the record.

To **delete** an existing record:

- Select the existing record to be deleted from the list.
- Click delete button to delete the record

Searching and Filtering:

- Enter the search word in the textbox.
- Click search button for getting the result in the grid.
- Filtering of data in the grid is done based on the Template, Category, Type, Publisher and Version
- Select data from the dropdown list for filtering.
- The searched and the filtered record are displayed in the grid.

Package:

Description:

A package contains necessary scripts and information to aid in managing the installation, repair and uninstallation process of a software.

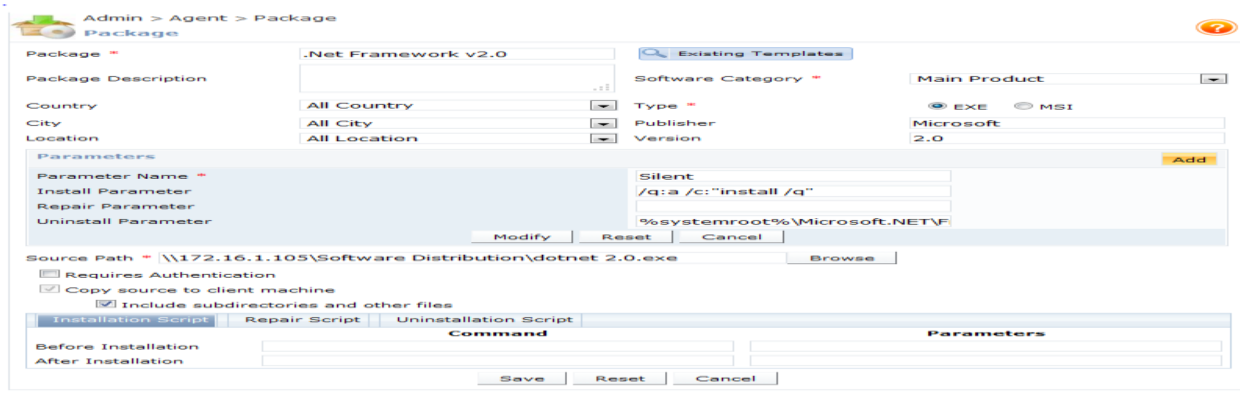
Operation:

- Click **new** button to add a new Package
- Enter package name
- Click existing template and select the predefined template from the list or enter manually
- Enter package description

- Select software category from the given dropdown list
- Select type as EXE or MSI if the existing template is not selected
- Enter publisher and version if the existing template is not selected
- Enter parameter to install, repair and uninstall the software if existing template is not selected
- The parameter are automatically fetched based on the template selected from the existing template
- Click browse and select the source path to access the share which contains the EXE or MSI file
- Click browse, a dialog box will pop-up displaying Domain, Username and Password.
- Select Domain from the dropdown list and enter credential for the selected domain, which will list the domain computers and enable the end user to access the share which contains the EXE or MSI installation file or enter the source path manually.
- If the end user does not have the permission to access the source path specified , then enable "requires authentication" and enter valid credential to access the source path
- Enable the check box to copy the source to client machine
- Enable the checkbox to copy the subdirectories and other files to client machine
- Enter script if required, before and after install, repair and uninstall based on command and parameters
- Click save to save the entry

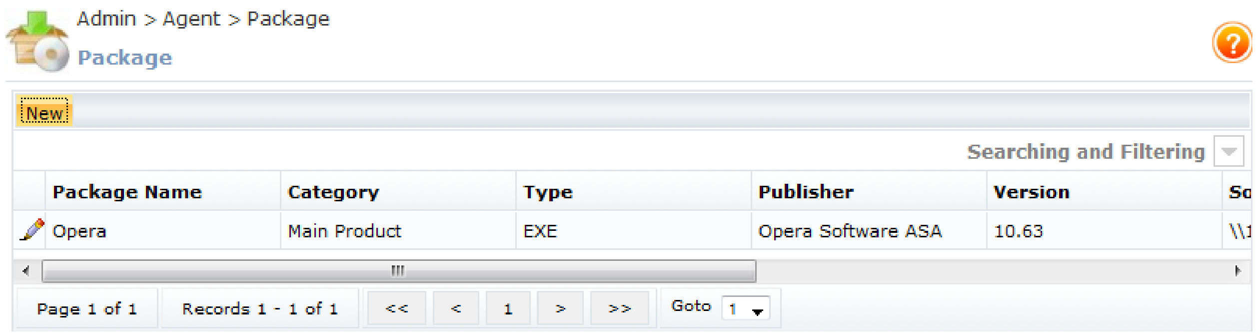
To **add** a new record:

- Click Add to enter the parameter name, install parameter, repair parameter and uninstall parameter



Searching and Filtering:

- Enter the search word in the textbox.
- Click search button for getting the result in the grid.
- Filtering of data in the grid is done based on the Package, Category, Type, Publisher and Version
- Select data from the dropdown list for filtering.
- The searched and the filtered record are displayed in the grid.



Deployment package

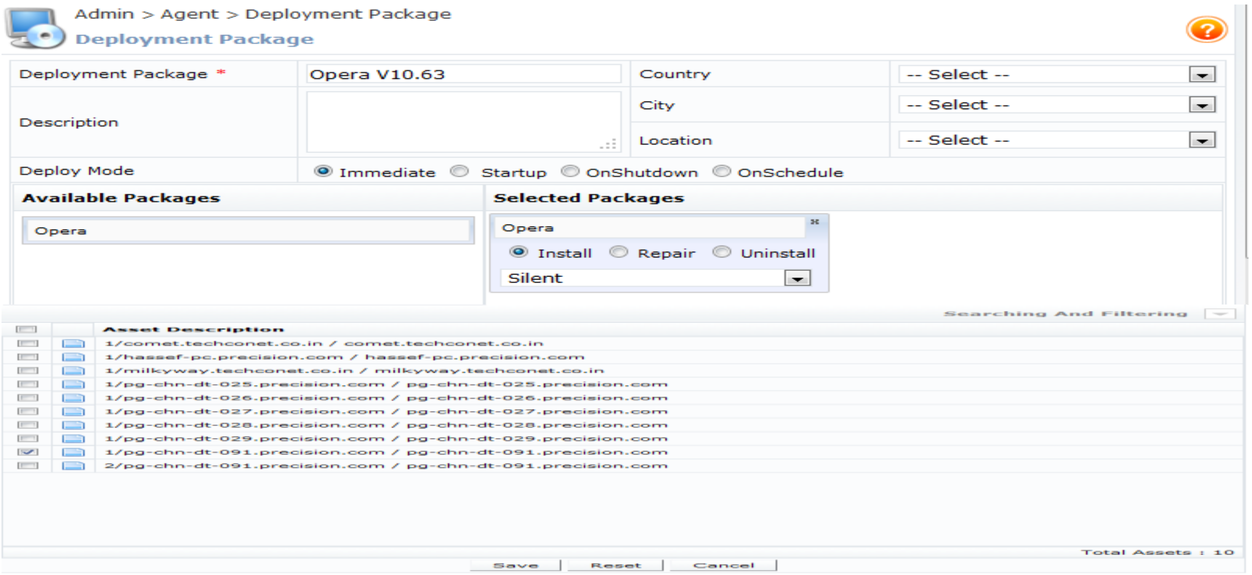
Description

The deployment package contains list of various package which is used to distribute software on client machines.

Operation:

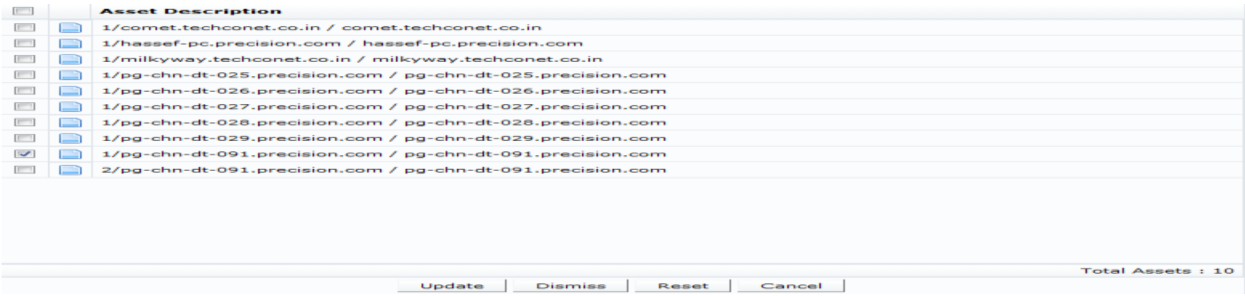
- Click new button to add a new deployment package
- Enter deployment package name and description
- Select deploy mode as immediate /on startup/on shutdown/on schedule
- Select location details (country, city, and location) from the dropdown list ,where it displays asset from the selected location
- Drag and drop packages, from available packages to selected packages
- Select install/repair/uninstall for a package and select the parameter mode (silent, passive, unattended etc.)from the dropdown list
- Select asset/multiple assets from the asset description list, where the software package to be deployed.
- Click save button to save the entry created
- The status of the deploying package can be viewed by clicking on the deploy history icon in the deployment package list

- On deploying a package, initially the status is Not Started and after three minutes the status is In-Progress and indicated by red icon
- On clicking the red icon the deployment package is suspended



To **reset** an existing record:

- Click **reset** button to roll back to the previous state.



To **cancel** current operation:

- Click **cancel** button to discard the current action.

To **update** an existing record:

- Select the existing record to be updated from the list if only the status is as Not Started.
- Perform the required changes.
- Click **update** button to update the record.

To **dismiss** a package:

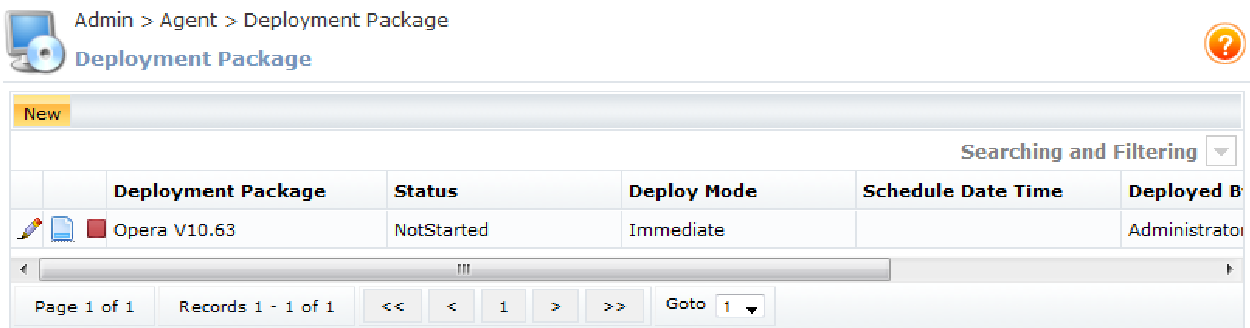
- Select the deployment package from the list
- Click **dismiss** button to dismiss the package

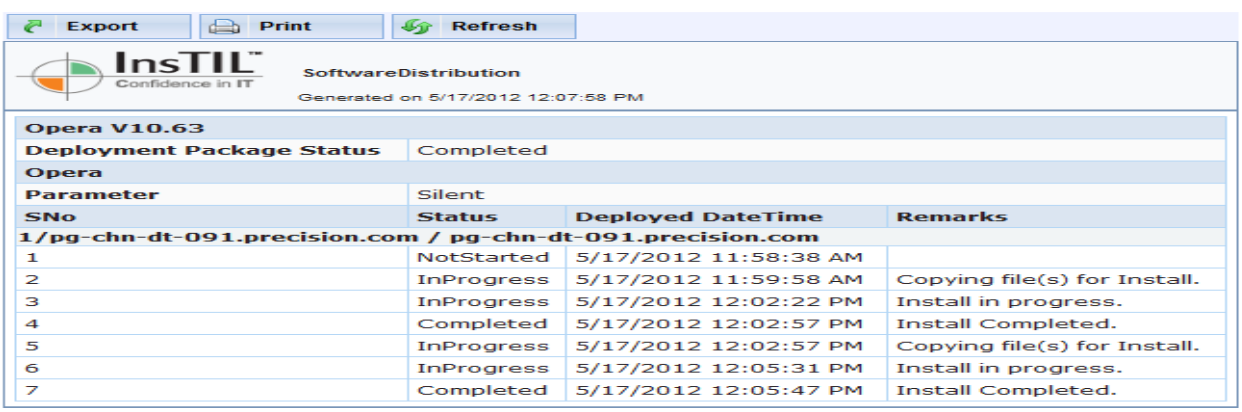
Searching and Filtering:

- Enter the search word in the textbox.
- Click search button for getting the result in the grid.

- Filtering of data in the grid is done based on the, Category, Device Type, Part Description, Asset Group, Domain and Network
- Select data from the dropdown list for filtering.

The searched and the filtered record are displayed in the grid

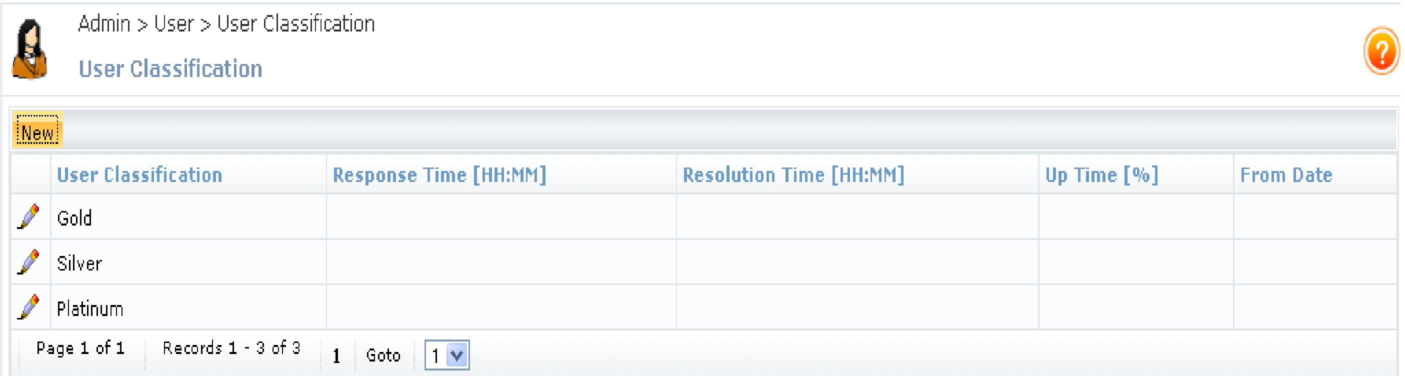




4.4 User

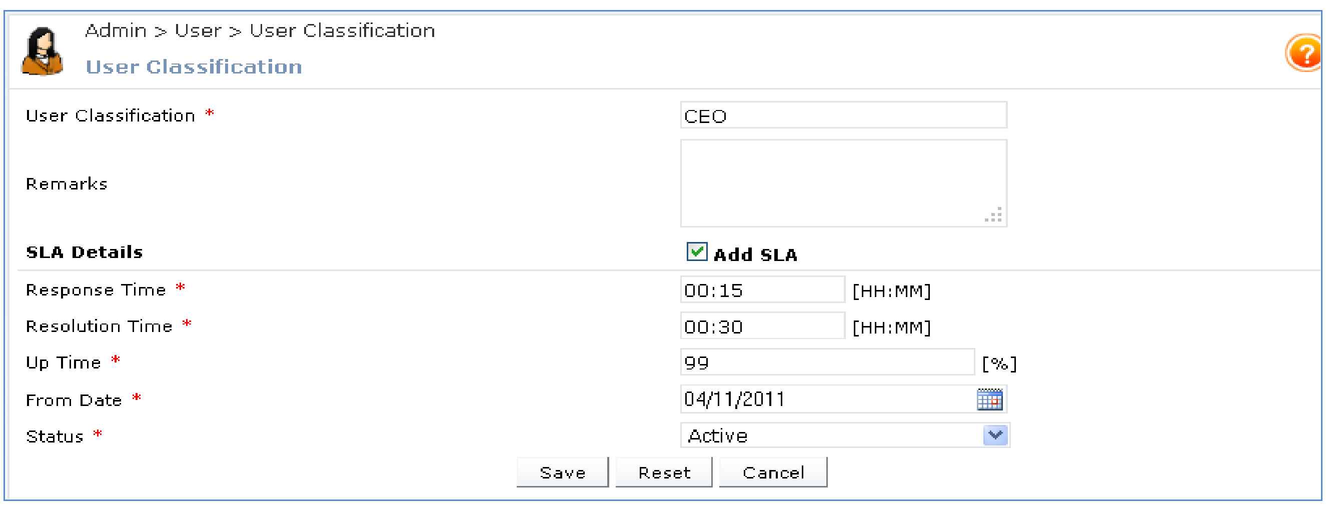
User – User classification

The below fig. represents the create option for User – User Classification. The administrator can create the User Classification for which the service level agreement (SLA) applies. User Classification can be a priority at which the incident needs to be attended. The administrator can define the classification as Gold, Silver, and Platinum. User Service level is divided into response and resolution. Response is the time frame within which the service has to be attended and Resolution is the time frame within which the problem needs to be solved.



Operation

To add a new user classification perform the following task

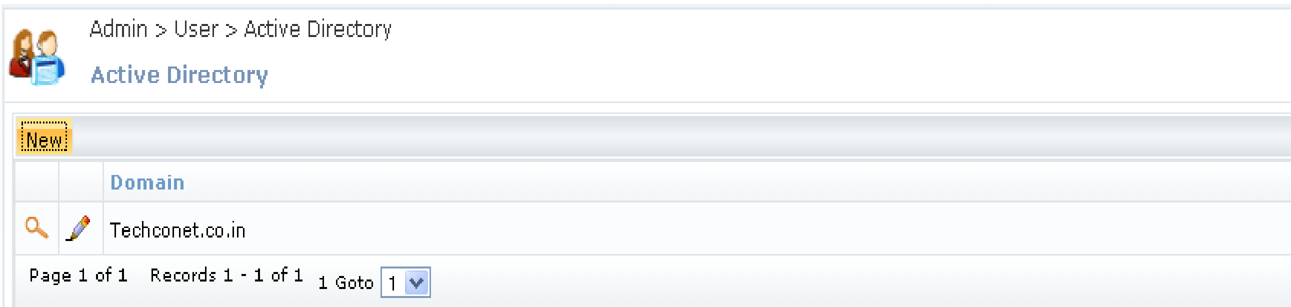


1. Click New
2. Enter the user classification name - The user class name is fixed for which the Service Level Agreement applies [SLA] when the SLA type is selected as User in Service Desk
3. Enable Add SLA

4. Enter the response time - The time frame within which the service has to be attended
5. Enter the resolution time - The time frame within which the problem needs to be solved
6. Enter the uptime
7. Click Save button to save the record created.
8. Click Reset to clear the entries created

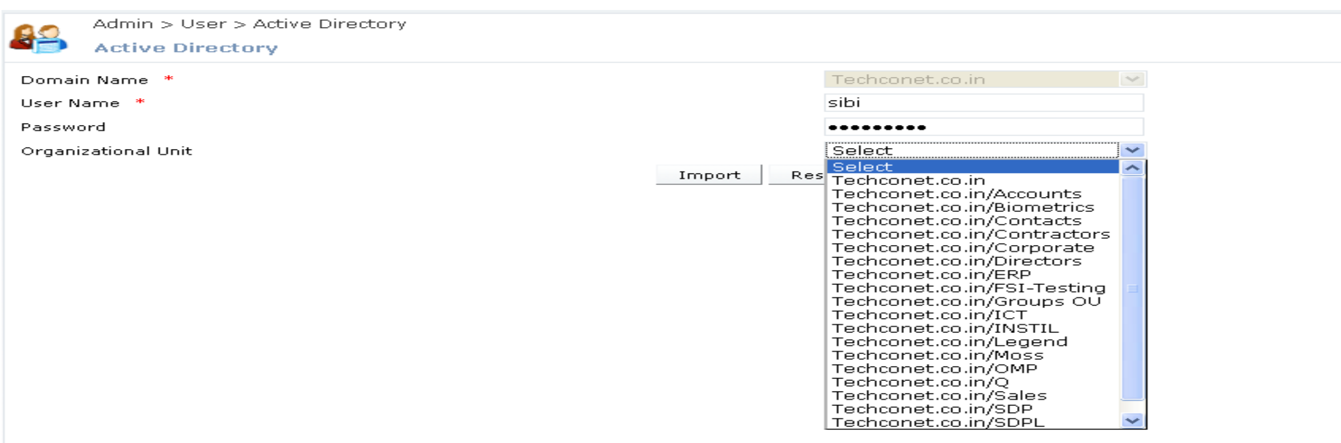
User – Active Directory

The application can be integrated with ADS and all the users in the ADS can be imported to the application. The users can therefore log calls with their respective domain login. The administrator can add all the users into the application using any domain credential.



Operation

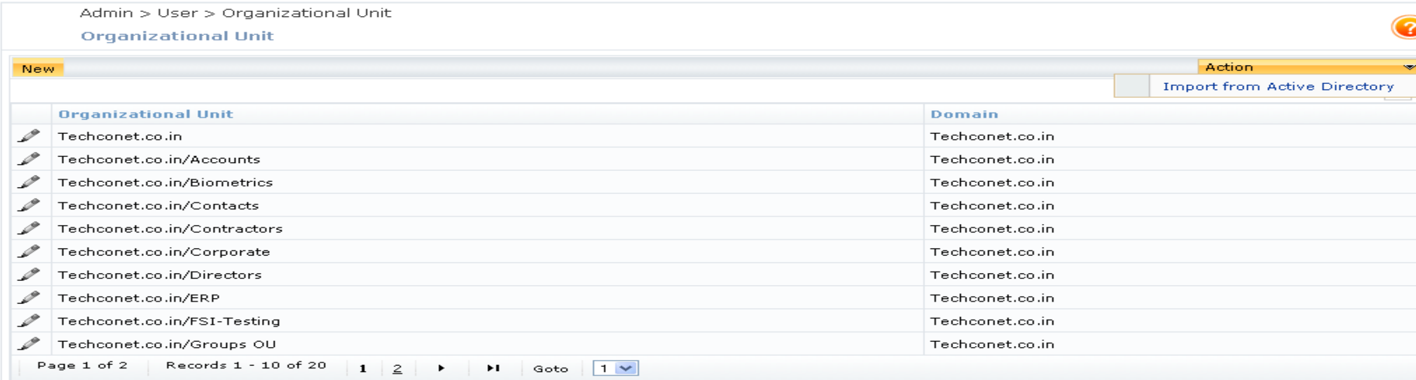
To synchronize the users from the Active Directory perform the following task



1. Select the Import icon for the respective domain for which the ADS synchronization is to be done
2. The domain user name and password are obtained from the master data
3. Select from which OU the users are to be imported and click Import
4. The screen shows the number of failure and new users
5. The users are automatically imported into the application.
6. Click on the Failure link and find the list of users and the reason for not being imported

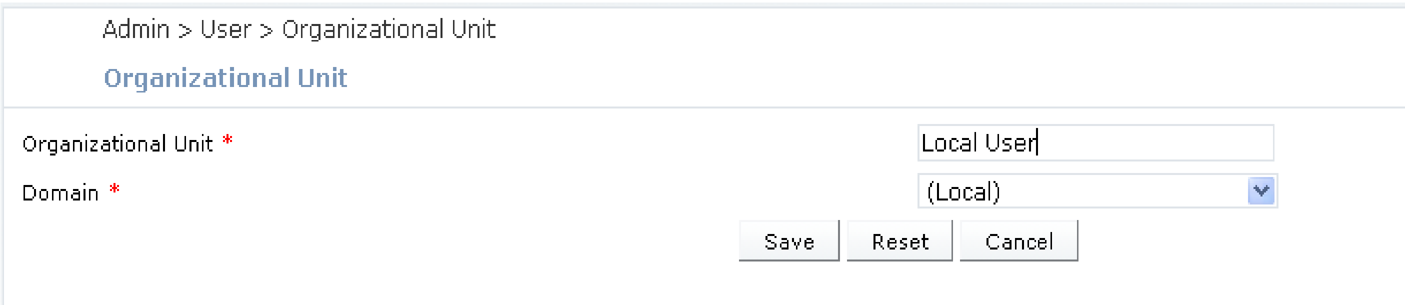
User – Organizational Unit

The list of Organizational Unit available in the domain is added to the master when the Active Directory synchronization process is done. The administrator also has the provision to add OU for non-domain user.



Operation

To add a OU manually perform the following task

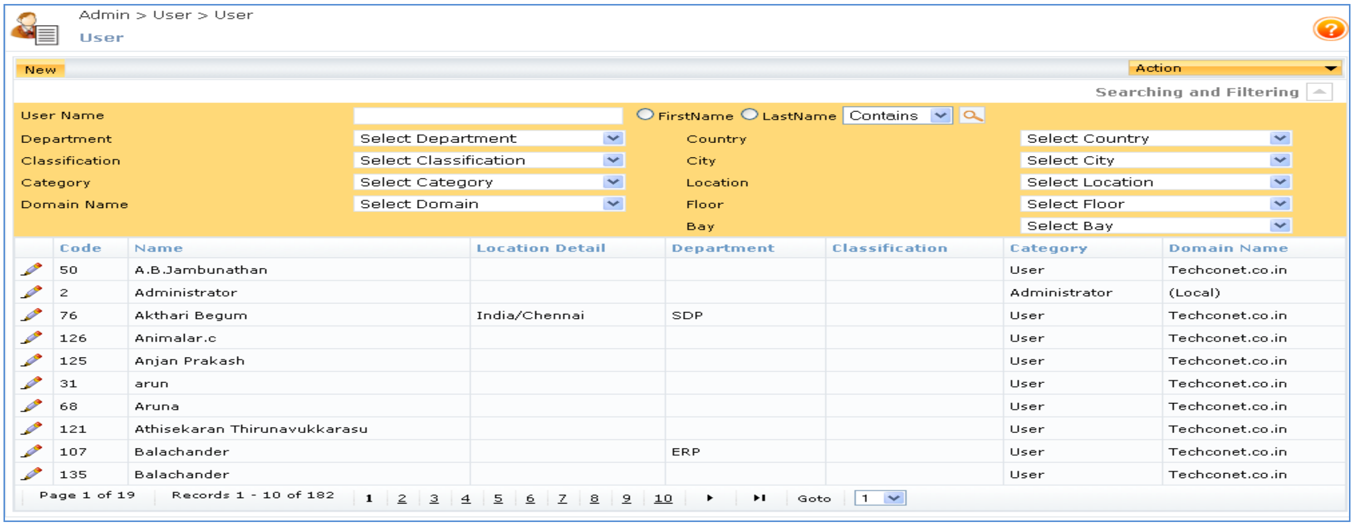


1. Click New
2. Enter the Organizational Unit name
3. Select the domain name from the dropdown list.
4. Click Save to save the record created
5. Click Reset to clear the entries created

User – User

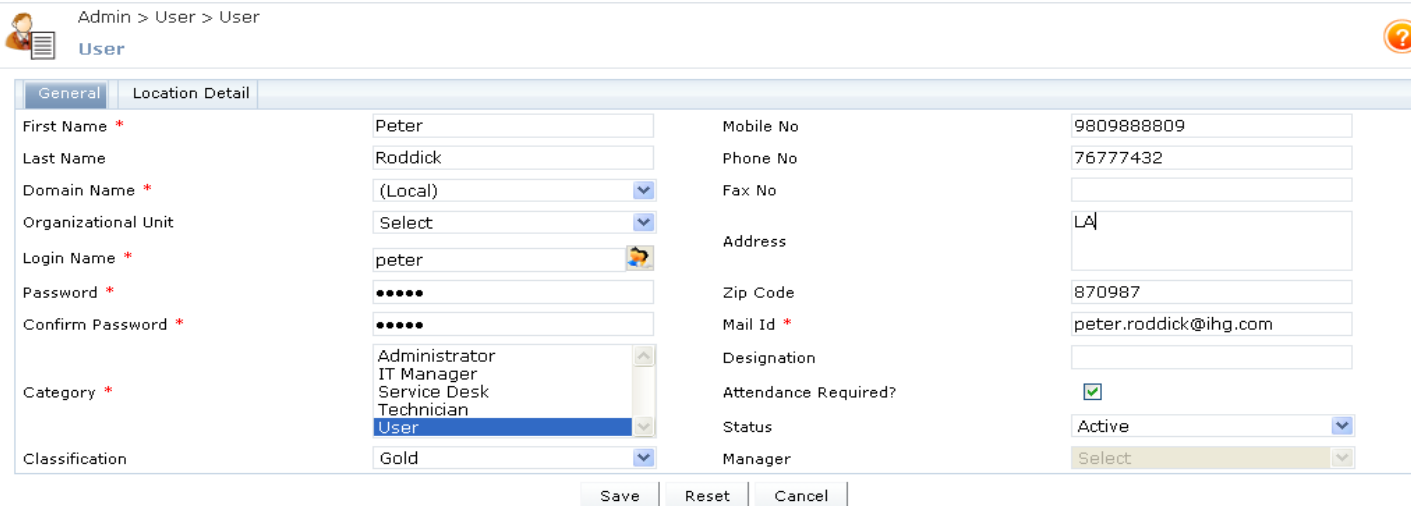
The users synchronized from ADS can be viewed using this menu. The administrator can also add a user who is not there in the domain. The user is alerted through an SMS and email when the account is created.

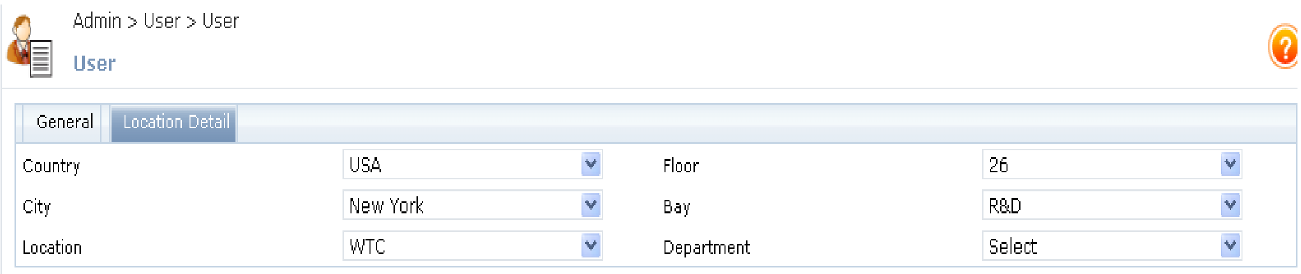
Search and filtering options are also provided for searching particular users. Filtering options are provided to search users based on first name, last name, department, classification, city, location etc. For bulk import of user Import from csv option is also provided. The user is alerted through an SMS when the account is created.



Operation

To add a new user perform the following tasks



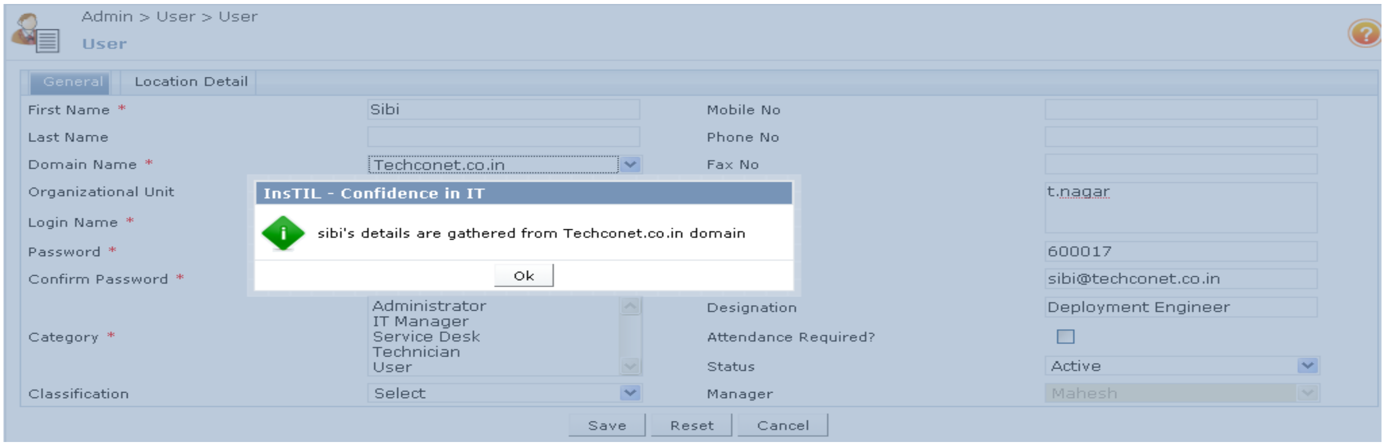


1. Click New
2. Enter the User name and other credentials of the user.
3. Select the category for the user. Note: Multiple categories can be selected for particular user.
4. Enter the mail Id and the user classification type.
5. Select the location tab and enter the location detail of the User
6. Click save button to save the record created.
7. Click Reset the clear the entries created

Single user import from Active Directory

Operation

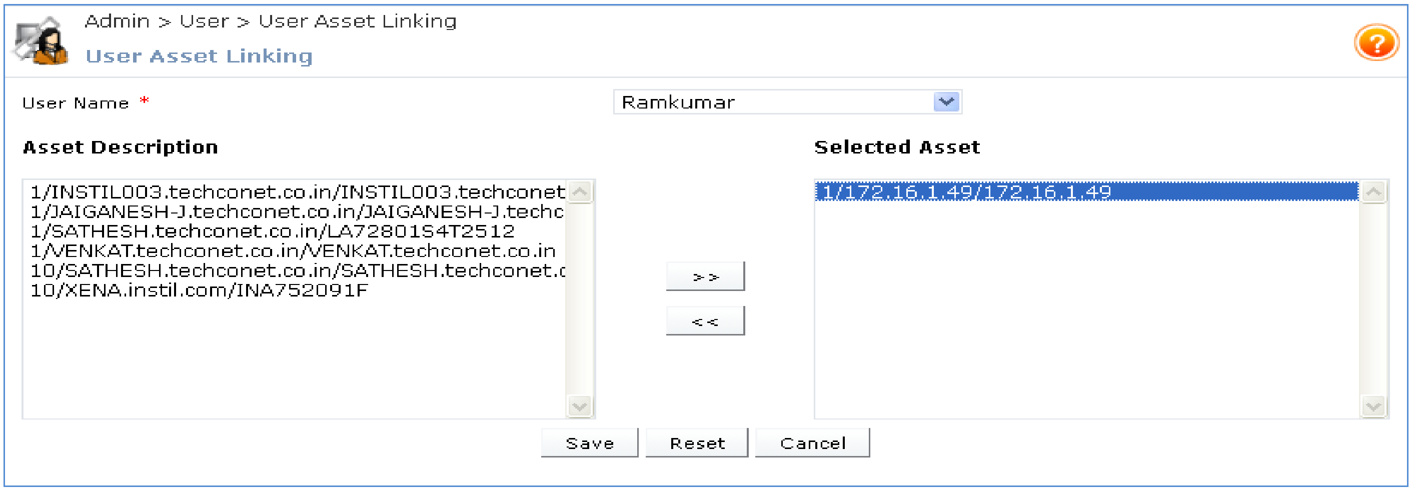
To import a single user from the active directory perform the following task,



1. Click New
2. Select the domain name from the dropdown list
3. Enter the login name of the user to be discovered and select the  icon
4. The information of the users is captured from the AD and the select the role that has to be assigned to the user
5. Click Save to save the entry created.
6. To update the user details, select the user from the list and perform the required changes.

User – User asset linking

The user created is linked with the asset so as to complete the process of user-asset linking. A single asset can be linked to many users or the vice-versa. The user and the asset can be linked only when the location detail of the asset and user are the same. For example if a user holds a desktop and laptop, then these two assets are linked with that particular user.



Operation

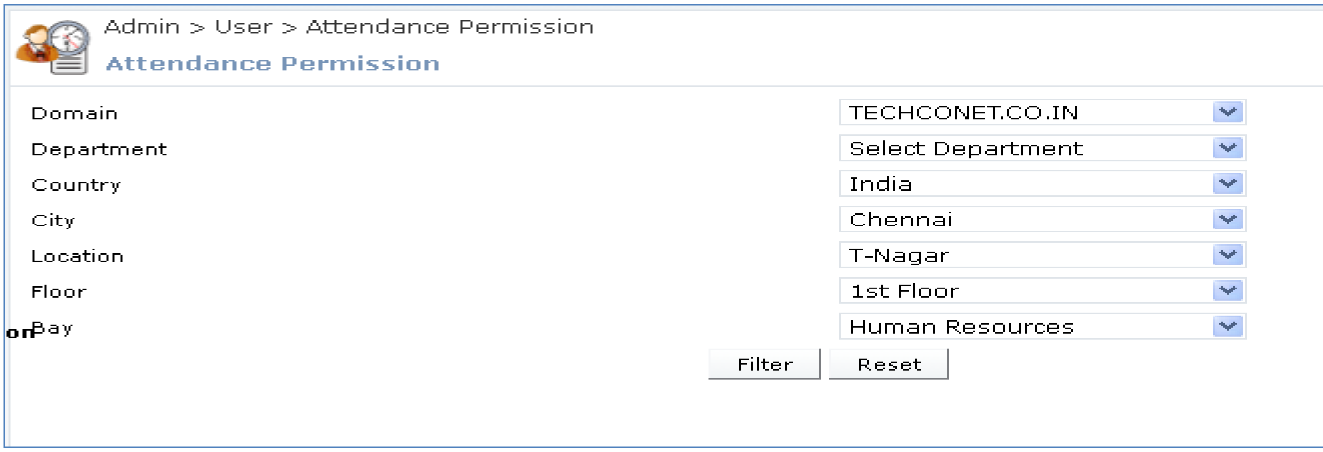
1. Click New
2. Select the user name from the dropdown list for which the asset is to be linked.
3. The list of assets will be shown
4. Select the assets that are to be linked and click >> button.
5. Click save button to save the entry created.
6. To delink an asset, select the user name from the list and click << button.
7. Click update button to update the modifications made.

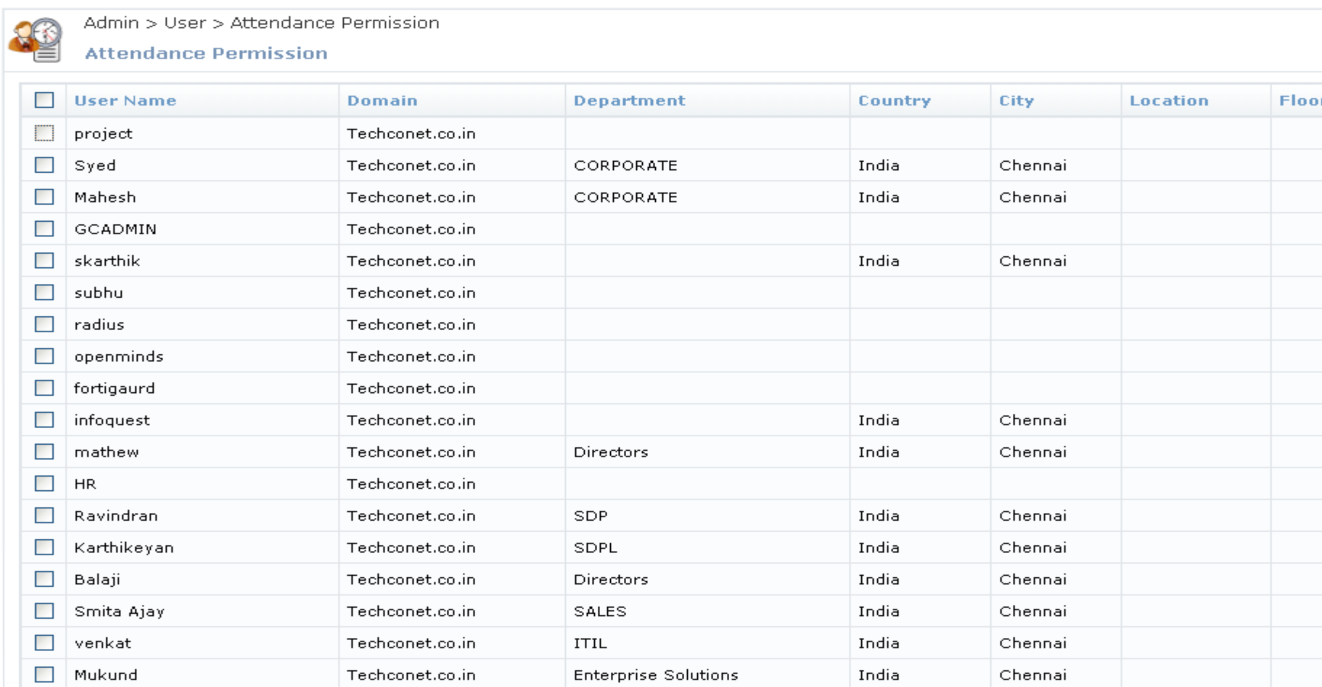
User – Attendance Permission

This feature enables the administrator to give attendance access rights to all users in a bulk fashion. The attendance permission can be enabled for all users by the administrator using selection criteria like Domain, Department, Country, City, Location, Floor and Bay

Operation

1. The users can be filtered based on domain, department, country, city, location, floor and bay
2. Select the above said parameters from the dropdown list
3. Click Filter
4. The list of users will be shown based on the parameters selected
5. Select the user for which the attendance permission is to be enabled or to provide permission for the entire user in the domain select the User name check box
6. Click Update attendance.




Admin > User > Attendance Permission

Attendance Permission

User Name	Domain	Department	Country	City	Location	Floo
project	Techconet.co.in					
Syed	Techconet.co.in	CORPORATE	India	Chennai		
Mahesh	Techconet.co.in	CORPORATE	India	Chennai		
GCADMIN	Techconet.co.in					
skarthik	Techconet.co.in		India	Chennai		
subhu	Techconet.co.in					
radius	Techconet.co.in					
openminds	Techconet.co.in					
fortigaurd	Techconet.co.in					
infoquest	Techconet.co.in		India	Chennai		
mathew	Techconet.co.in	Directors	India	Chennai		
HR	Techconet.co.in					
Ravindran	Techconet.co.in	SDP	India	Chennai		
Karthikeyan	Techconet.co.in	SDPL	India	Chennai		
Balaji	Techconet.co.in	Directors	India	Chennai		
Smita Ajay	Techconet.co.in	SALES	India	Chennai		
venkat	Techconet.co.in	ITIL	India	Chennai		
Mukund	Techconet.co.in	Enterprise Solutions	India	Chennai		

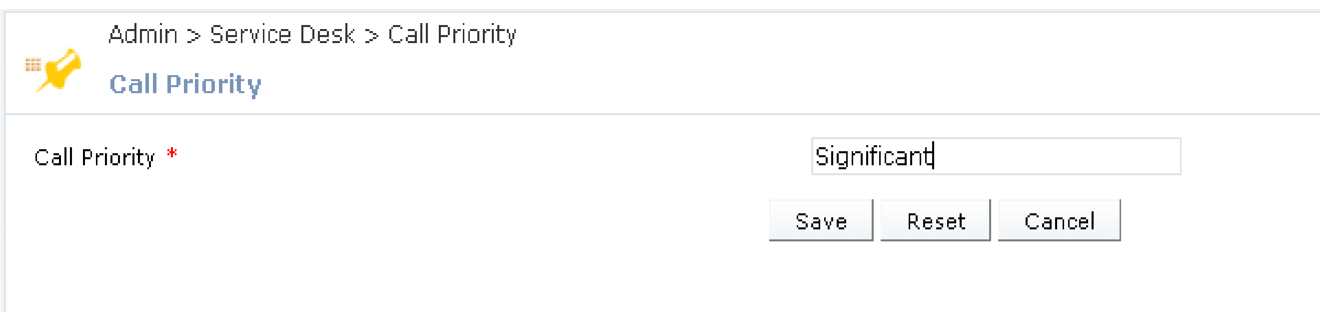
4.4 Service Desk

Service Desk – Call Priority

Every call received at the service desk will come with a priority which describes on what priority the call has to be resolved. By default the call priority master is hard coded as High, Medium and Low. The administrator can add more call priorities to the master.

Operation

To add a call priority perform the following tasks



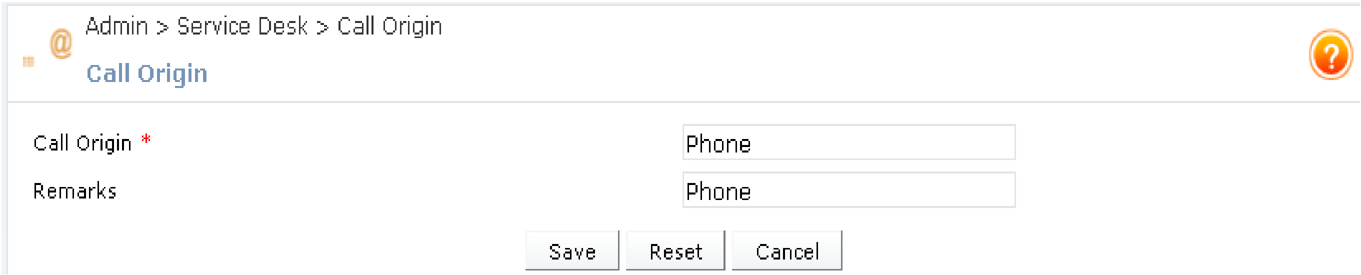
1. Click New
2. Enter the description of the call priority
3. Click Save to save the entry created.

Service Desk – Call Origin

Every call received at the service desk from the user, needs to be provided as to where the call originated or how the problem or issue is informed to the service desk. The user would have used the web or phone or mailed the service desk to intimate the problem or issue. Such mode of call is created in this master screen. By default the call origin option is hard coded in the application as Web, Phone, E-mail and Threshold

Operation

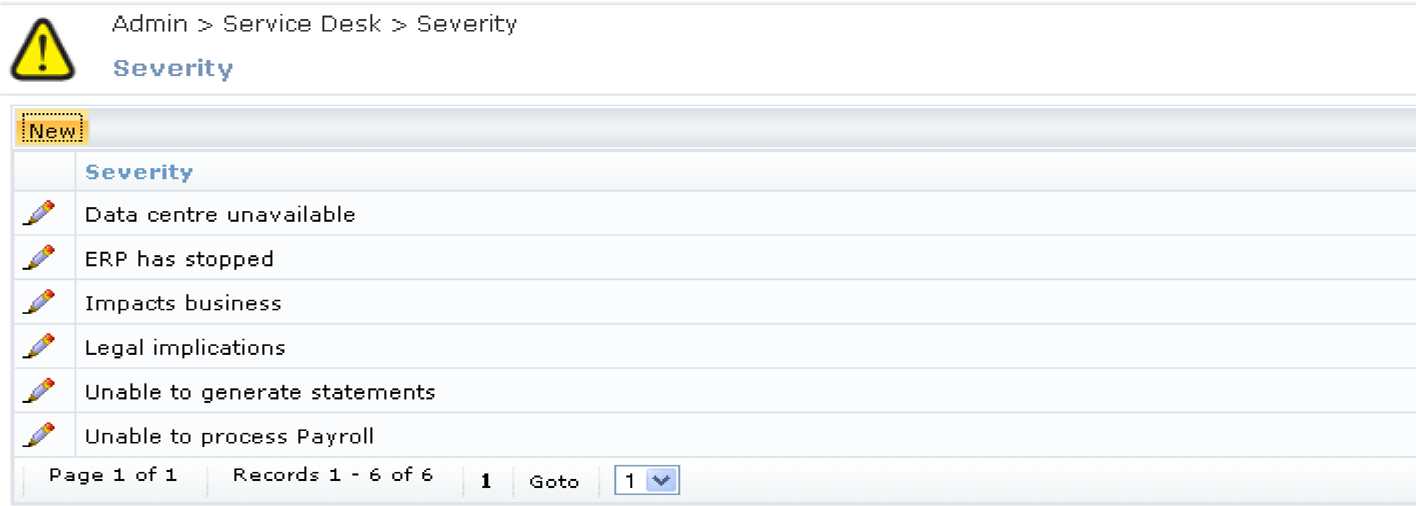
To add a new call origin perform the following task



1. Click New
2. Enter the call origin
3. Use Remarks field for any additional description.
4. Click Save button to save the record created
5. Click Reset button to reset the entries.
6. Click Cancel button to cancel the process

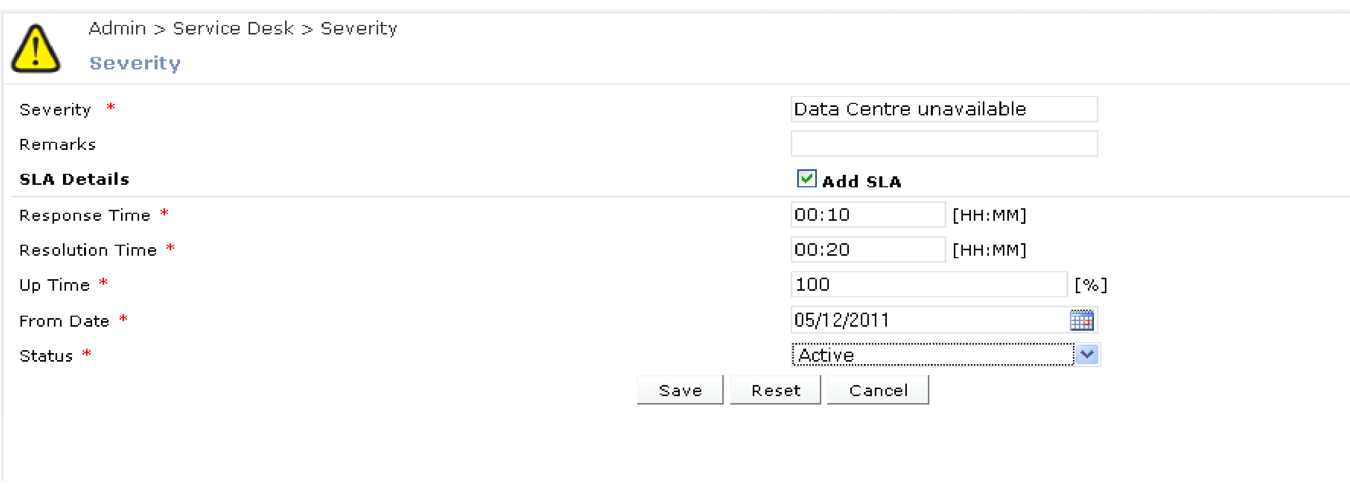
Service Desk – Severity

Severity is a measure of the impact on the business of the failure of a service. Severity is often measured by the number of people or systems affected. The SD specifies the severity of the problem at the time of Classification of the call. For each Severity, there will be an SLA added which will start depending on the severity of the call.



Operation

To add a new severity type perform the following task

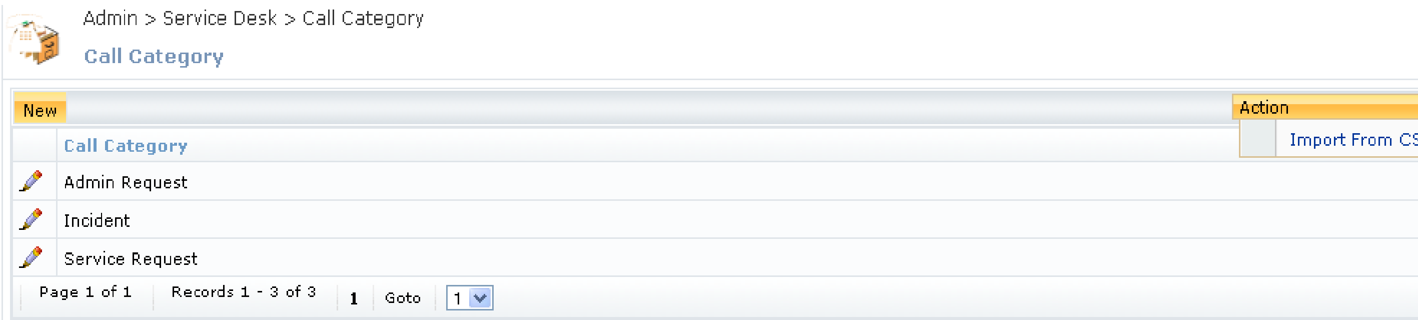


1. Click New
2. Enter the Severity type
3. Enable Add SLA
4. Enter the Response Time for SLA
5. Enter the Resolution Time for SLA

6. Enter the Up Time for the Severity call
7. Enter From Date
8. Select the status from the dropdown list
9. Use Remarks field for any additional description.
10. Click Save button to save the record created
11. Click Reset button to reset the entries.
12. Click Cancel button to cancel the process

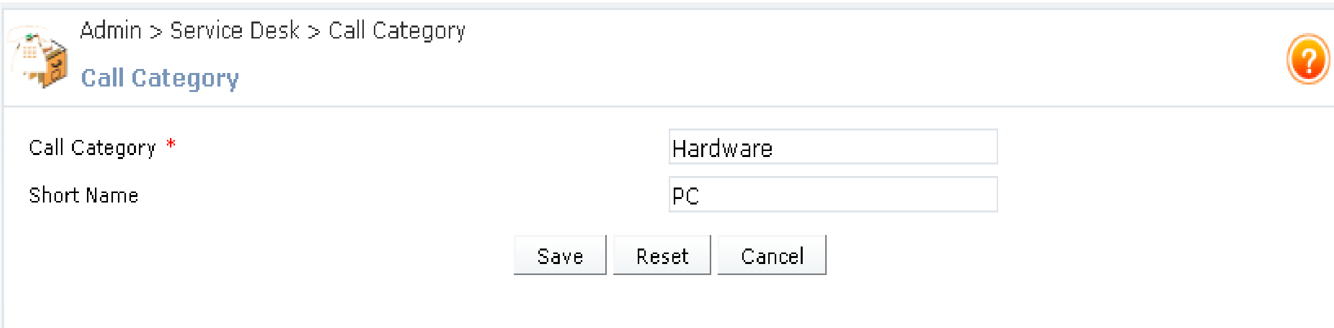
Service Desk – Call Category

The support calls received from the users need to be categorized initially, so that the issues can be tracked properly and the support provided successfully and problem solved can be updated logically in the knowledge base of InsTIL. Therefore, prior to defining the actual complaint, it would be better to categorize all such categories. InsTIL also provides option for importing the service desk masters like Call Category, Complaint and Complaint Detail from excel sheet. This helps the service desk and the technician refer the knowledge base and provide first line support for the common issues faced.



Operation

To add a new call category perform the following task

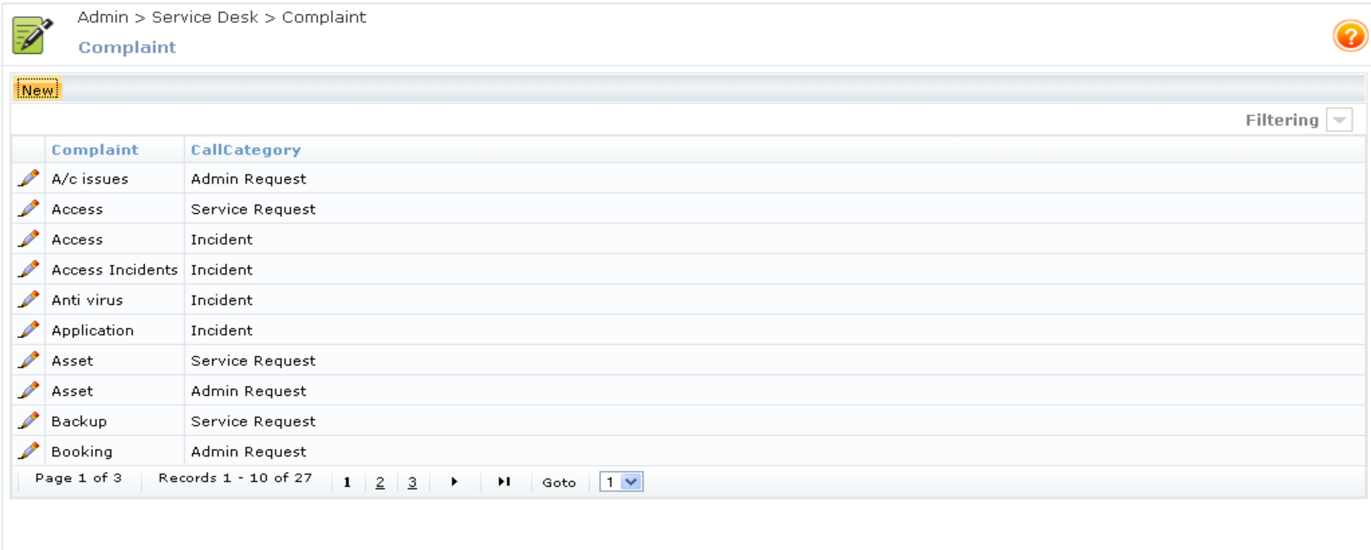


1. Click New to add a new call category
2. Enter the Call Category name – Ex- Hardware, Operating System and Application. This will be useful for the SD to classify the type of call that has been logged.
3. Use Remarks field for any additional description.
4. Click Save button to save the record created
5. Click Reset button to reset the entries.
6. Click Cancel button to cancel the process

Note: to import the call category master select Import from csv and select the file and click Import

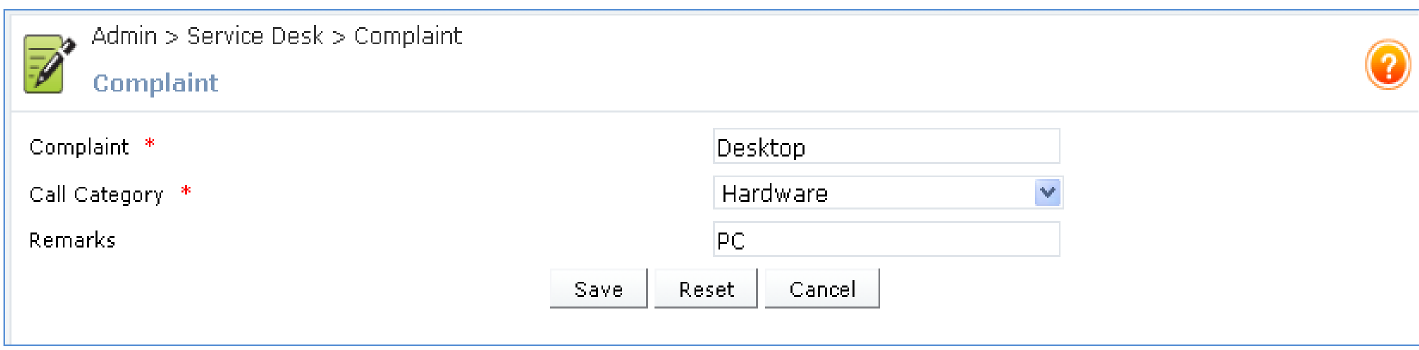
Service Desk - Complaint

After defining the call category, the administrator can pre-define the nature of complaint as shown in the below screen. Click complaint master from the Service Desk menu, the below screen appears



Operation

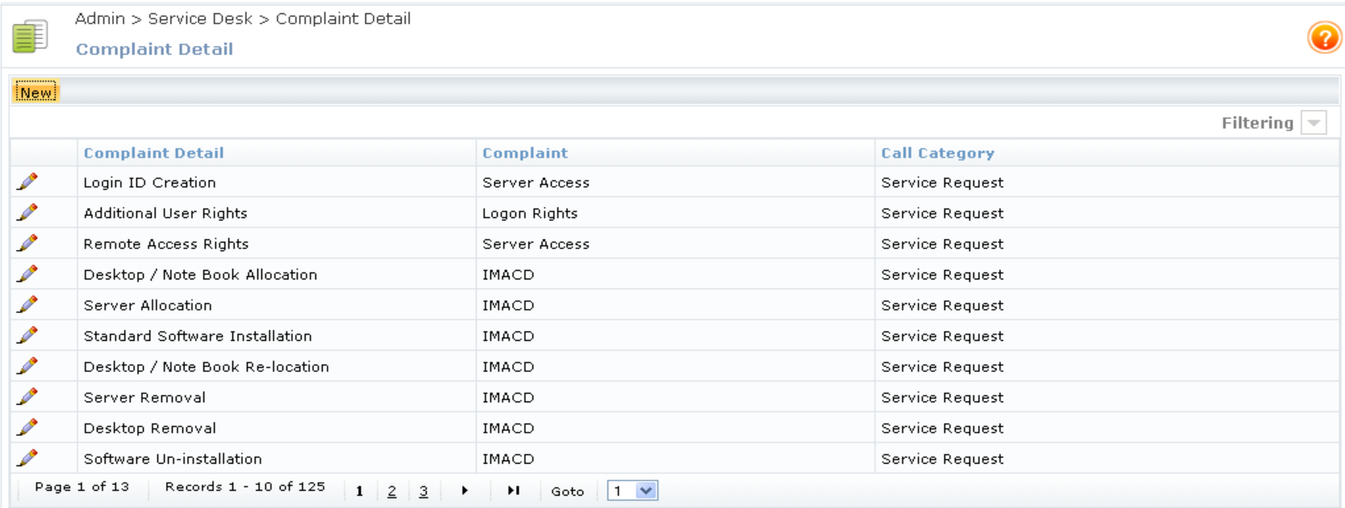
To add a new complaint perform the following tasks



1. Click New
2. Enter the complaint – Monitor, Operating System errors, UPS Shut down etc
3. Select the call category from the dropdown list - select the most appropriate one.
4. Use Remarks field for any additional description.
5. Click Save button to save the record created
6. Click Reset button to reset the entries.
7. Click Cancel button to cancel the process

Service Desk – Complaint Detail

After a broad classification of complaint is created, the administrator can create the complaint detail related to the complaint.


Admin > Service Desk > Complaint Detail

Complaint Detail

New

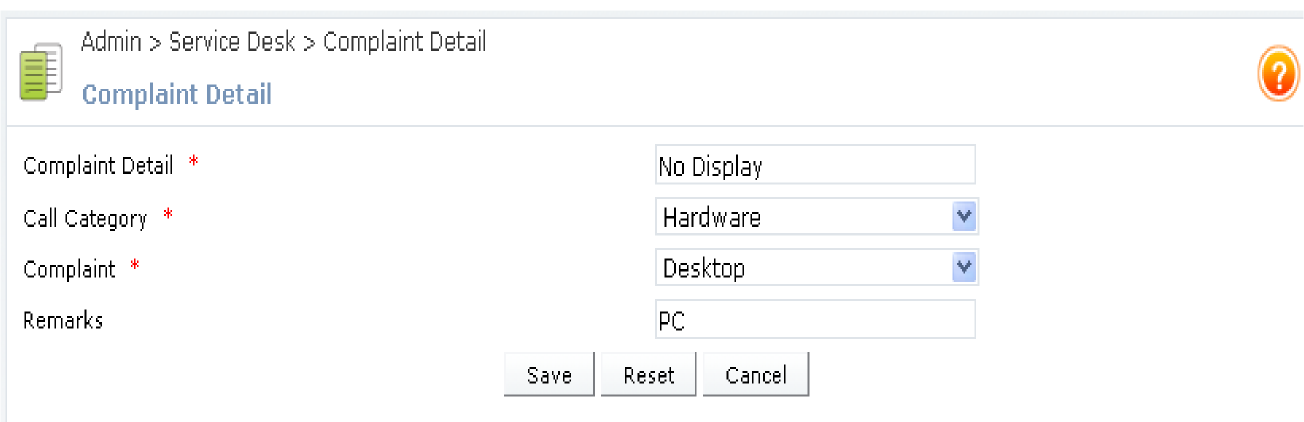
Filtering

Complaint Detail	Complaint	Call Category
Login ID Creation	Server Access	Service Request
Additional User Rights	Logon Rights	Service Request
Remote Access Rights	Server Access	Service Request
Desktop / Note Book Allocation	IMACD	Service Request
Server Allocation	IMACD	Service Request
Standard Software Installation	IMACD	Service Request
Desktop / Note Book Re-location	IMACD	Service Request
Server Removal	IMACD	Service Request
Desktop Removal	IMACD	Service Request
Software Un-installation	IMACD	Service Request

Page 1 of 13 Records 1 - 10 of 125 1 2 3 Goto 1

Operation

To add a new complaint detail perform the following task

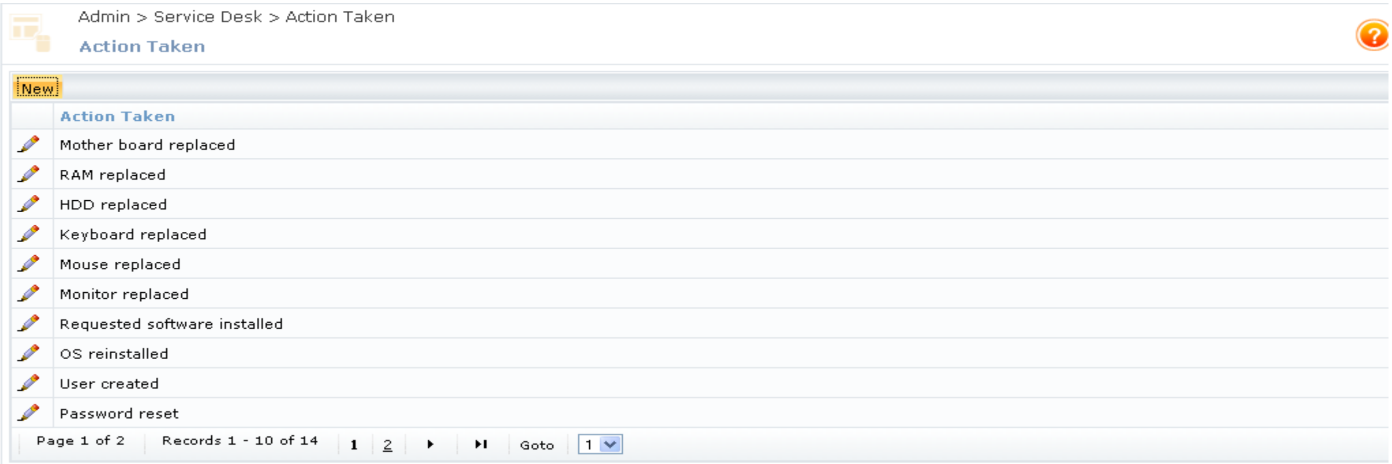


1. Click New
2. Enter the complaint detail related to call category and complaint selected
3. Select the call category from the dropdown list
4. Select the complaint from the dropdown list
5. Use Remarks field for any additional description.
6. Click Save button to save the record created

7. Click Reset button to reset the entries.
8. Click Cancel button to cancel the process

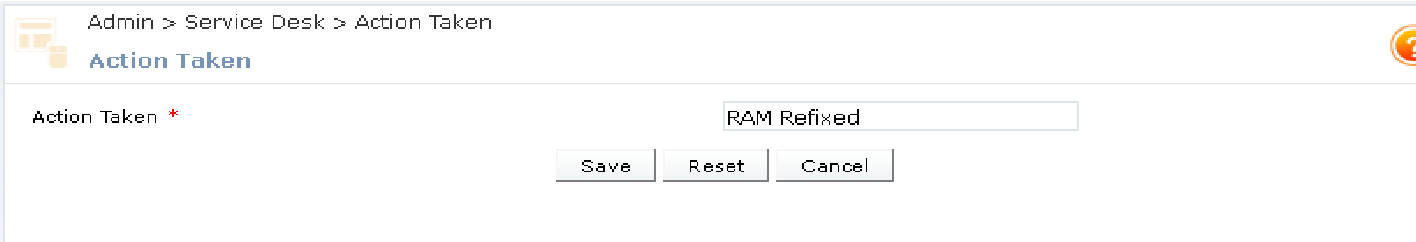
Service Desk – Action Taken

The technician updates the call by describing the action taken for the problem. The technician can also choose the pre-defined Action taken from the Action taken master. By default the application comes with a set of default call Action Taken



Operation

To add a new Action Taken perform the following task



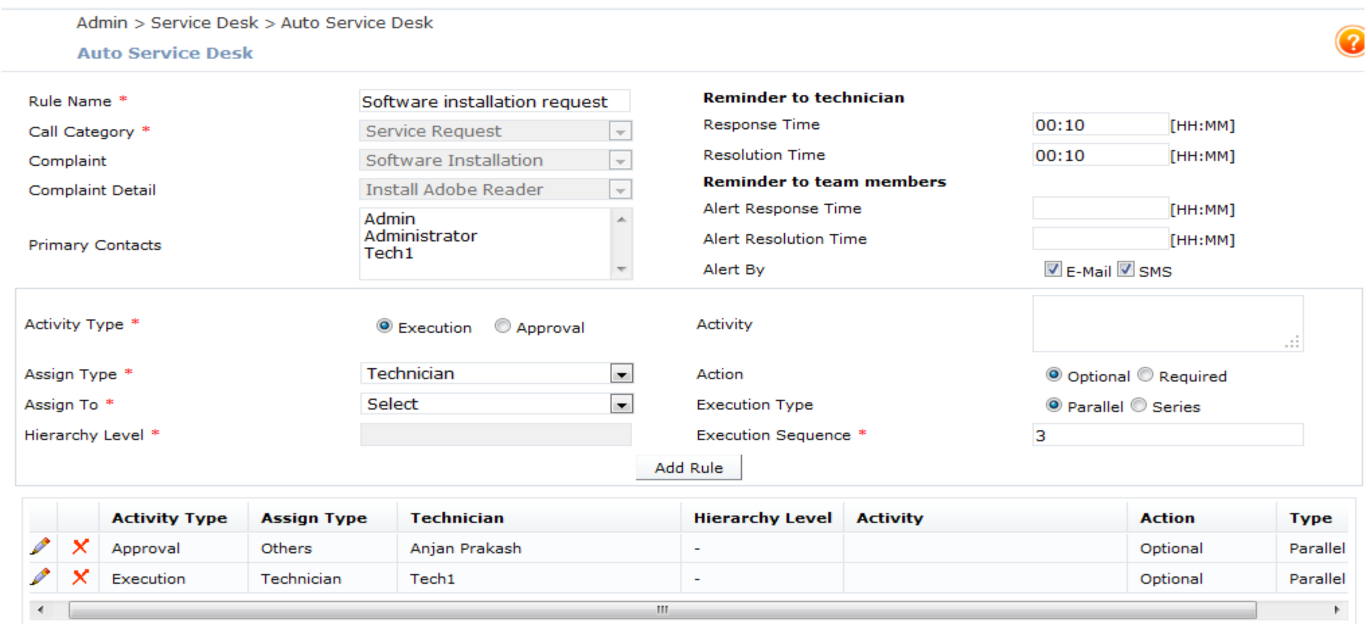
1. Click New
2. Enter the description of the Action taken
3. Click Save button to save the record created
4. Click Reset button to reset the entries.

5. Click Cancel button to cancel the process

Service Desk – Auto Service desk

The service desk rules are defined to make the incident flow process automated. The rules are created for various call categories. The reminders to various technicians and other team members are created in these master settings.

This feature is enabled based on license purchased.



Steps for creating a new rule

Step 1: Click New
Step 2: Enter the rule name in order to identify a rule
Step 3: Select the call category from the dropdown list which is created as masters. For example
Application, Hardware etc.
Step 4: Select the sub category levels from the masters if required.
Step 5: Enable the Alert By as E-mail / SMS

Step 5: Select the Technician name to which the rule is to be applied.
Step 6: The action type is either selected as Optional or Required.
Note:
Optional Action type means, the selected technician is optional for completing the call.
Required Action type means, the selected technician is definitely required to complete the call.

Step 7: Select the execution type as either Parallel or Series
Note:
Parallel refers when a particular call is assigned to multiple technicians, either of the technicians can attend the call.
Series execution type refers when a call is assigned to multiple technicians; the technician has to respond to the call according to the sequence that is defined.

Step 8: Click Add rule to save.
Step 9: Repeat step 8 to add multiple rules in the same sequence.

Reminder to the technician and other team members

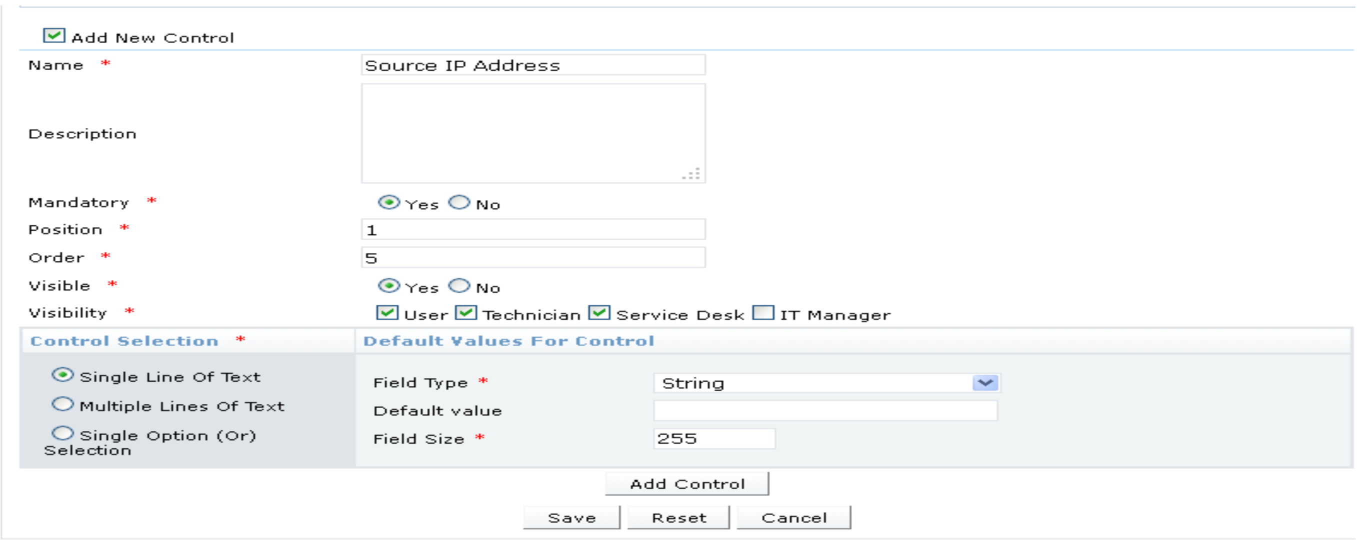
1. Set the response time and resolution time for the alert to be triggered

2. A mail will be triggered to the technician if the defined response time and resolution time is not met.

3. In case of a call assigned to multiple technicians, the mail will be triggered to other team members also.

Service Desk - Template Creator

The incident template creator generally enables the administrator to create templates for various types of workflow within the organization. The administrator creates templates, which can be accessed by the User, Service Desk and Technician while raising a request. The user selects the template based on the workflow requirement while raising a request.



Steps to create an Incident Template

1. Click New
2. Type the name of the template and a suitable description
3. The template can be made accessible to certain user community based on the workflow requirements
4. By default the application has tabs like Logging, Classification, Assign, Update, Clarification and Close. For each tab various controls can be added
5. For example - Adding New control in Logging tab
6. Enable Add New control and name the control that has to be created
7. The administrator can make that particular control as mandatory or not, by selecting either Yes or No
8. The position and the order of the control can also be defined, and the controls will be displayed based on the position and order
9. The added control can be made visible or not to each categories like User, Technician, Service Desk and IT Manager
10. Select the visible status as Yes or No and also select the categories for which the control is to be displayed
11. The control created can be of various selection types like Single Lines of text or Multiple lines of text or Single option

a. For single lines of text the created control can be of String , Date Time, Number, Mail and Date field types

12. For Multiple lines of text the user can enter text of multiple lines i.e. a sample control of Remarks type
13. For single option the created control can be of Radio button, Dropdown and Checkbox field type

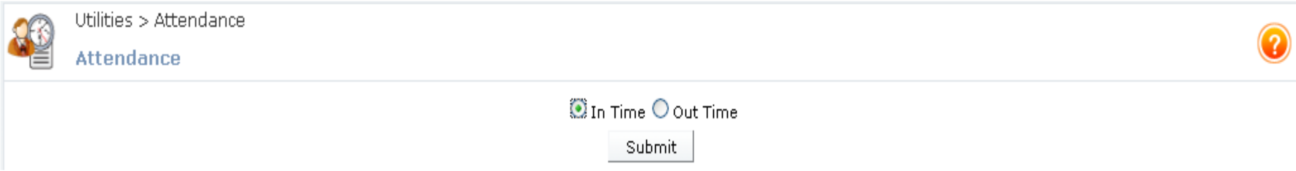
Utilities

Attendance

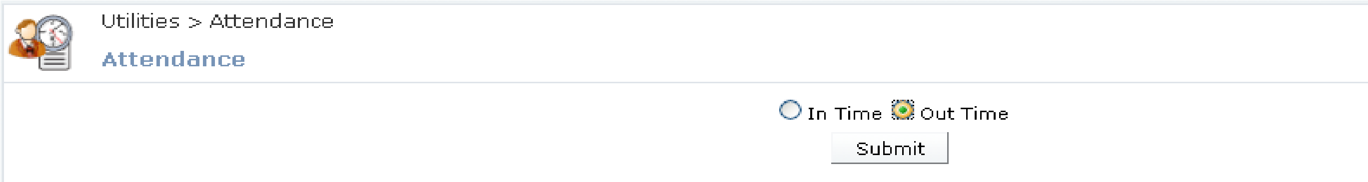
This feature enables the user to mark the Punch In time and Punch Out time for the particular day. This feature is made available for all the roles in InsTIL.

Operation

1. Select Punch In time and submit which marks the in time for the user

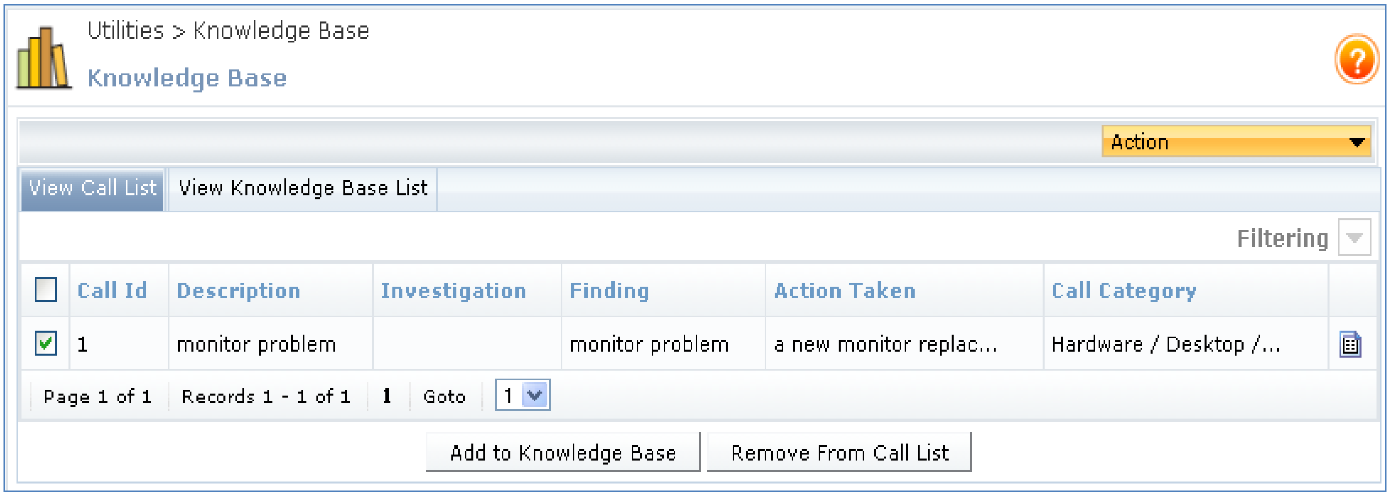


2. Similarly select Punch Out time and submit which marks the out time for the user.



Knowledge Base

The knowledge base is populated with the information from the incident data. All incidents with status as Completed or Closed will be displayed in the Grid. These incidents can be moved to the knowledge base. The administrator has the provision for updating the knowledge base or the administrator can be given the permission for viewing the knowledge base alone.

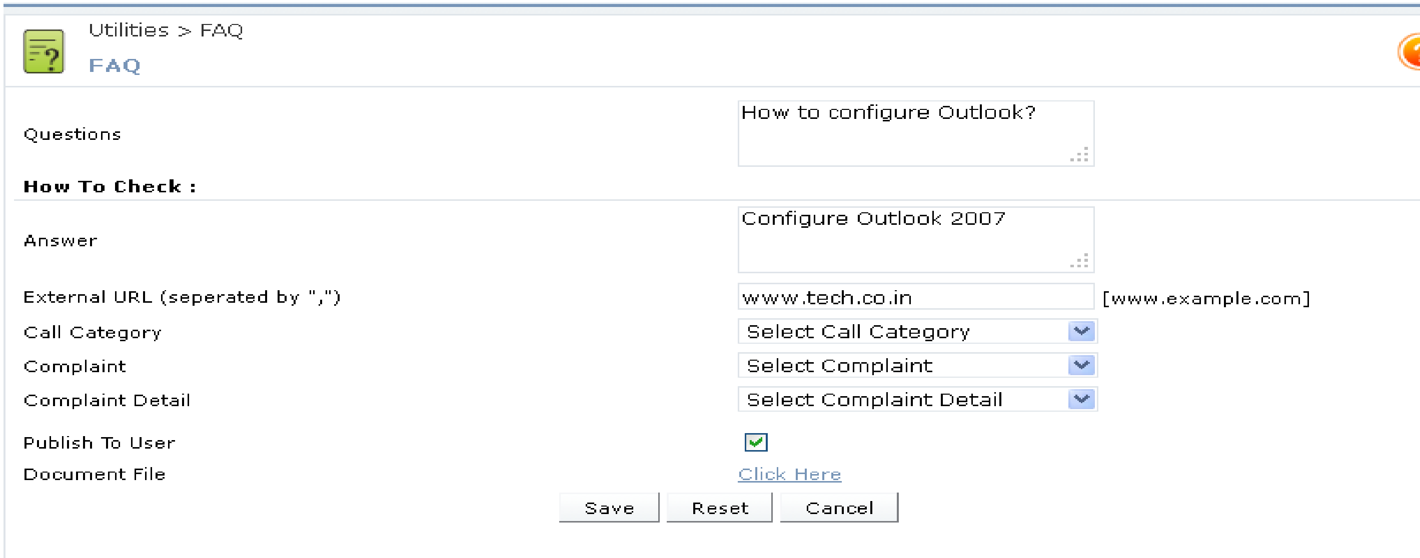


Operation

1. The calls with the status closed and completed will be displayed in the grid.
2. Click view to see the complete call history of the call.
3. Select the calls that has to be added to the knowledge base
4. Click Add to Knowledge base to add the call to the knowledge base.
5. Click View Knowledge base to see the calls that are added in the knowledge base
6. To remove a call from the database, select the call and click Remove button.
7. To search a content from the knowledge base, type a keyword and click Search knowledge base

FAQ

The FAQ module is to use to gather some information related to the queries posted .The FAQ can be updated by the Service desk, Administrator, Technician and IT Manager if permissions are given by the Administrator in the settings menu.



Operation

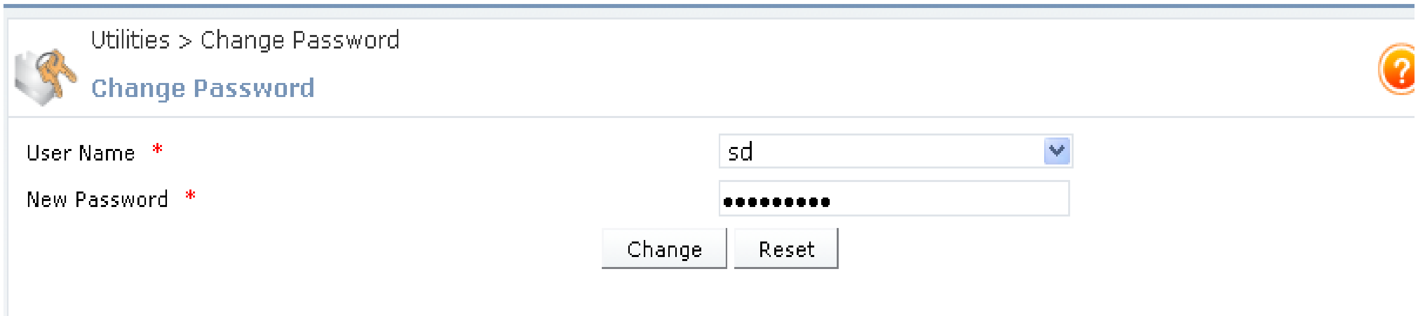
1. Type the question for the FAQ (Search keyword)
2. Type the answer.
3. Type the Url(s) for providing the information.
4. Upload a document file.
5. Select the Call Category, Complaint and Complaint detail (if needed), to group the FAQ.
6. Enable Publish to user knowledge base to be viewed by the end user.
7. Click Submit to save the FAQ created.
8. To view a FAQ select search FAQ and type the keyword to be searched and click search.

Change Password

This utility allows the administrator to change the password for a locally created user.

Operation

1. Click on Admin → Utilities → Change Password
2. Select the local user name
3. Type the new password
4. Click on change to save the new password



Preference

To set owner's favorite as default. It can be set by all categories (Administrator, User, Technician, IT manager, Service Desk) with their options provided. If the preferences are not set, the default settings are used. The screen for Preference is shown below.

Operation

Asset Status:

Select the status such as Active, Inactive, Sold, and Written off. (Can choose either one or all).

User Status:

Select the status such as Active and Inactive (Can choose either one or both).

Services:

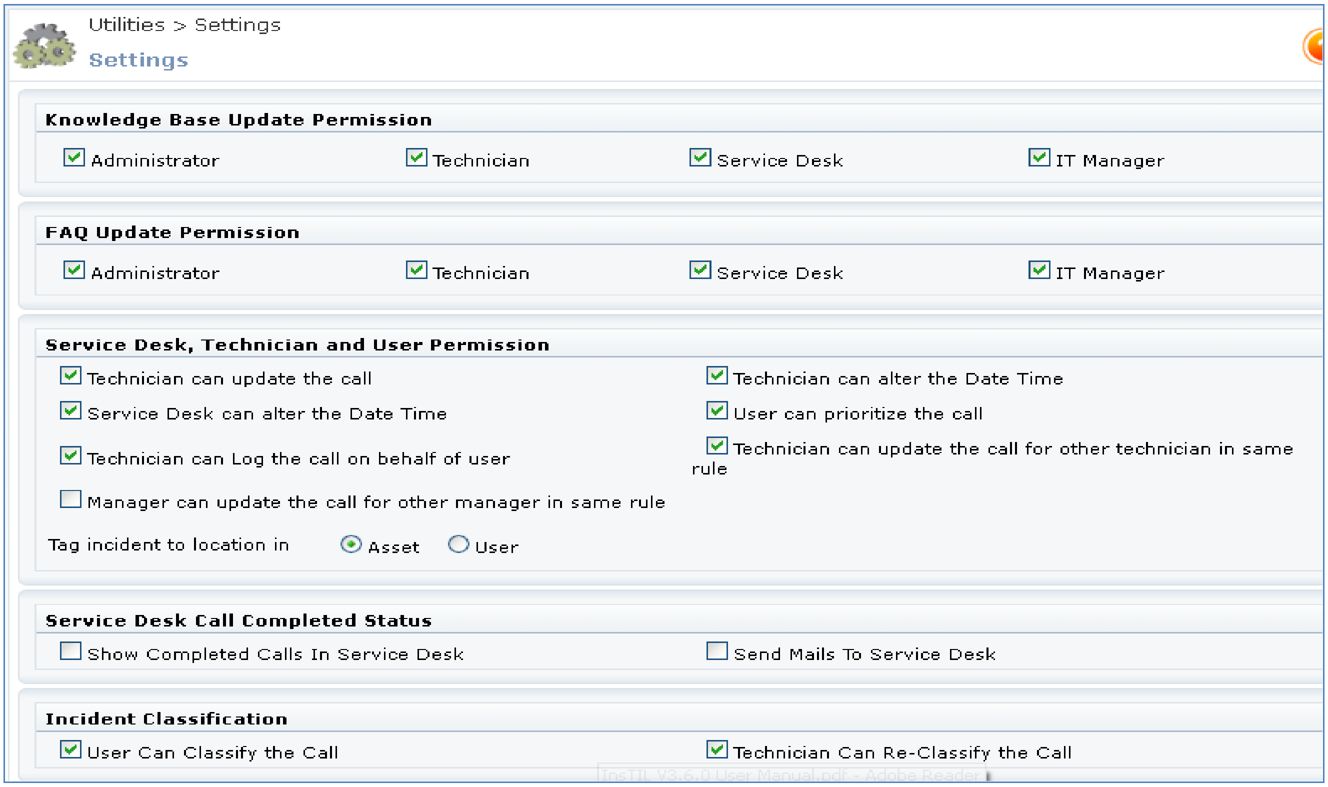
1. Enter the Call close in days. To enable Automatic Closure from the status complete
2. Enter the Time Interval For Escalation (Timer Application).

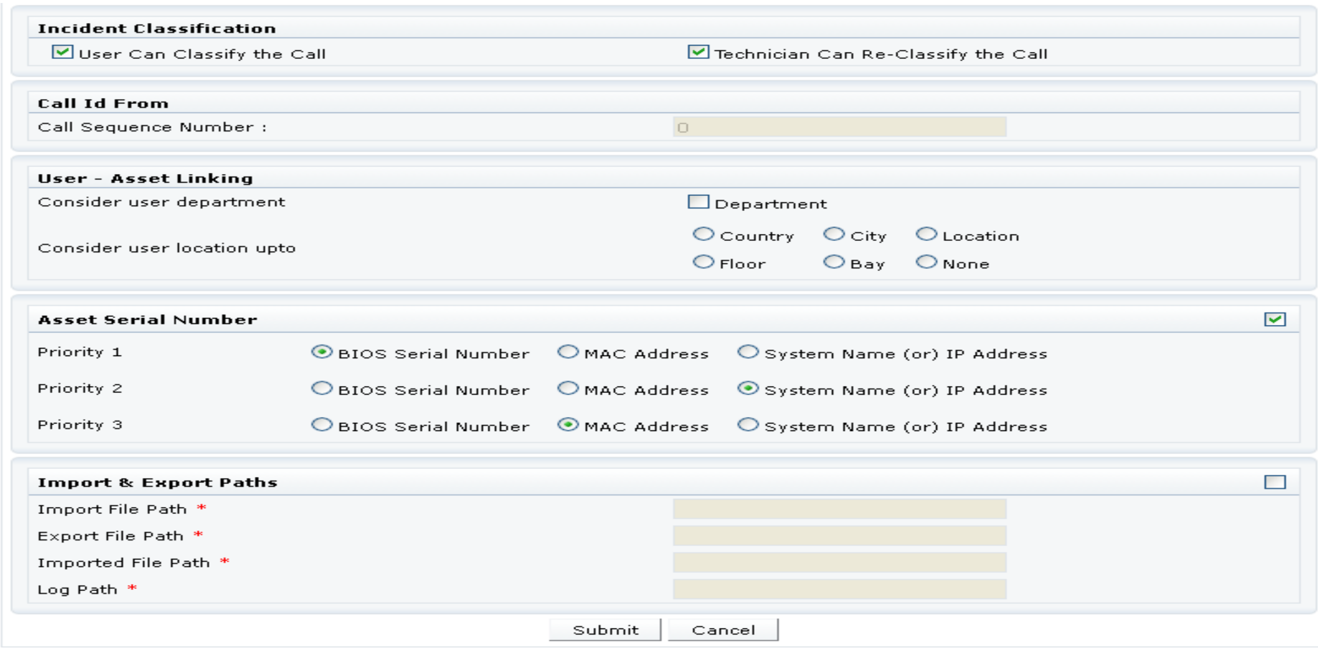
3. Enter the Time Interval For Tasks (Timer Application).
4. To save a setting: Click Set Preferences Button to save the settings.

Settings

The various settings required for performing certain functionality in the application are listed below

1. Knowledge base updates permission.
2. FAQ update permission.
3. Service desk and Technician permission.
4. Call Id Sequence number.
5. User-Asset linking settings.
6. Import/ Export path.
7. Time intervals for Importing and Exporting.





Knowledge base and FAQ update permission

1. The permissions for updating the knowledge base and FAQ are set in this menu.
2. Enable the check box for the roles for which the update permission is to be enabled.

Service desk and Technician permission

1. Options are provided to the technician for updating the call and for altering the date and time.
2. Enable the check box for technician and service desk for various call update permissions

Service Desk completion status

1. Enable the check box “Show completed calls in service desk” , so that the calls with the status completed will be displayed in the Service desk grid

2. Enable the check box “Send mails to service desk” in order to send a mail alert to the service desk for all the status of the call.

Incident Classification

The automated service desk functionality brings into the process of call logging self-automated. Once the call is classified by the user, the calls are automatically sent to the technician/support person. Technician can also re-classify the call, if the classification selected by the user is in-appropriate

1. Enable “User can classify the call” in order to give the permission to classify the calls
2. Enable “Technician can re-classify the call” to change the call classification selected by the user.

Call Id sequence

The administrator has the provision to set the call Id sequence number. For example if the call id has to be started from id 100, he can set the call sequence number as 100.

User-Asset linking

This feature enables administrator to customize user-asset linking according to various considerations like department, country, city, floor etc. So it is not mandatory to link the assets and user manually. The asset description will be listed according to various Considerations set by the administrator.

Asset Serial Number

This setting enables the administrator to select the priority for capturing the Asset Serial Number of an Asset. Based on the priority and options selected, the application will capture the information during Auto Discovery.

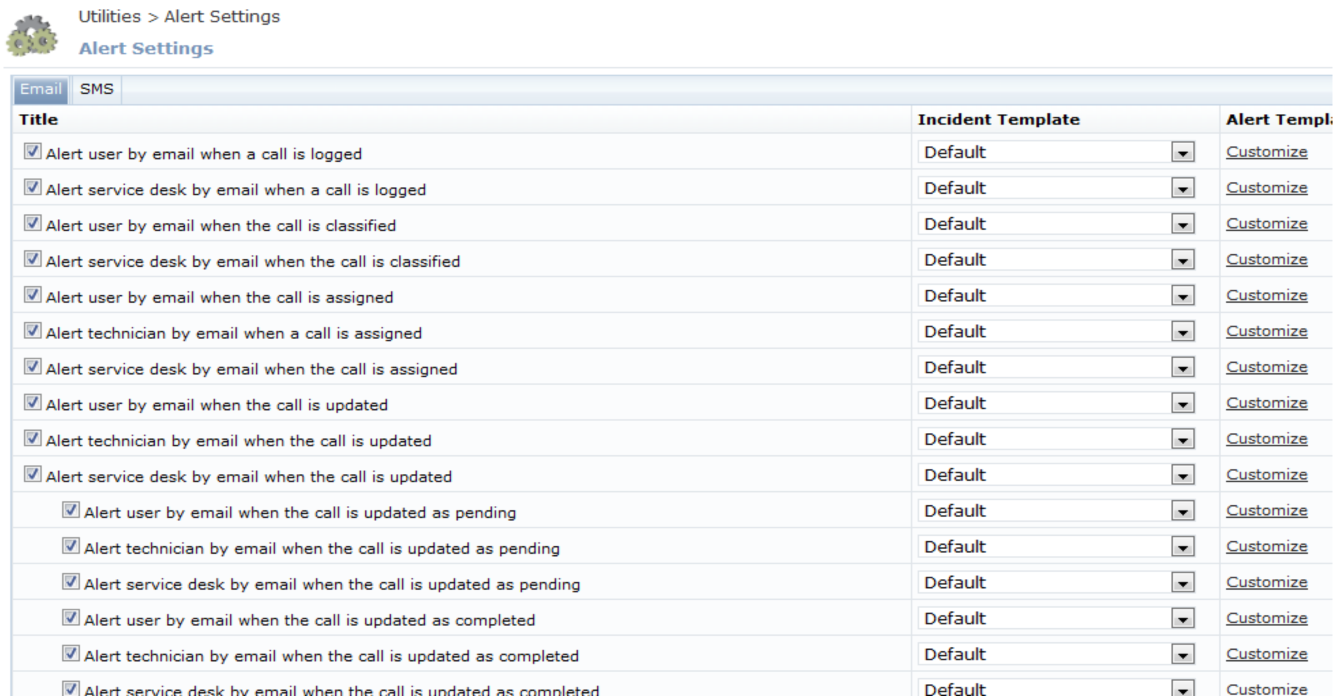
Import/Export paths

There are four file paths required for import, export, imported and log file path. All the four folders should be created in the server where InsTIL is installed and asp.net users should be added and given read, write and execute permission for that folder. Select the path where the respective folders are created in this menu.

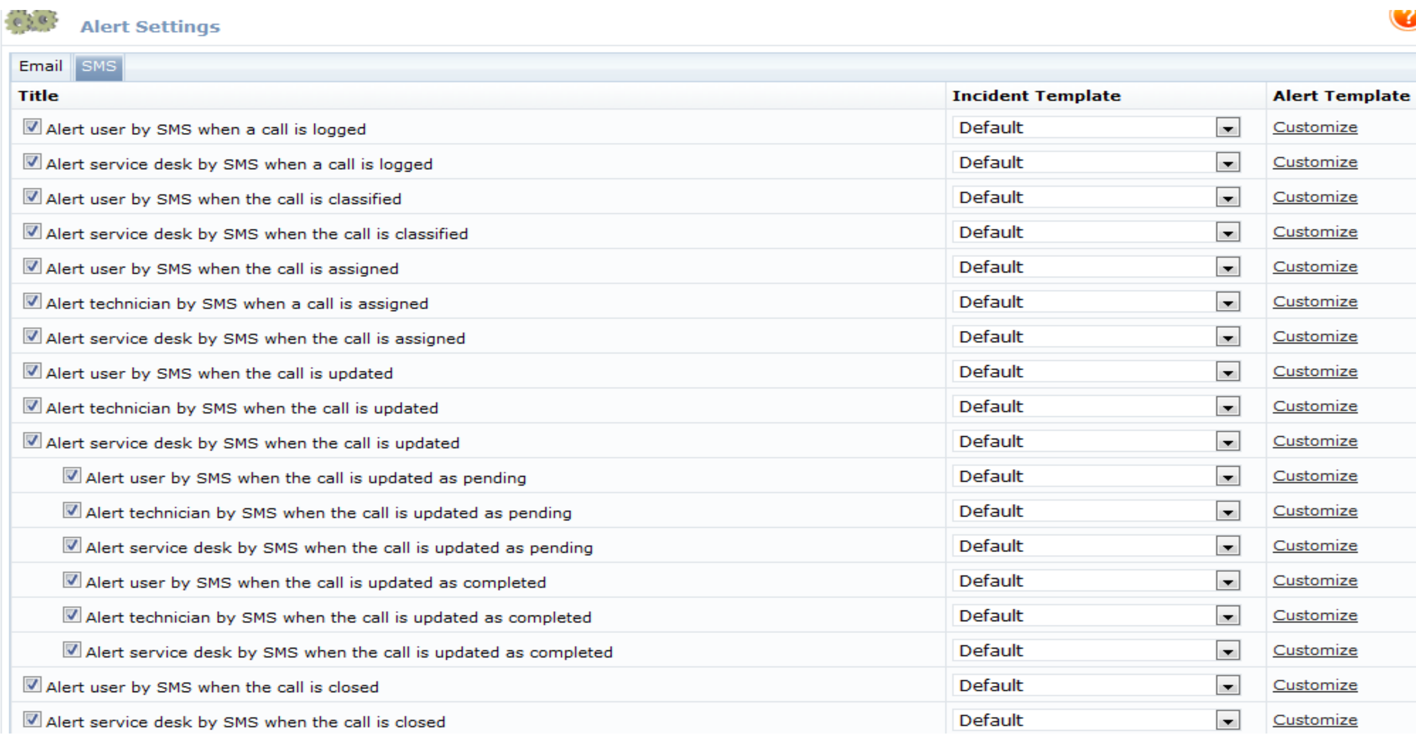
Alert Settings

This feature enables the administrator to customize the Email and SMS content for various call status available in the application. The administrator can edit the content of the Email/SMS by selecting the default fields available in the Incident lifecycle and also an option is provided to type certain information to be triggered along with the Email/SM.

An example is shown below for the customization of the Email content to be triggered throughout the incident lifecycle.

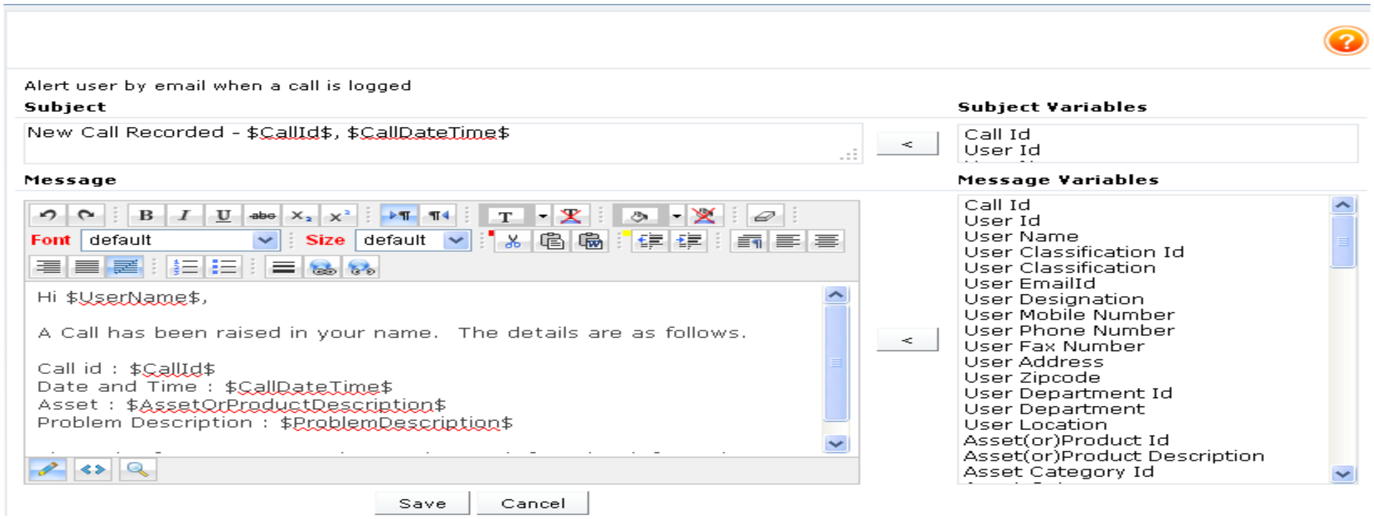


An example is shown below for the customization of the SMS content to be triggered throughout the incident lifecycle.



Operation – Email Alert

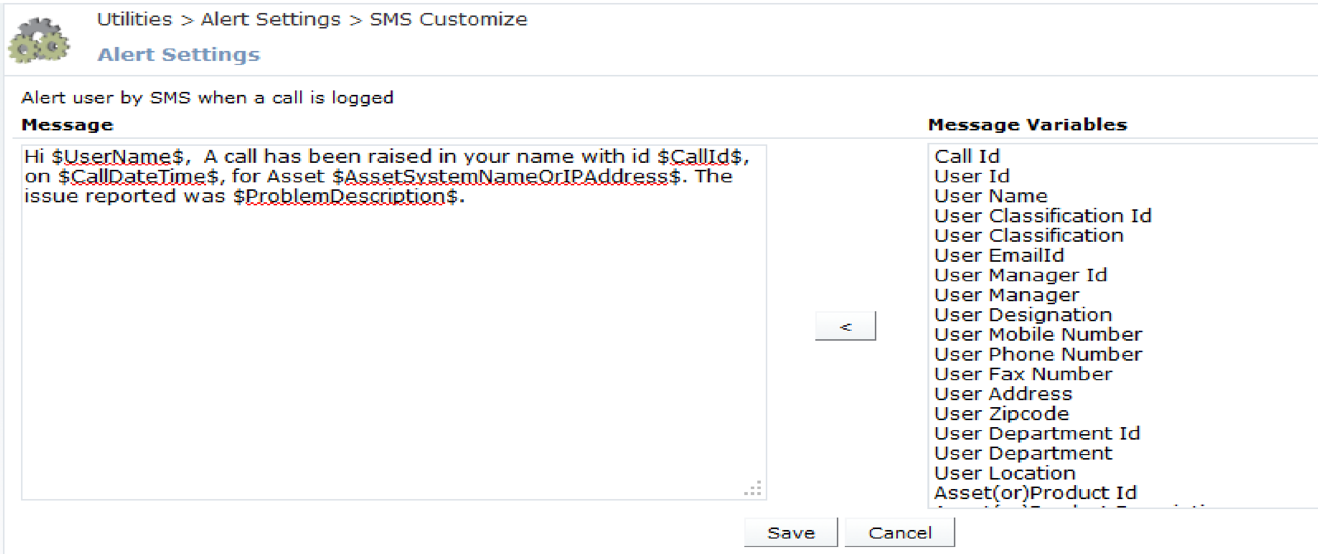
The default fields that can be added in the subject line are listed in the subject variables. The content in the subject line and also the message to be triggered can be modified in the following steps. Similarly the customizations can be done for all call status available in the application and also based on roles like Service Desk, Technician and User depending on the workflow defined.



1. Select the fields one by one from the subject variable list that you want to be displayed and click < button, the fields selected are automatically transferred to the subject line
2. Make the required modifications and type any text information if required
3. Select the fields one by one from the message variable list and when < button is clicked the selected field are transferred to the message line and make any modifications where the variable has to be displayed based on the priority.
4. Click Save to save the modifications made.

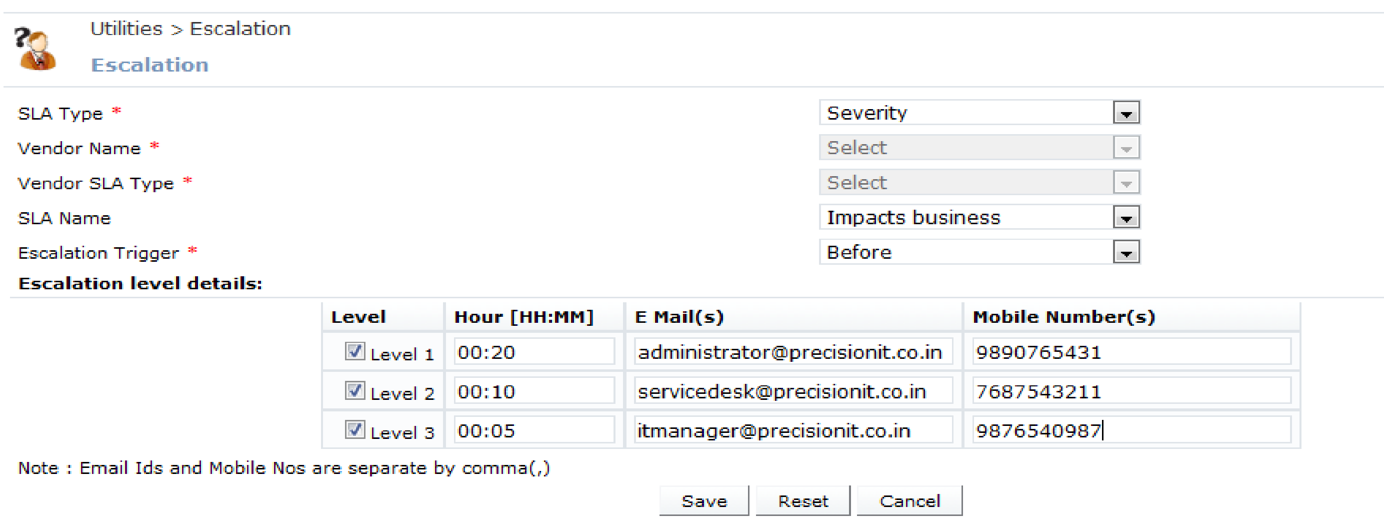
Operation - SMS Alert

The SMS trigger facility is enabled for all the call status throughout the Incident lifecycle. By default a predefined content is given in the message column and the administrator is provided the option to edit the content of the message to be trigerred.



Escalation

This feature enables the administrator to escalate the higher officials, if the problem intimated by the user is not responded or resolved within the stipulated time frame. Escalation is available for the Asset – Internal, Asset – External, Severity and the User. Levels (1, 2 and 3) are assigned for each of the SLA types. When the percentage time mentioned in the Level exceeds, the incident will be escalated according to the matrix defined and alert sent through SMS/Email.

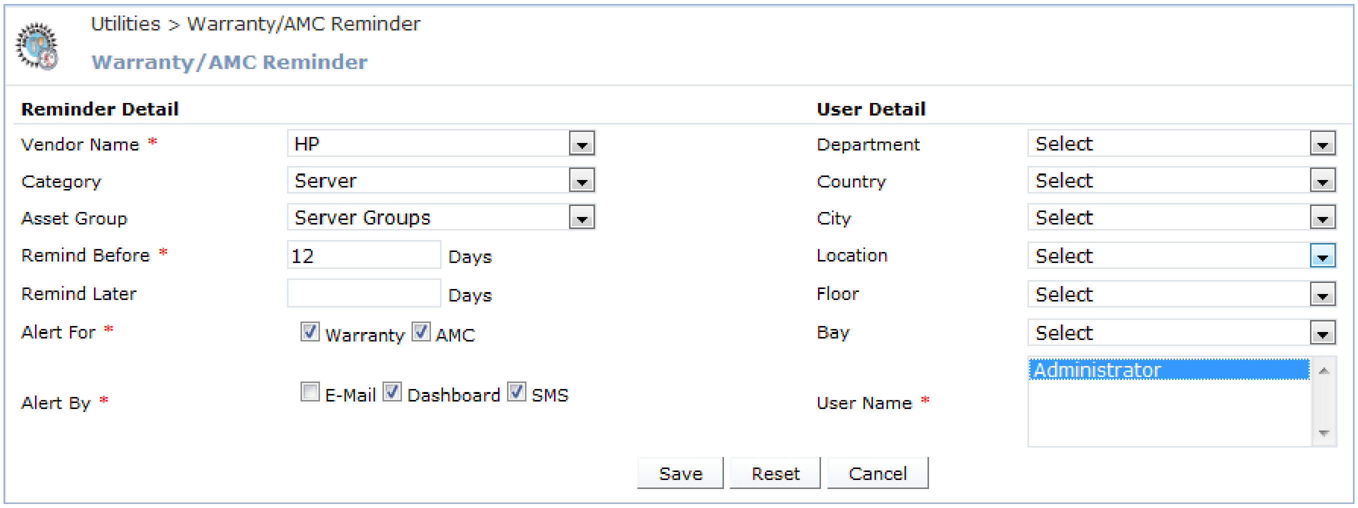


Operation

1. Click New
2. Select the SLA type – There are four SLA type – Asset Internal (Asset group), Asset External (Vendor), Severity and User SLA.
3. If SLA type is selected as Asset External
a. Select vendor name from the dropdown list
b. Select the Vendor SLA type as Device or Call Category for which the SLA is fixed in the vendor master
4. Select SLA name from the dropdown list
5. Select the Escalation trigger – Example – Before and After - The SLA can be triggered before the response and resolution type and after the response and resolution time
6. Enable the checkbox and define the time interval at which the alert is to be triggered.
7. Enter the Email id and Mobile number information in the respective column.
8. Click Save button to save the record created
9. Click Reset button to reset the entries.
10. Click Cancel button to cancel the process

Warranty / AMC Reminder

Reminders are set for whom, when and where the application should remind for Warrant/AMC expiry dates.

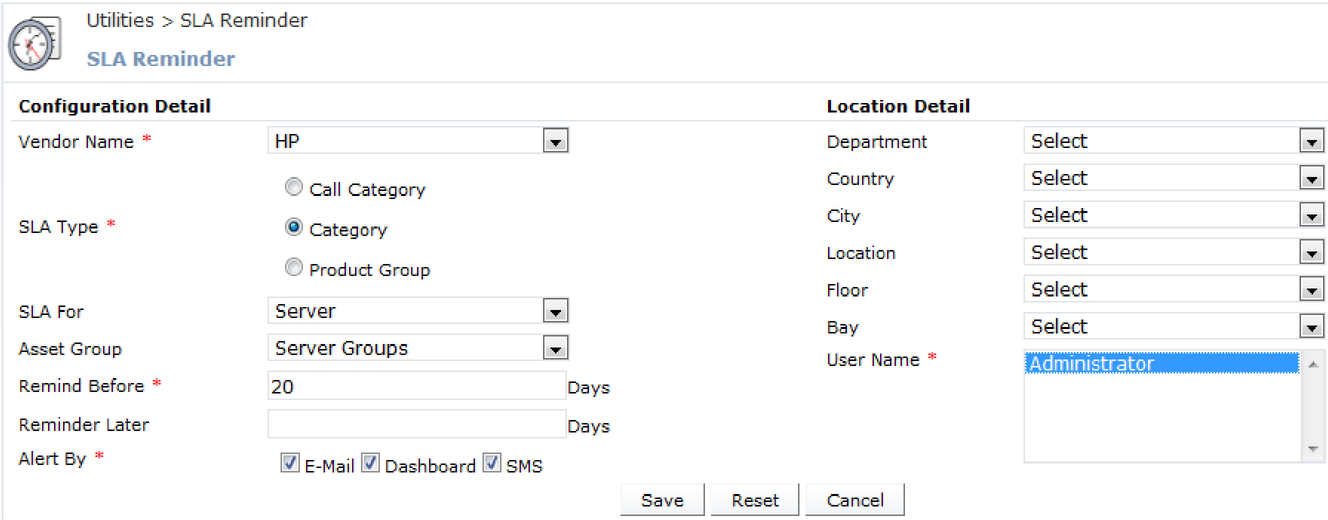


Operation

1. Click New
2. Select the Vendor Name from where the Asset has been purchased
3. Select the Category name of the Asset for the selected vendor
4. Select the Asset group for the Asset
5. The Reminder can be set before and after the expiry date
6. Select the location detail of the Asset using the filtering option
7. Select whether the Reminder is to set for Warranty/AMC
8. Select Alert By as E-Mail/Dashboard/SMS
9. Select the user names whom the reminder has to be triggered
10. Click Save button to save the record created
11. Click Reset button to reset the entries.
12. Click Cancel button to cancel the process

SLA Reminder

Reminders are set for SLA expiry dates. When the SLA of the Vendor is about to expire a reminder is triggered in the Dashboard, E-mail/SMS alerts to the user.



Operation

1. Click New
2. Select the Vendor Name
3. Select the SLA type as Device Category or Call Category

a. If SLA type is selected as Device category, then select Laptop or Desktop from the SLA For dropdown list

b. If SLA is selected as Call Category, then select Hardware or Application from the SLA For dropdown list

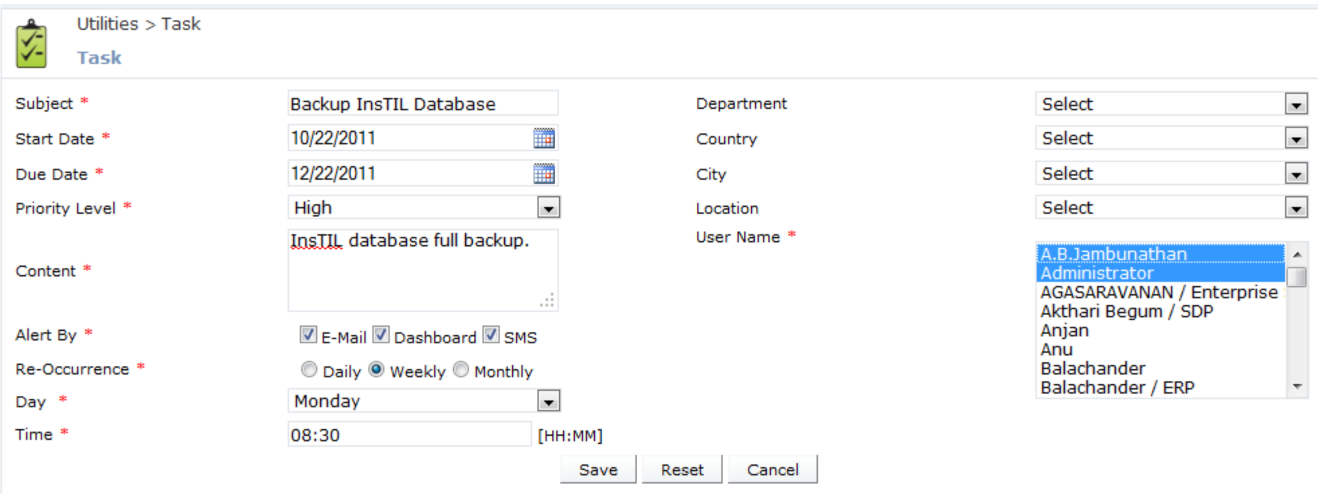
4. Select the Asset group for the selected vendor
5. The Reminder can be set before the expiry date of the SLA
6. The option is provided for setting a second reminder
7. Select the location detail of the Asset
8. Select Alert By as E-Mail/Dashboard/SMS
9. Select the user names whom the reminder has to be triggered
10. Click Save button to save the record created
11. Click Reset button to reset the entries.
12. Click Cancel button to cancel the process

Task

Task can be created and assigned to self and groups. Some of them include:

1. Backup Tasks.
2. Preventive maintenance task.
3. Information on meeting. Etc
4. Re-occurrence is set for Daily, Weekly and Monthly frequencies.

5. The screen for setting task is shown below



Operation:

1. Click New
2. Enter the Subject – Brief outline of the task to be set
3. Enter the From Date – The task will be triggered starting from this date
4. Enter the Due Date of the task
5. Set the Priority level – High, Medium and Low
6. Enter the Content of the Task
7. Select Alert By as E-Mail/Dashboard/SMS
8. Select the frequency of occurrence of the task- daily, weekly or monthly
9. Select the user names whom the reminder has to be triggered
10. For selecting the department in a particular location:

a) Select the Department name.

b) Select the Country Name.

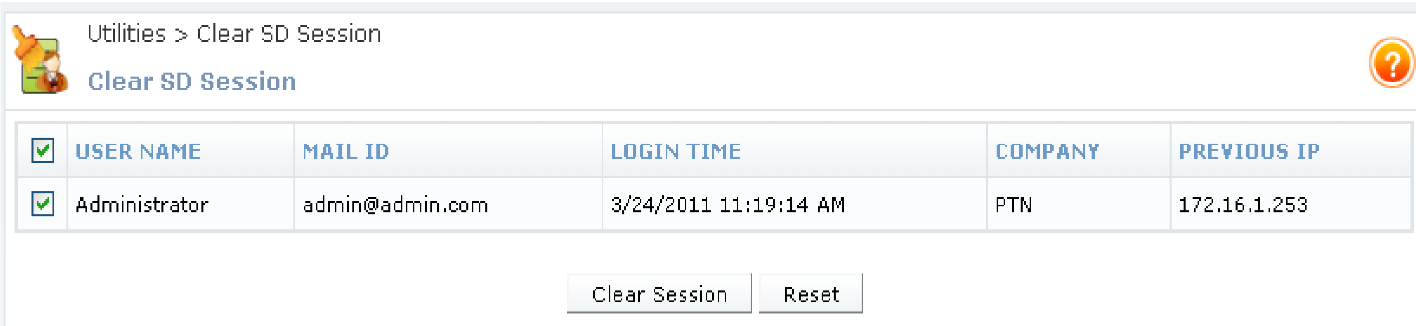
c) Select the City Name.

d) Select the Location name.

11. Click Save button to save the record created
12. Click Reset button to reset the entries.
13. Click Cancel button to cancel the process.

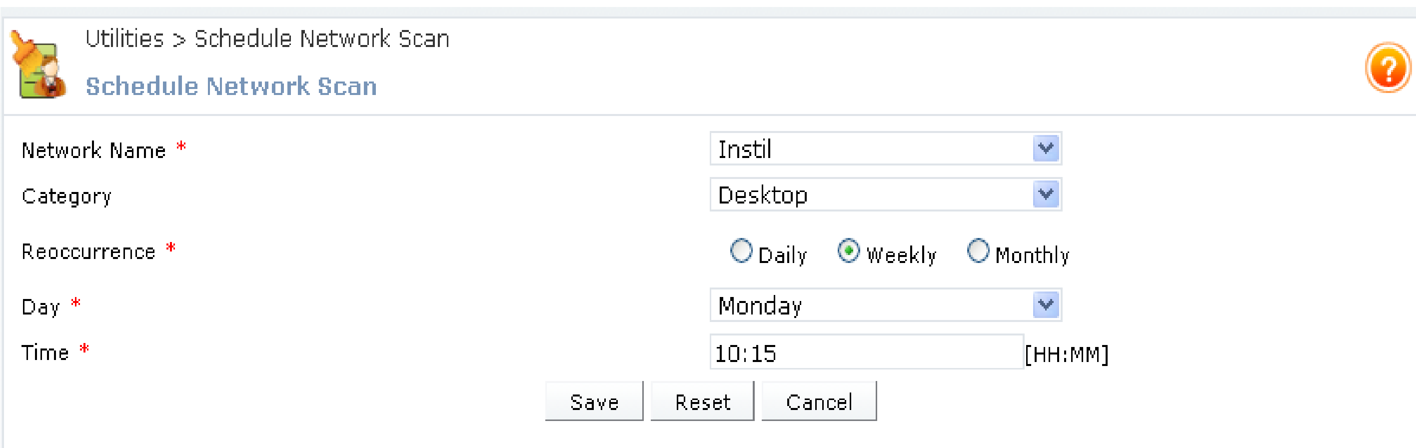
Clear SD Session

When the number of Service desk logins exceeds the license limit or if the Service desk session gets timed out, then the SD will be unable to login to the application. This feature enables to clear the session if the number of SD logins is locked.



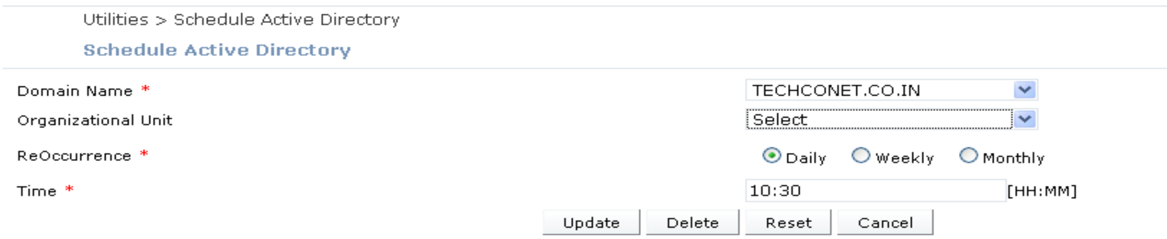
Schedule Network Scan

This feature enables the user to run a routine scan on a specified network on a specific schedule. To enable the Scheduled Auto Discovery function, login as administrator, click "**Schedule scan**" in Utilities. Click on "**Add New Schedule** "tab and enter the network name, category & Schedule details. A sample screen is shown below;



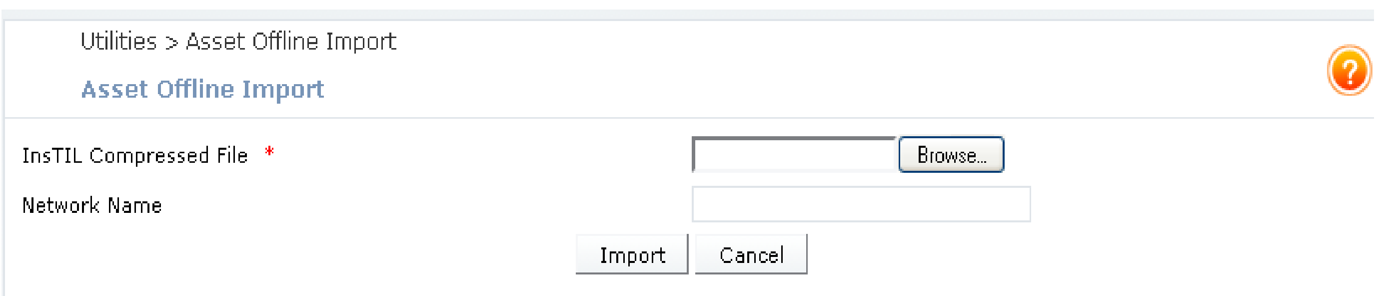
Schedule Active Directory

This feature enables the user to run a routine scan on a specified network on a specific schedule. To enable the Scheduled Active Directory function, login as administrator, click "**Schedule Active Directory**" in Utilities. Click on "**Add New** "tab and enter the Domain name, Organizational & Scheduled details. A sample screen is shown below;



Asset Offline Import

Auto Discovery of Assets can be performed in two modes Online & Off-line. During an online mode the Assets would be discovered through the InsTIL Server where the connectivity to the server is said to exist, in other words it is said to be an online discovery. However if the administrator has to discover the assets from another location situated outside the LAN, the offline discovery is suggested as the best feasible option. The functioning of the Offline tool is similar to the network scan. For detailed procedure on how to perform an Offline discovery, refer to Offline Discovery Manual. This feature enables the administrator to import the asset information into the InsTIL server.



Operation

1. Click on Utilities → Asset Offline Import
2. Click on Browse → Select the file named .InsTIL
3. The network name will automatically be displayed, based on the file selected.
4. Click on Import to complete the process.

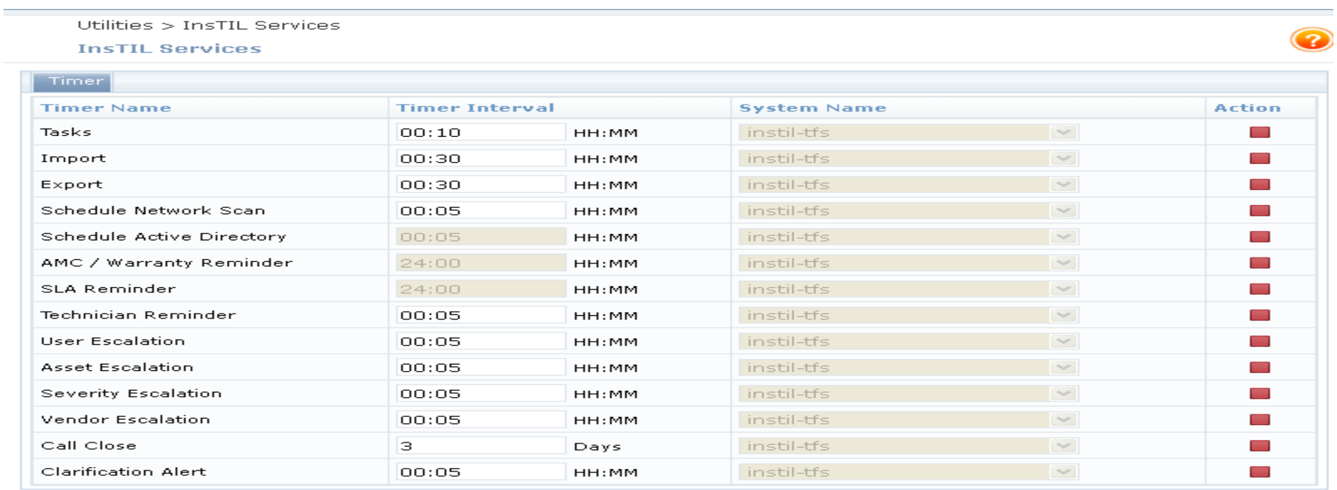
InsTIL Services

All the services in InsTIL are configured in this particular screen which enables certain triggers as defined in the product functionality

Operation

To enable a particular service perform the following task

1. Select the system name where the InsTIL Timer application is configured and select the Start button



Timer Name	Timer Interval		System Name	Action
Tasks	00:10	HH:MM	instil-tfs	
Import	00:30	HH:MM	instil-tfs	
Export	00:30	HH:MM	instil-tfs	
Schedule Network Scan	00:05	HH:MM	instil-tfs	
Schedule Active Directory	00:05	HH:MM	instil-tfs	
AMC / Warranty Reminder	24:00	HH:MM	instil-tfs	
SLA Reminder	24:00	HH:MM	instil-tfs	
Technician Reminder	00:05	HH:MM	instil-tfs	
User Escalation	00:05	HH:MM	instil-tfs	
Asset Escalation	00:05	HH:MM	instil-tfs	
Severity Escalation	00:05	HH:MM	instil-tfs	
Vendor Escalation	00:05	HH:MM	instil-tfs	
Call Close	3	Days	instil-tfs	
Clarification Alert	00:05	HH:MM	instil-tfs	

Reports

InsTIL application has the option to generate reports related to the Asset, Call Details, Escalation and Alerts and Notifications. These reports can be viewed in detail for various types of grouping which are provided in the application. The available reports can be scheduled in Reoccurrence type of Daily, Weekly and Monthly and reports triggered to various roles in the application.

The reports related to Assets includes

Asset

1. Asset detail

- Asset linking
- Asset group
- Brand
- Department
- Category
- Location
- User classification
- User linking
- Vendor

2. AMC Reminder

- Asset group
- Category
- Brand
- Department
- Location
- Vendor

3. Warranty Expiry

- Asset group
- Category
- Brand
- Department
- Location
- Vendor

4. Asset Transfer

5. Asset Physical verification report

6. Baseline report

User

User Detail – The user details can be viewed using this group

Call Analysis

1. Call Details

The reports related to Call Analysis includes

1. Incident – Time wise – Based on priority, call type and user

2. Incident – Day wise - Based on priority, call type and user

3. Incident – Monthly - Based on priority, call type and user

4. Call Detail

- Asset
- Call category
- Call origin
- Call status
- Technician status
- Call analysis
- Technician performance
- FLS report
- Maximum Calls – Asset
- Maximum Calls– Call category
- Maximum Calls – Duration
- Maximum Calls – Engineer
- Maximum Calls – User
- Re-occurrence
- Wrong classification
- User
- Time sheet
- Call Summary
- Call Priority Summary
- Technician Pending calls
- Technician call summary
- Category based calls

- SLA Report
- Deviated/Pending calls – Engineer wise
- Incident at a glance report
- Summary reports
- Location wise call report
- Periodical call report

SLA Analysis

1. SLA analysis

IT –Organization

1. Attendance report

Alerts and Notification

1. AMC/Warranty and SLA reminders
2. Task reminders
3. Escalation Details
4. SMS

Monitoring Reports

All Devices (11 Reports)

This section provide a graphical representation of a complete set of Availability, Health status & Interface Monitoring reports for all categories based on the CPU Utilization, Memory Utilization, Disk Utilization, Incoming Traffic, Outgoing Traffic, Incoming Error, Outgoing Error, Traffic Utilization(R_x - incoming), Traffic Utilization(T_x - outgoing), Total Bandwidth & Availability Report parameters.

1. Desktop (11 Reports)

This section provide a graphical representation of complete set of Availability, Health status & Interface Monitoring reports for Desktop category based on the CPU Utilization, Memory Utilization, Disk Utilization, Incoming Traffic, Outgoing Traffic, Incoming Error, Outgoing Error, Traffic Utilization(R_x - incoming), Traffic Utilization(T_x - outgoing), Total Bandwidth & Availability Report parameters.

2. Servers (9 Reports)

   This section provide a graphical representation of complete set of Availability, Health status & Interface Monitoring reports for Server category based on the CPU Utilization, Memory Utilization, Disk Utilization, Incoming Traffic, Outgoing Traffic, Traffic Utilization(R_x - incoming), Traffic Utilization(T_x - outgoing), Total Bandwidth & Availability Report parameters.

3. Domain Controllers (9 Reports)

   This section provide a graphical representation of complete set of Availability, Health status & Interface Monitoring reports for Domain Controllers category based on the CPU Utilization, Memory Utilization, Disk Utilization, Incoming Traffic, Outgoing Traffic, Traffic Utilization(R_x - incoming), Traffic Utilization(T_x - outgoing), Total Bandwidth & Availability Report parameters.

4. Routers (10 Reports)

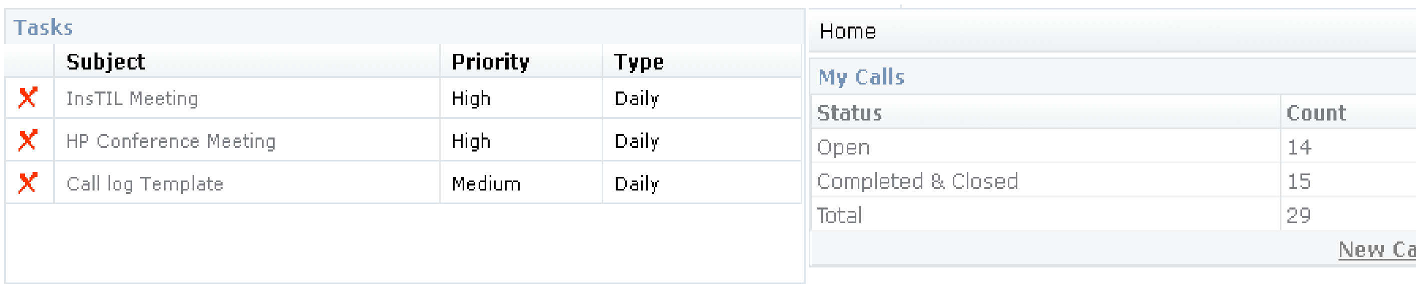
   This section provide a graphical representation of complete set of Availability, Health status & Interface Monitoring reports for Routers based on the CPU Utilization$^+$, Memory Utilization$^+$, Incoming Traffic, Outgoing Traffic, Incoming Error, Outgoing Error, Traffic Utilization(R_x - incoming), Traffic Utilization(T_x - outgoing), Total Bandwidth & Availability Report parameters.

5. Switches (8 Reports)

   This section provide a graphical representation of complete set of Availability, Health status & Interface Monitoring reports for Switches based on the Incoming Traffic, Outgoing Traffic, Incoming Error, Outgoing Error, Traffic Utilization(R_x - incoming), Traffic Utilization(T_x - outgoing), Total Bandwidth & Availability Report parameters.

5.0 Logging in as User

Every user within or outside the organization is provided a user id and password by the administrator and can login the application as an ordinary user or domain user. This helps the users to log in their complaints and the user is also given the permission to classify the call based on the complaints. The calls are then automatically assigned to the technician on the basis of the rule created by the Administrator. On each stages of the call the user is alerted with an e-mail defining the status of the call. The user can also log the call with the service desk, and the service desk in turns assigns the call to the technician for response and resolution. The user can also select template based on which the call has to be logged.



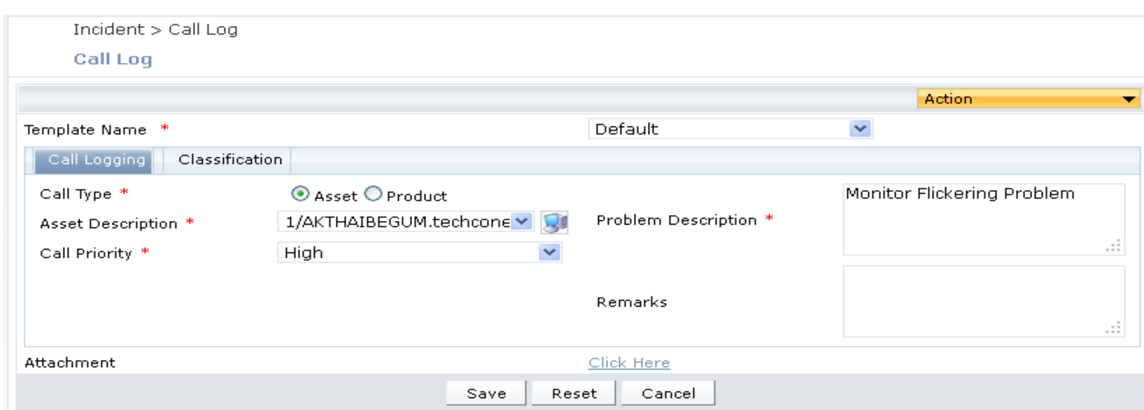
Incident

Call Log

This feature allows users to log in a service request or an incident with a proper description and also with a priority for the Service Desk to process accordingly. The user can add an attachment w.r.t to the incident logged. InsTIL also provides an option for the user to classify the call and based on the classification defined the calls are automatically assigned to the Technician.

Operation

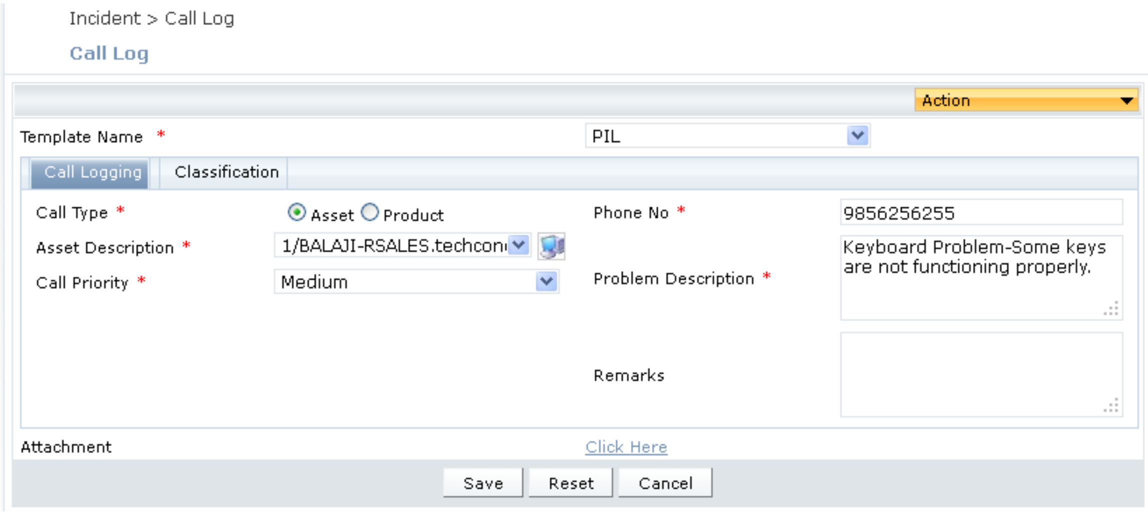
To add a new call perform the following tasks



Operation

1. Click New
2. Select the call type as Asset or Product
3. The asset description is automatically selected if the asset is linked to the user. If asset-user linking is not done select the asset from the drop down list
4. From the drop down list, select the priority at which the service needs to be attended.
5. The user can type the problem or the service request that needs to be solved.
6. Any additional information related to the problem can be provided in the Remarks column.
7. Click on Click Here link to add an attachment.
8. Click Save button to save the record created
9. Click Reset button to reset the entries.
10. Click Cancel button to cancel the process

Call Logging based on the default template



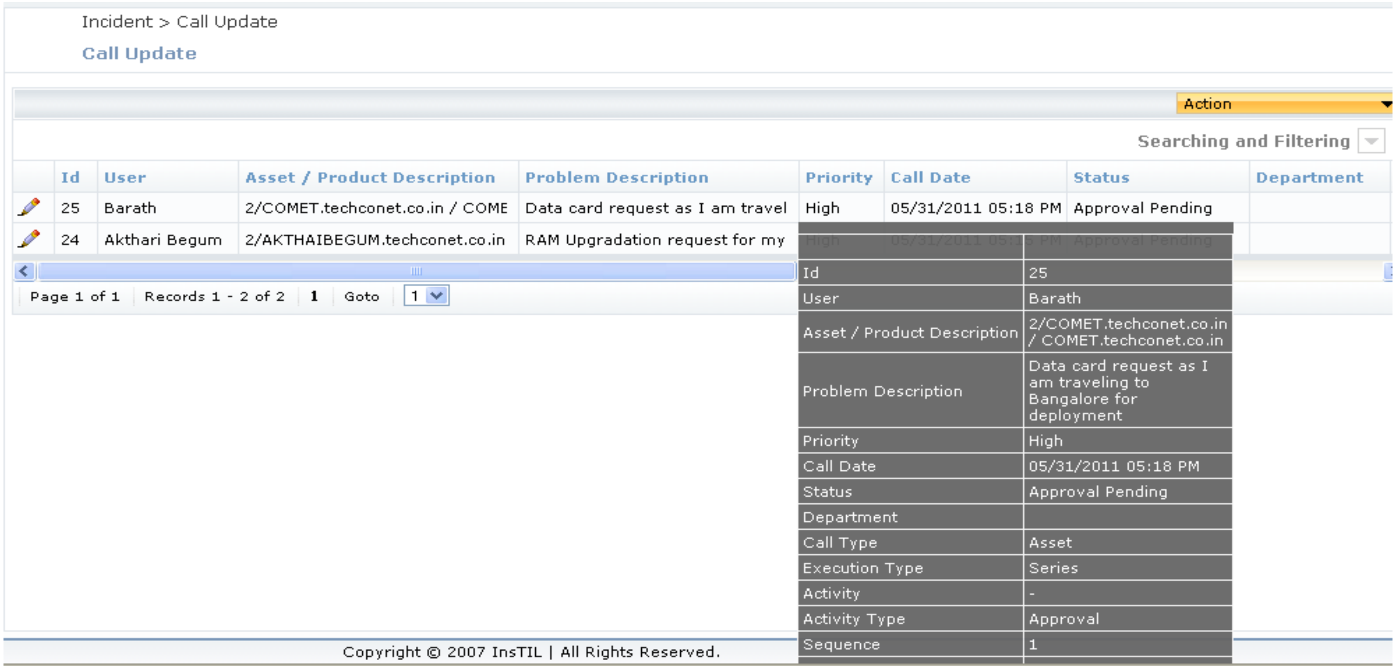
Operation

1. Click New to login an incident or service request.
2. Select the template name from the dropdown list for which the call is to be logged.
3. From the drop down list of Product Description, select your particular product.
4. The user can type the problem or the service request that needs to be solved.
5. Any additional information related to the problem can be provided in the Remarks column.
6. An attachment can also be added with the call logged.
7. Click Save button to save the record created
8. Click Reset button to reset the entries.

9. Click Cancel button to cancel the process

Call Update

The Call update menu is enabled for the User for to view the calls assigned to him for the approval. The user based on the rights assigned to him does either approve or reject the request.



Operation

1. Select the call id from the grid
2. Select the approval status as Approved or Rejected
3. Select the Approved Date and Time
4. Provide remarks if any

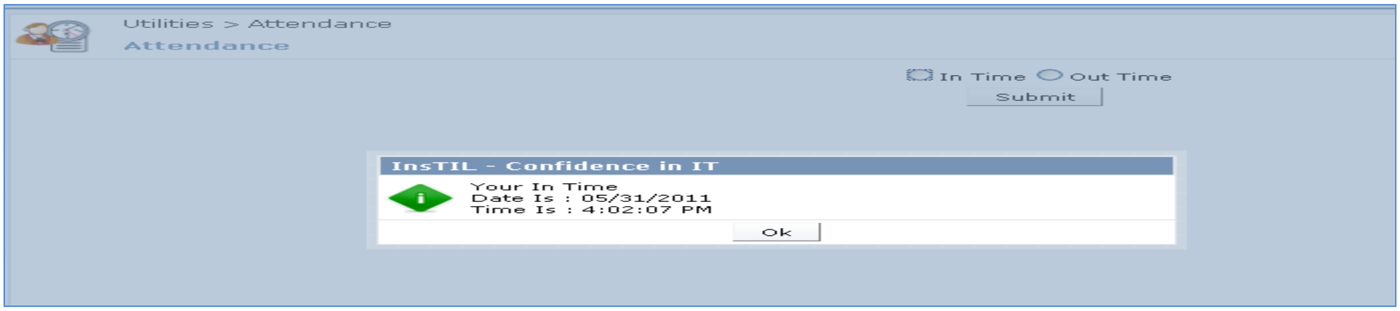
Utilities

Attendance

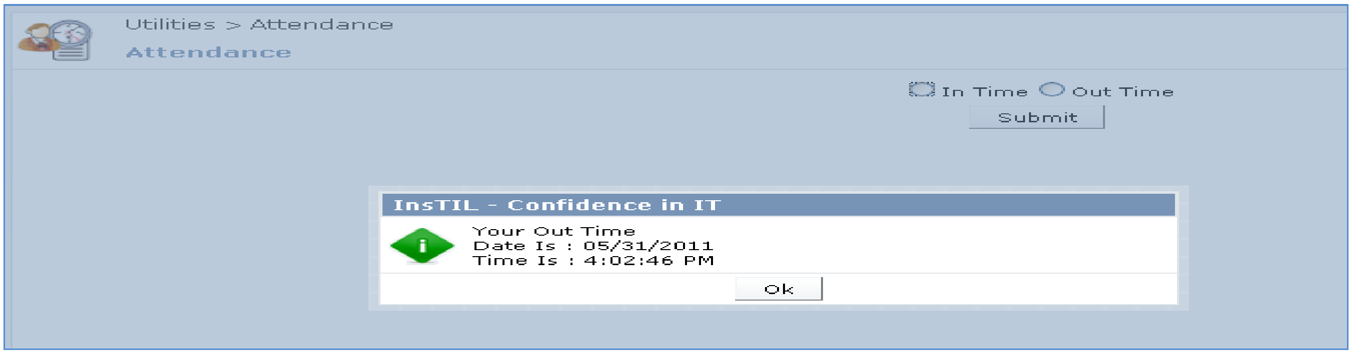
This feature enables the user to mark the Punch In time and Punch Out time for the particular day. This feature is made available for all the roles in InsTIL.

Operation

1. Select Punch In time and submit which marks the in time for the user

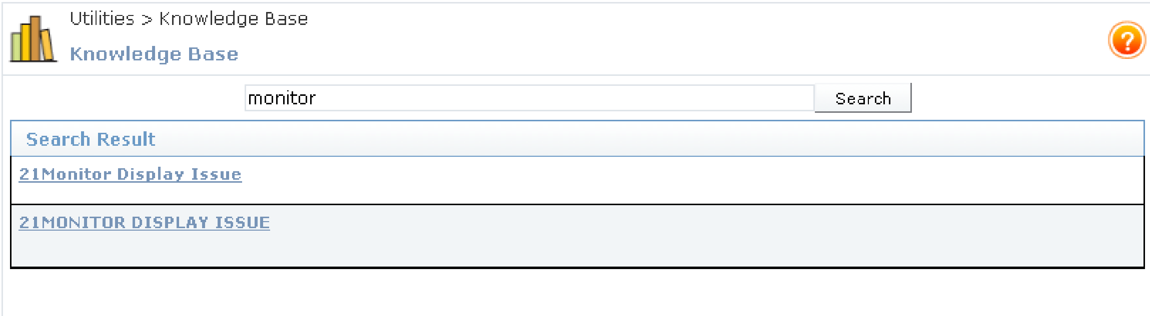


2. Similarly select Punch Out time and submit which marks the out time for the user.



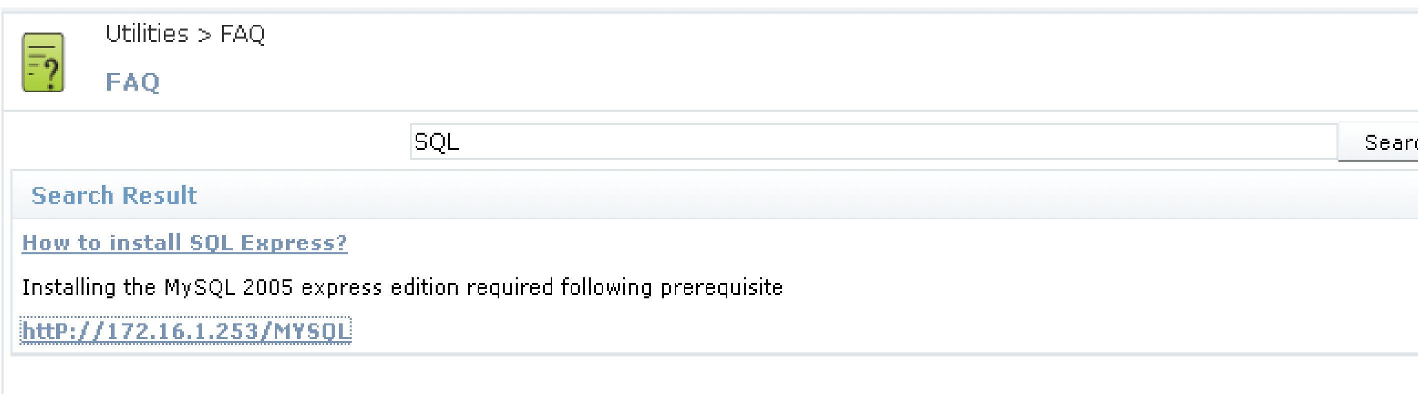
Knowledge Base

User is provided with the knowledge base option to search for Incidents and the resolution pertaining to the incident provided by the IT team. The user has the permission only to view information updated in the knowledge base by providing a suitable keyword and the information w.r.t keyword is populated for the User.



FAQ

FAQ is provided for the user to search for any documents or links which is added to the InsTIL FAQ by the administrator. The user can search by providing a particular keyword in the FAQ



Change Password

This screen is used to change the password which is used by the user to login to the application. Only local user's password can be changed by the administrator.

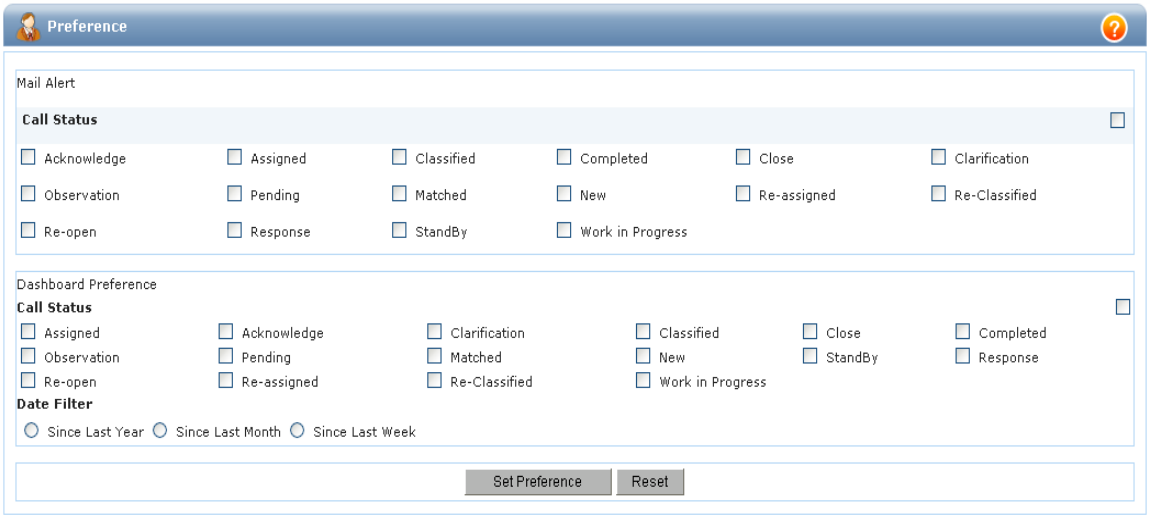
Operation

1. Select Change Password from the Utilities menu
2. Type the current password
3. Type the new password and confirm new password
4. Click change to save the new password created

Note: Domain User's password can be changed only in the ADS

Preferences

To set owner's favorite as default. It can be set by all categories (Administrator, User, Technician, IT manager, Service Desk) with their options provided. If the preferences are not set, the default settings are used. The screen for Preference is shown below.



Operation

Mail Alert - Call Status:

Select the call status such as Acknowledge, Assigned, and Classified etc., (Can choose either one or all). The users would receive mail alerts for the call status based on the preferences set.

Dashboard Preference - Call Status:

Select the call status such as Acknowledge, Assigned, Classified etc., (Can choose either one or all). The user's dashboard will have the call status displayed, based on the preferences set.

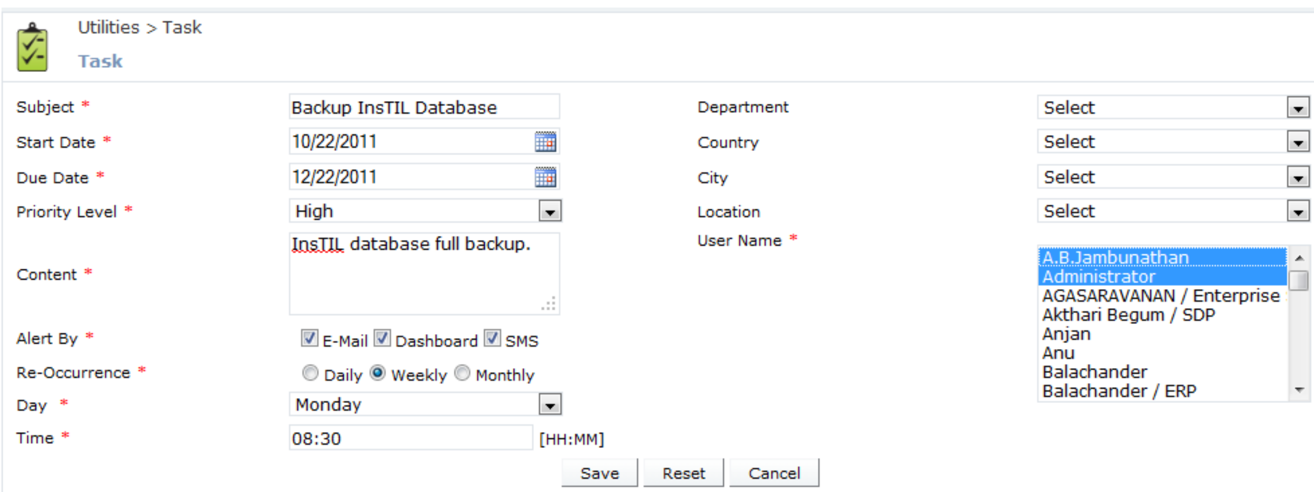
Date Filter

This feature enables the user to set preference for the calls logged by user on yearly, monthly or weekly basis.

Task

Task can be created and assigned to self and groups. Some of them include:

1. Backup Tasks.
2. Preventive maintenance task.
3. Information on meeting. Etc
4. Re-occurrence is set for Daily, Weekly and Monthly frequencies.



Operation:

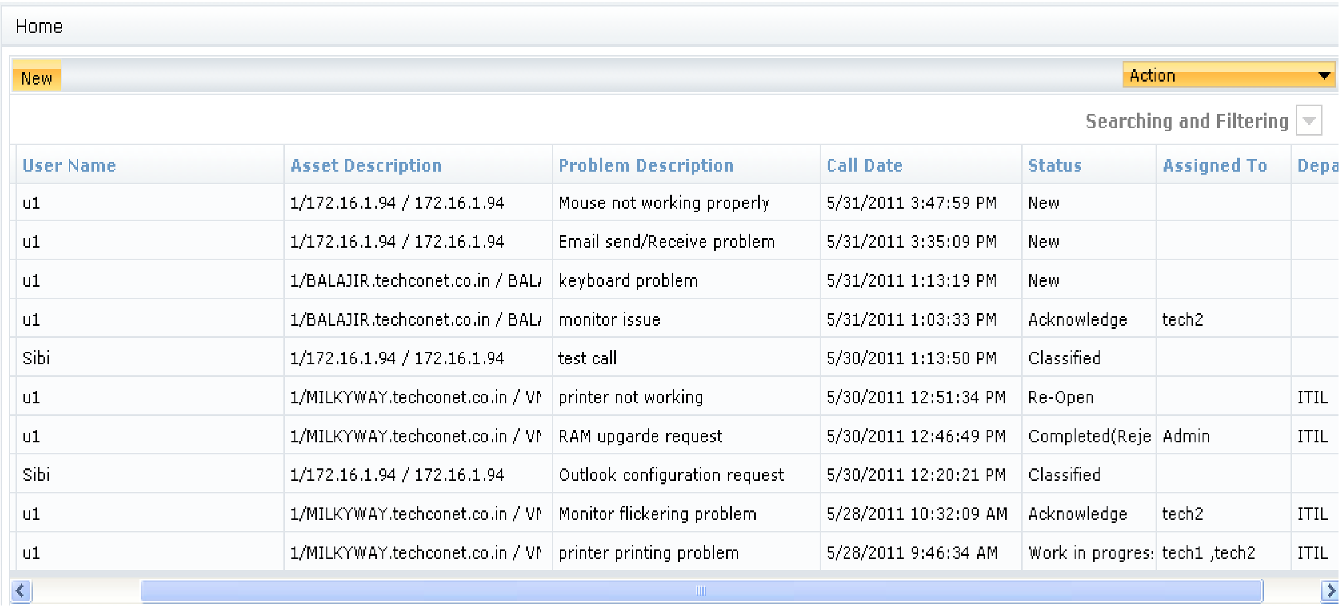
1. Click New
2. Enter the Subject – Brief outline of the task to be set
3. Enter the From Date – The task will be triggered starting from this date
4. Enter the Due Date of the task
5. Set the Priority level – High, Medium and Low
6. Enter the Content of the Task
7. Select Alert By - either through his dashboard or E-mail
8. Select the frequency of occurrence of the task- daily, weekly or monthly

9. Enter the time or day according to the re-occurrence
10. Select the user names whom the reminder has to be triggered
11. For selecting the department in a particular location:
e) Select the Department name.
f) Select the Country Name.
g) Select the City Name.
h) Select the Location name.

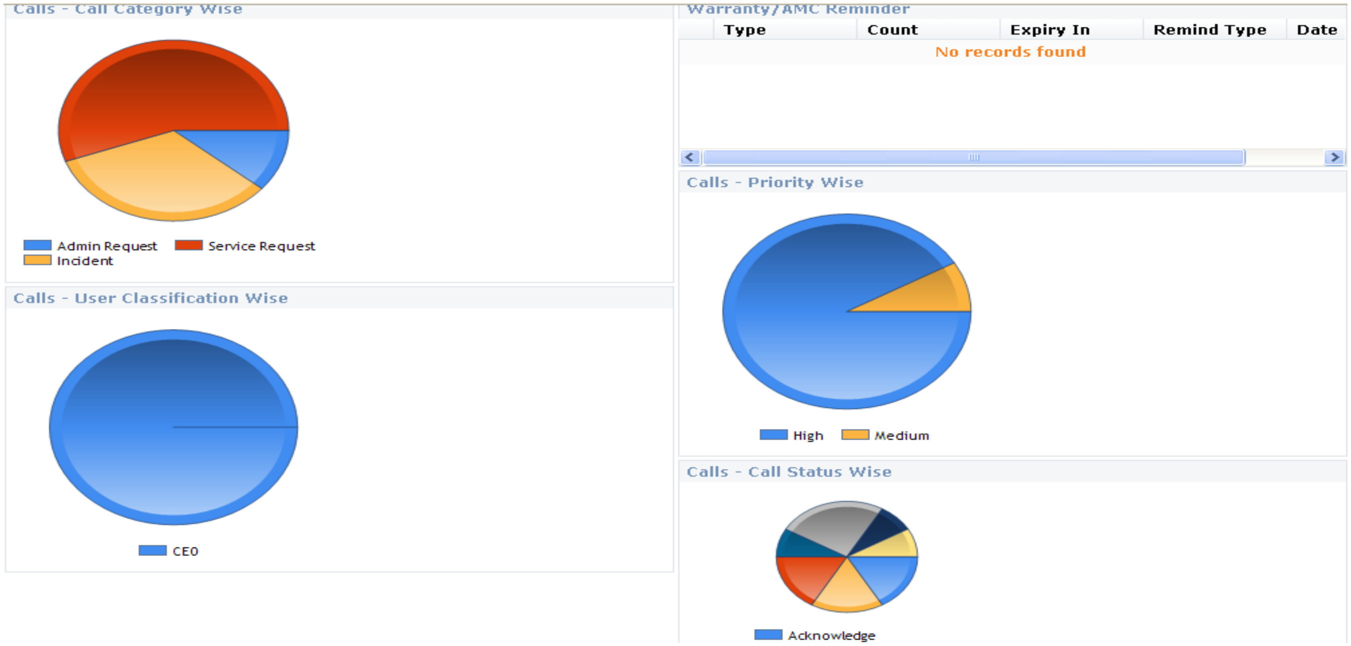
12. Click Save button to save the record created
13. Click Delete button to delete the record
14. Click Reset button to reset the entries.
15. Click Cancel button to cancel the process

6.0 Logging in as Service Desk

The Service Desk plays an important role in the application, the service desk can log calls on behalf of user, classify, assign/re-assign and update the calls. The incidents raised by the users are displayed in the home page of the Service Desk. Service Desk selects the particular call from the grid and assigns to the technician or Vendor. The service desk has the functionality to take the users system through remote and provide a first level solution to the issue raised and further updates the call. The service desk also has certain dashboard icons where he can view the call history, asset history, knowledge base and engineer statistics to analyze each calls. If the call logging process is self-automated, the Service desk will have its other functionality like call logging, classification, clarification and assign/re-assign process.



User Name	Asset Description	Problem Description	Call Date	Status	Assigned To	Depa
u1	1/172.16.1.94 / 172.16.1.94	Mouse not working properly	5/31/2011 3:47:59 PM	New		
u1	1/172.16.1.94 / 172.16.1.94	Email send/Receive problem	5/31/2011 3:35:09 PM	New		
u1	1/BALAJIR.techconet.co.in / BAL	keyboard problem	5/31/2011 1:13:19 PM	New		
u1	1/BALAJIR.techconet.co.in / BAL	monitor issue	5/31/2011 1:03:33 PM	Acknowledge	tech2	
Sibi	1/172.16.1.94 / 172.16.1.94	test call	5/30/2011 1:13:50 PM	Classified		
u1	1/MILKYWAY.techconet.co.in / VI	printer not working	5/30/2011 12:51:34 PM	Re-Open		ITIL
u1	1/MILKYWAY.techconet.co.in / VI	RAM upgarde request	5/30/2011 12:46:49 PM	Completed(Reje	Admin	ITIL
Sibi	1/172.16.1.94 / 172.16.1.94	Outlook configuration request	5/30/2011 12:20:21 PM	Classified		
u1	1/MILKYWAY.techconet.co.in / VI	Monitor flickering problem	5/28/2011 10:32:09 AM	Acknowledge	tech2	ITIL
u1	1/MILKYWAY.techconet.co.in / VI	printer printing problem	5/28/2011 9:46:34 AM	Work in progres	tech1 ,tech2	ITIL



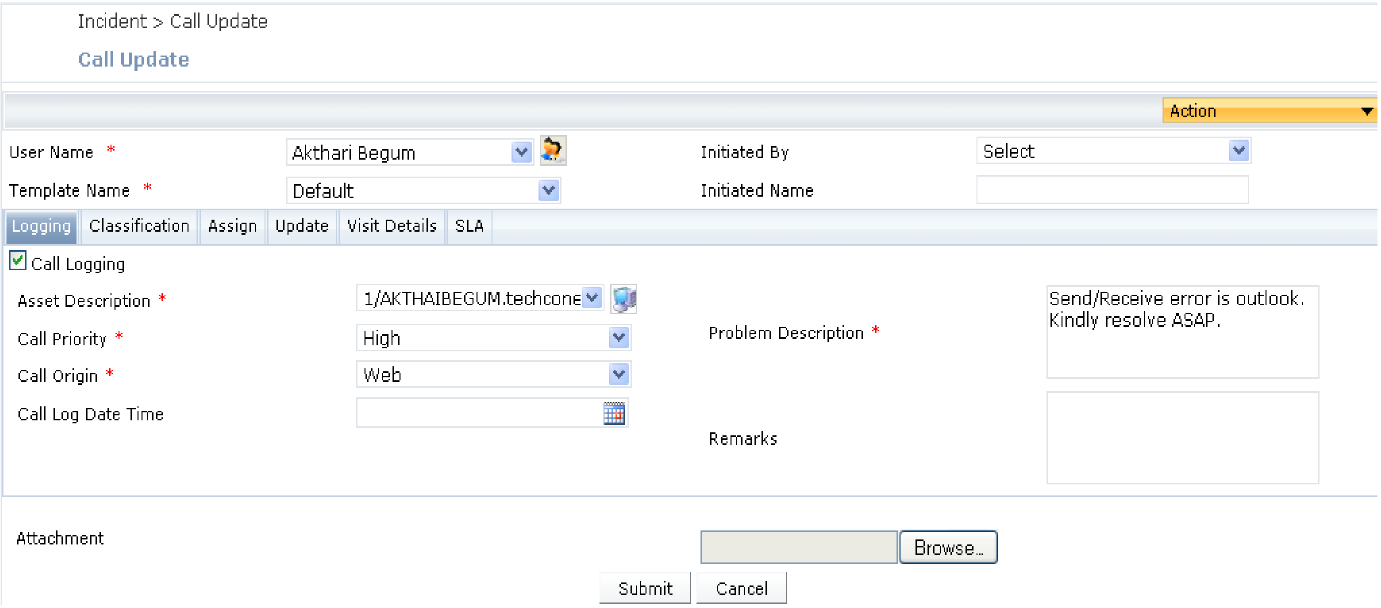
Service Desk - Incident

Call Logging

1. The call logging tab is automatically updated if the user logs the call directly.

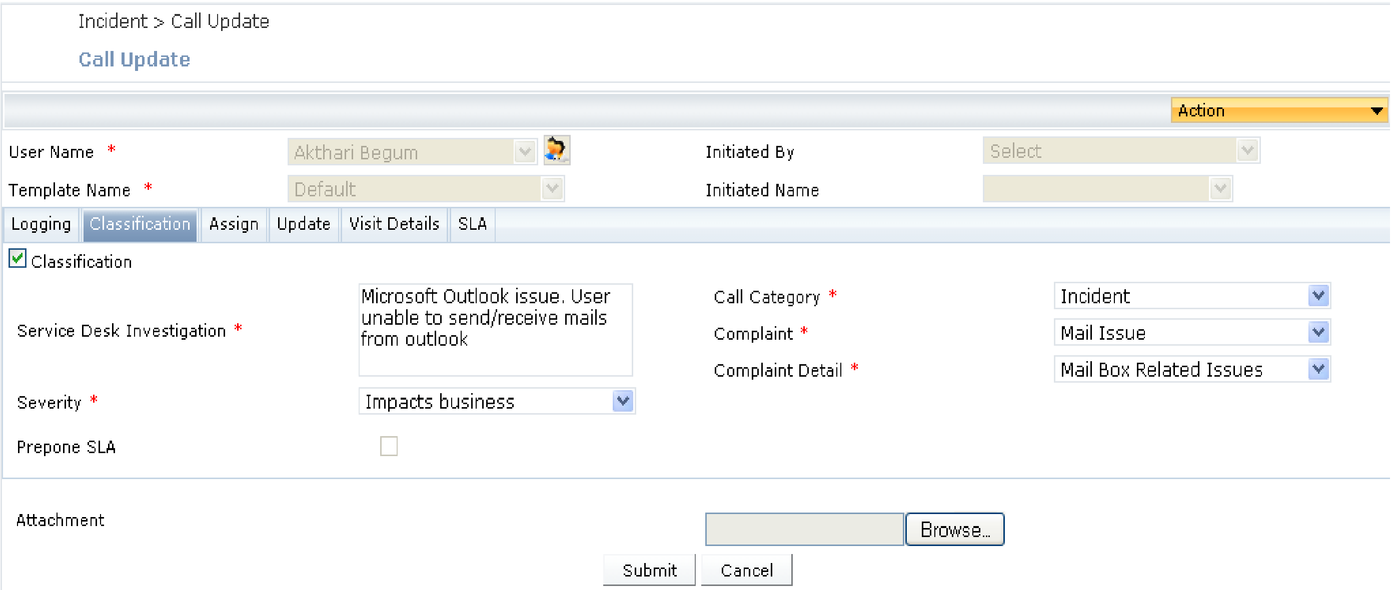
2. If SD logs the call on behalf of the user the following actions are performed.

a. Click New
b. Select the user name from the dropdown list – The initiator of the call
c. Select the Template name based on which the call is to be logged.
d. Select Call Logging check box.
e. Select the priority of the call- High, Medium and Low
f. Select the call origin – If the user logs the call through the InsTIL application, then the call origin will be Web as default. The call origin is selected as Phone or Email in other case.
g. Type the description of the call.
h. Click submit button to submit the call.



Call Classification

1. After the call is logged, the SD classifies the call based on the request/issue raised.
2. The SD does some initial investigation of the call and gives his feedback
3. The severity of the call is selected.
4. The call category, complaint and complaint detail related to the request/issues raised is classified
5. SLA override option is provided in case if the SD wants to override the organization calendar, so that the technician has to attend the call irrespective of the defined SLA.
6. Attachment option is also provided if the SD wants to add a screenshot related to the incident.

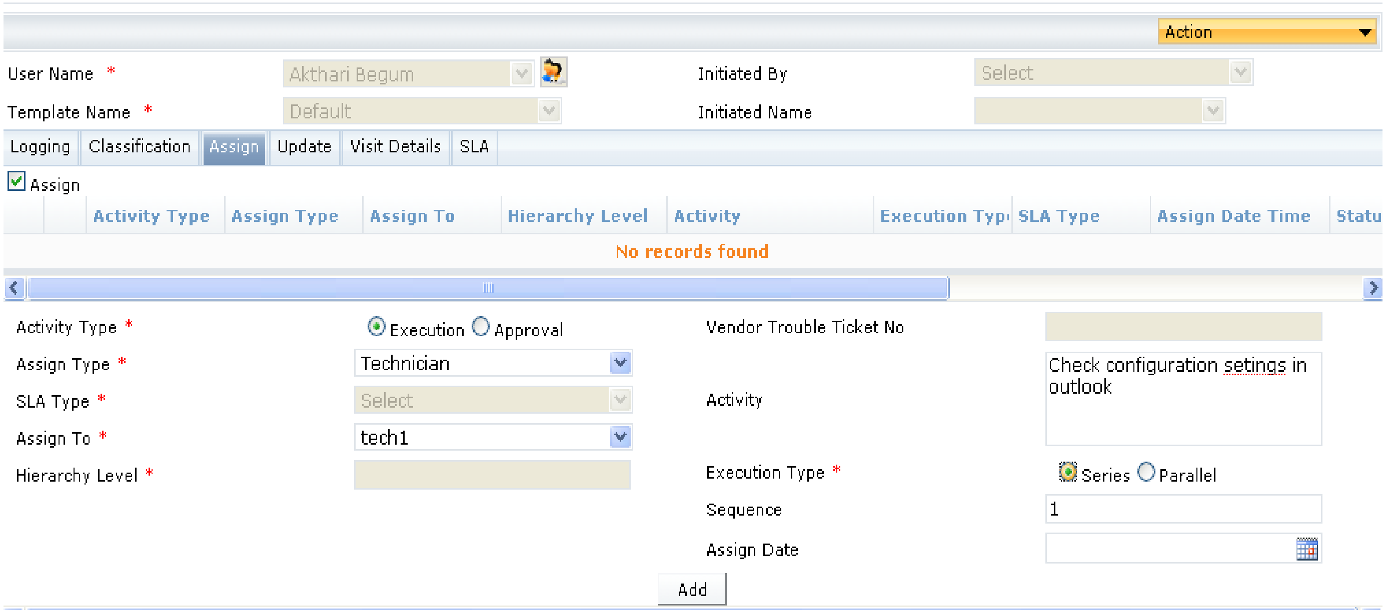


Assign / Re-Assign

There are two activities involved in the Assign Process

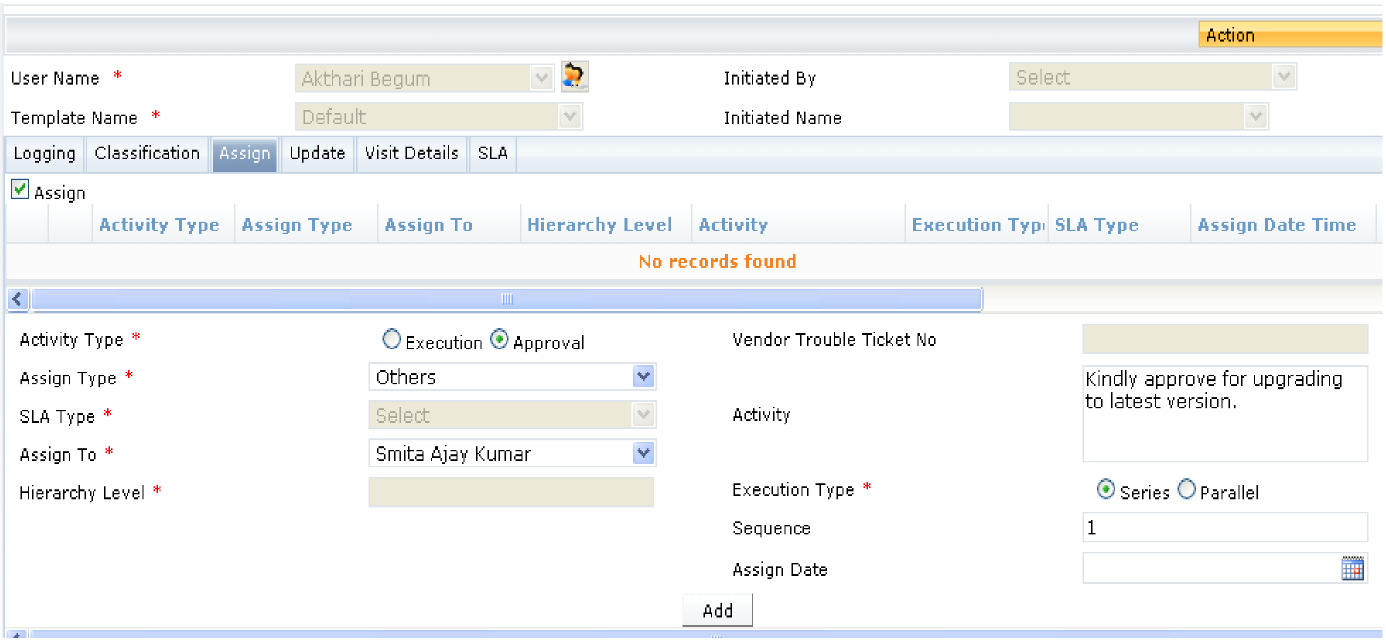
Execution Process – In the execution process the incidents are assigned directly to the respective Technician, and the Technician updates the call upon resolving the incident. If the activity type is selected as Execution, then the following steps has to be done

1. Select Assign type as either Technician or Vendor
2. Select the Technician name form the dropdown for whom the incident is to be assigned
3. Define a activity for the Technician for resolving the incident
4. Select the Execution type as either Series or Parallel. This implies whenever a scenario like multiple person required for resolving an incident.
5. Click Add to add the technician selected
6. The same incident can also be assigned to multiple technician, in this scenario follow the above steps from 1 to 6
7. Click Submit to submit the incident



Approval Process – In the approval process for certain service request like any software purchase request, server access request, etc can be sent to either the Reporting Manager of the user or to any other user who is part of the domain. If the activity type is selected as Approval, then the following steps has to be done

1. Select Assign Type as either Manager or Others
2. If the Assign type is selected as Manager, then the incident is directly sent to the reporting manager of the user for Approval
3. If the Assign type is selected as Others, then select the user name for whom the incident has to be sent for approval
4. Define a activity for the approver to perform on the incident
5. Select the Execution type as either Series or Parallel. This implies whenever a scenario like multiple person required for approving an incident.
6. Click Add to add the approver selected
7. The same incident can also be sent to multiple approver , in this scenario follow the above steps from 1 to 6
8. Click Submit to submit the incident



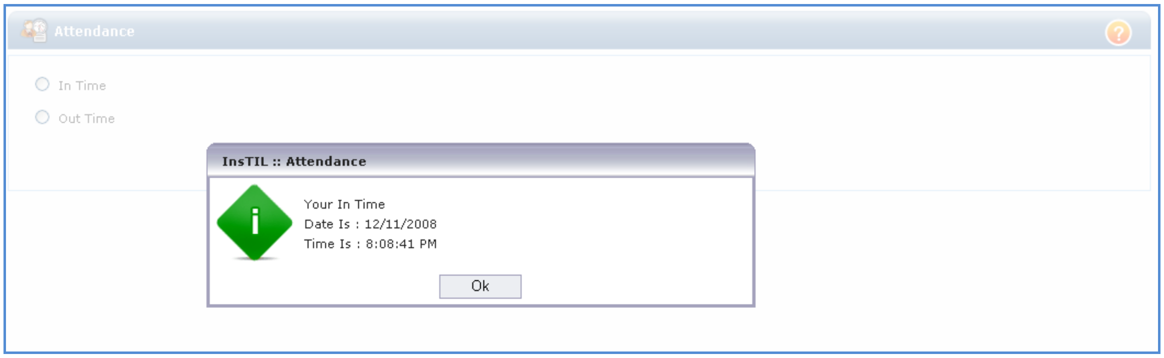
Utilities

Attendance

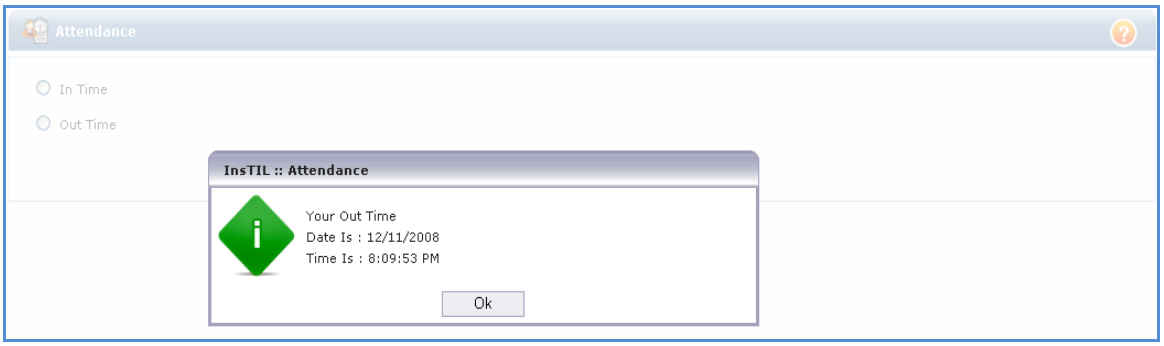
This feature enables the user to mark the Punch In time and Punch Out time for the particular day. This feature is made available for all the roles in InsTIL.

Operation

1. Select Punch In time and submit which marks the in time for the user

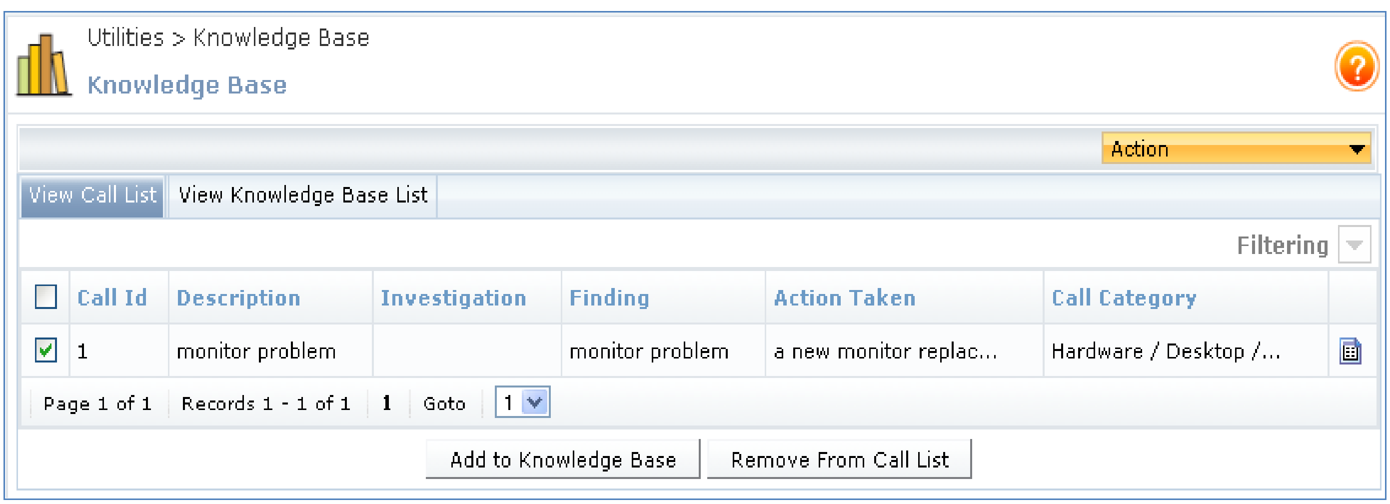


2. Similarly select Punch Out time and submit which marks the out time for the user.



Knowledge Base

The knowledge base is populated with the information from the incident data. All incidents with status as Completed or Closed will be displayed in the Grid. These incidents can be moved to the knowledge base. The administrator has the provision for updating the knowledge base or the administrator can be given the permission for viewing the knowledge base alone.

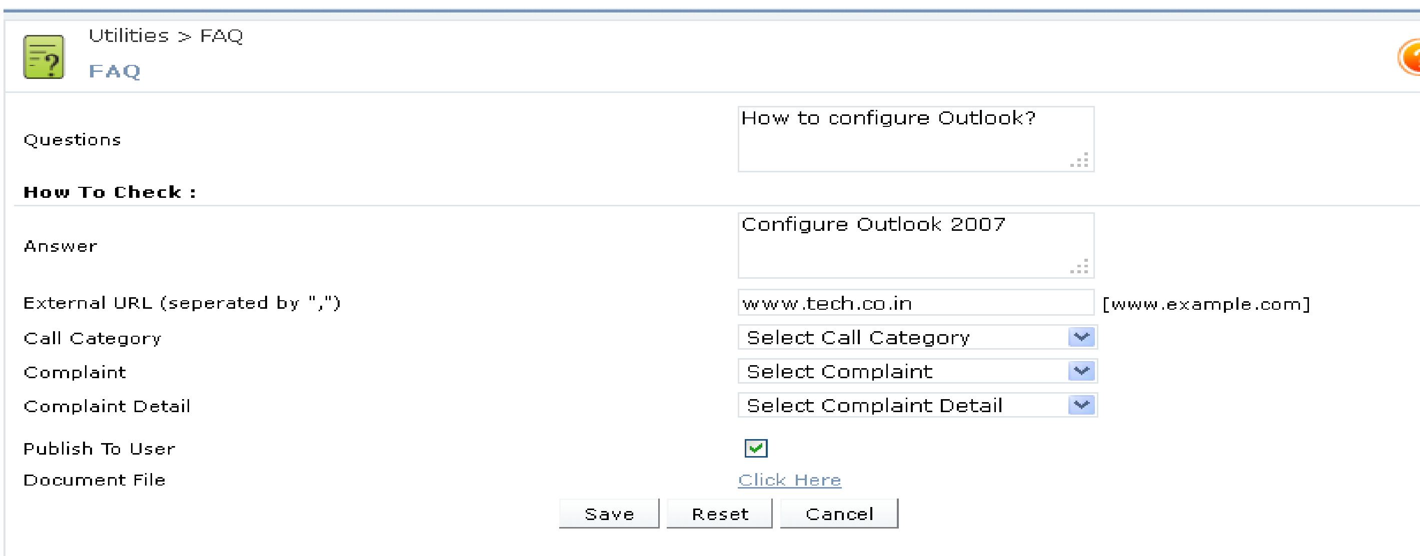


Operation

8. The calls with the status closed and completed will be displayed in the grid.
9. Click view to see the complete call history of the call.
10. Select the calls that has to be added to the knowledge base
11. Click Add to Knowledge base to add the call to the knowledge base.
12. Click View Knowledge base to see the calls that are added in the knowledge base
13. To remove a call from the database, select the call and click Remove button.
14. To search a content from the knowledge base, type a keyword and click Search knowledge base

FAQ

The FAQ module is to use to gather some information related to the queries posted .The FAQ can be updated by the Service desk, Administrator, Technician and IT Manager if permissions are given by the Administrator in the settings menu.



Operation

9. Type the question for the FAQ (Search keyword)
10. Type the answer.
11. Type the Url(s) for providing the information.

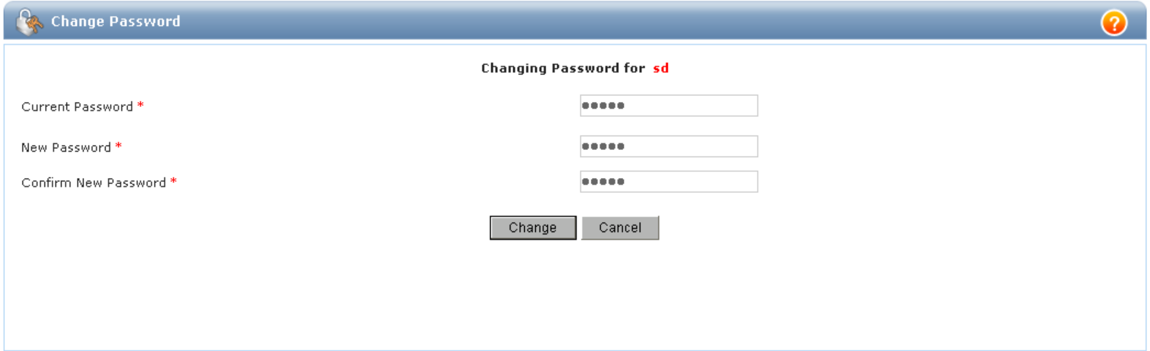
12. Upload a document file.
13. Select the Call Category, Complaint and Complaint detail (if needed), to group the FAQ.
14. Enable Publish to user knowledge base to be viewed by the end user.
15. Click Submit to save the FAQ created.
16. To view a FAQ select search FAQ and type the keyword to be searched and click search.

Change Password

This screen is used to change the password. Only local user can change their password.

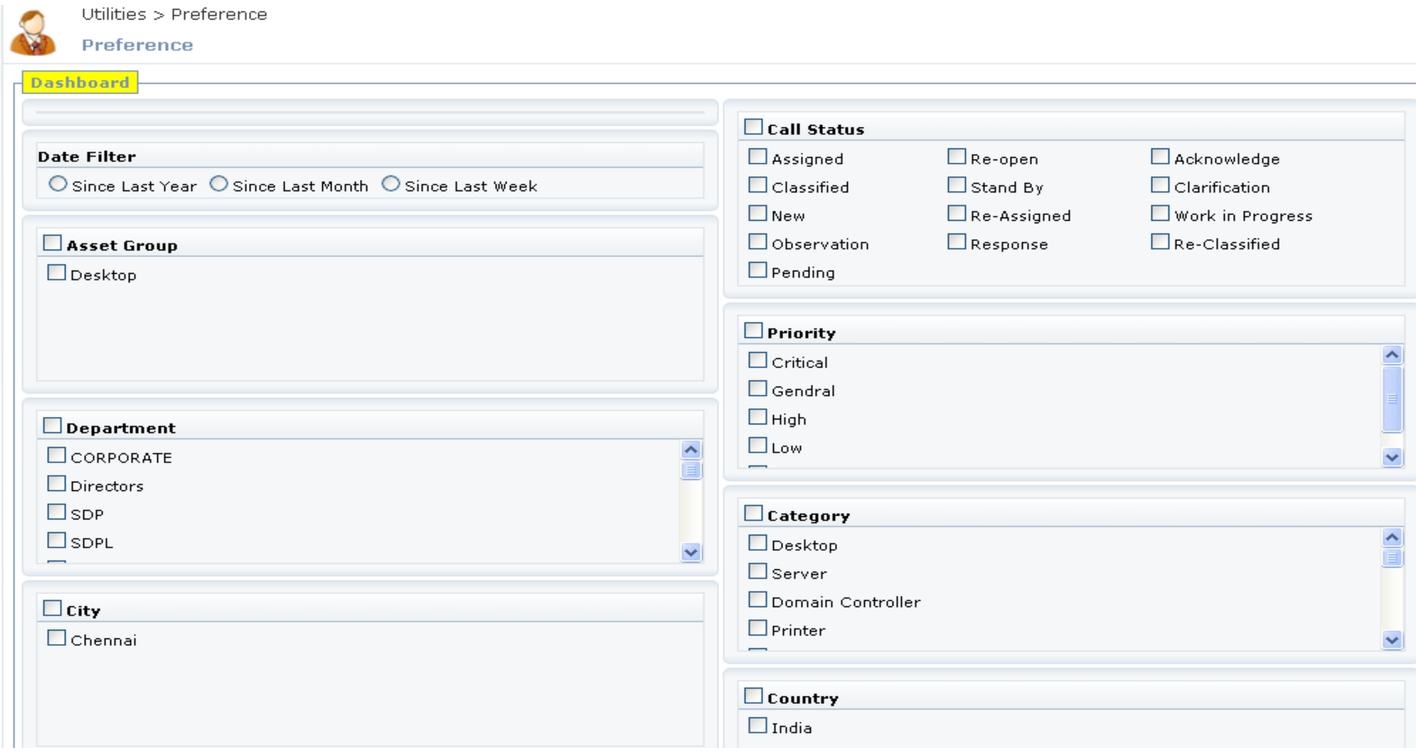
Operation

1. Enter your current password
2. Enter your new password and confirm password
3. Click change to change the password



Preference

To set owners favorite as default preference is used. The Service Desk can set Preference for dashboard based on call status and various other groupings. Service Desk can set preference such that the calls which are not closed by the user should close automatically within the days that have been defined by SD.



Operation

1. Select Preference option from the Utilities
2. The screen for Preference is shown below
3. Select the call status that has to been displayed in the call detail list
4. Similarly the Service Desk can set preference for different categories like priority, Asset group, department etc
5. Click the Set Preference Button to set the Preferences.

Task

Task can be created and assigned to self and groups. Some of them include:

- Backup Tasks.
- Preventive maintenance task.
- Information on meeting. Etc
- Re-occurrence is set for Daily, Weekly and Monthly frequencies.
- The screen for setting task is shown below

Operation:

1. Click the Add New Task.
2. Enter the Subject – Brief outline of the task to be set
3. Enter the From Date – The task will be triggered starting from this date
4. Enter the Due Date of the task
5. Set the Priority level – High, Medium and Low
6. Enter the Content of the Task
7. Select Alert By - either through his dashboard or E-mail/SMS
8. Select the frequency of occurrence of the task- daily, weekly or monthly
9. Select the user names whom the reminder has to be triggered
10. For selecting the department in a particular location:
11. Select the Department name.
12. Select the Country Name.
13. Select the City Name.
14. Select the Location name.
15. Click Save button to save the record created
16. Click Delete button to delete the record
17. Click Reset button to reset the entries.
18. Click Cancel button to cancel the process.

Reports

Service Desk has the complete call analysis report. The various groupings are listed below.

Call Analysis

Call Details

The reports related to Call Analysis includes

1. Incident – Time wise – Based on priority, call type and user
2. Incident – Day wise - Based on priority, call type and user
3. Incident – Monthly - Based on priority, call type and user
4. Call Detail

- Asset
- Call category
- Call origin

- Call status
- Technician status
- Call analysis
- Technician performance
- FLS report
- Maximum Calls – Asset
- Maximum Calls– Call category
- Maximum Calls – Duration
- Maximum Calls – Engineer
- Maximum Calls – User
- Re-occurrence
- Wrong classification
- User
- Time sheet
- Call Summary
- Call Priority Summary
- Technician Pending calls
- Technician call summary
- Category based calls
- SLA Report
- Deviated/Pending calls – Engineer wise
- Incident at a glance report
- Summary reports
- Location wise call report
- Periodical call report

7.0 Logging In as Technician

A call once logged by the user will be assigned by the service desk to the concerned technician by considering the availability of the technician or the process will be automated. Once the Technician logs into the application, the calls assigned will be displayed at his/her home page. The technician cannot update the call unless the authorization is given by the administrator

The Technician will be able to provide

1. Information on action taken to resolve the problem.
2. Send a clarification to the user.
3. Re-assign the call , if the cal category selected by the user is wrong.
4. Check-in and Check-out date and time
5. Status such as Completed, Pending, Standby, Completed, Re-assigned etc.

ID	USER	ASSET DESCRIPTION	DESCRIPTION	PRIORITY	CALL DATE	STATUS	APPROVALS	EXECUT
98	User	LEO / 10/LEO	Mouse Problem	Urgent	12/23/2008 6:13:47 P...	Acknowledge	Approved - ThanikaChalam -	Parallel
97	User	COMET / 10/COMET	Mouse Problem	Very Important	12/23/2008 5:52:06 P...	Acknowledge	-	Parallel
96	Priya	LEO / 10/LEO	ss	Important	12/23/2008 5:27:37 P...	Acknowledge	-	Parallel
5630	Alagurani	00:19:bb:43:f5:d6 / ...	The Monitor value is...	Low	1/16/2009 9:09:04 PM	Acknowledge	-	Parallel
547	Ayyappa	DRACO / 10/DRACO	Problem	Dont prefer	12/29/2008 4:32:30 P...	Acknowledge	-	Parallel
5050	chandramohan	DUMP / 10/DUMP	sad	Important	1/15/2009 3:44:00 PM	Acknowledge	-	Parallel

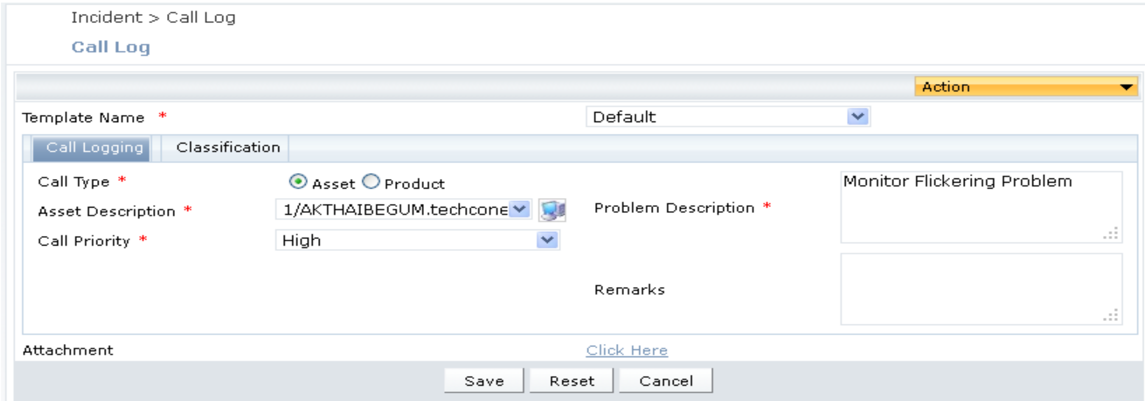
Incident

Call Log

This feature allows Technician to log in a service request or an incident with a proper description and also with a priority for the Service Desk to process accordingly. The user can add an attachment w.r.t to the incident logged. InsTIL also provides an option for the user to classify the call and based on the classification defined the calls are automatically assigned to the Technician.

Operation

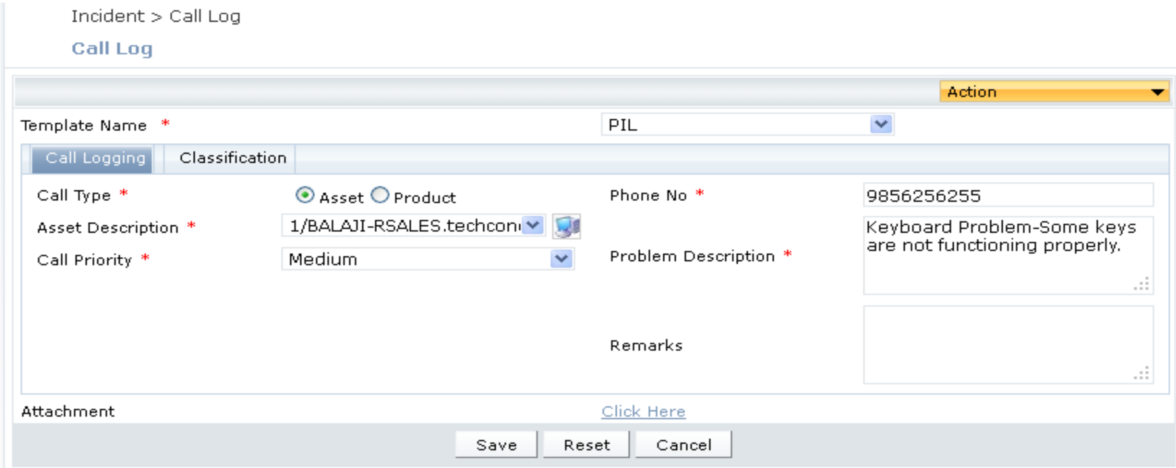
To add a new call perform the following tasks



Operation

1. Click New
2. Select the call type as Asset or Product
3. The asset description is automatically selected if the asset is linked to the user. If asset-user linking is not done select the asset from the drop down list
4. From the drop down list, select the priority at which the service needs to be attended.
5. The user can type the problem or the service request that needs to be solved.
6. Any additional information related to the problem can be provided in the Remarks column.
7. Click on Click Here link to add an attachment.
8. Click Save button to save the record created
9. Click Reset button to reset the entries.
10. Click Cancel button to cancel the process

Call Logging based on the default template



Operation

1. Click New to login an incident or service request.
2. Select the template name from the dropdown list for which the call is to be logged.
3. From the drop down list of Product Description, select your particular product.
4. The user can type the problem or the service request that needs to be solved.
5. Any additional information related to the problem can be provided in the Remarks column.
6. An attachment can also be added with the call logged.
7. Click Save button to save the record created
8. Click Reset button to reset the entries.
9. Click Cancel button to cancel the process

Call Update

Once the technician receives the call on his/her home page, technician can update the status for the call by finding the problem and providing a solution. The various call status provided for the technician while updating a call is as follows

1. Pending - This status tells about the call pending, where the same technician has to close and if it exceeds the SLA, it will be in the deviation.
2. Completed - This status tells about the completed call by Technician and the call will be in the customer's basket for his feedback.
3. Response - This status will provide an advantage to technician to give his responsiveness towards the call, meanwhile he shall attend the call as per the priority.
4. Re assigned - This status tells about the engineer is unable to complete the call and needs to reassign to the Service Desk, the SD the assigns call to another technician or a Vendor
5. Standby - There may be calls which cannot be closed by giving the resolution on the same machine, hence engineer has provided the standby in order maintain the SLA.
6. Observation - The engineer has completed the call but he wants to make the system under observation to complete the call satisfactorily

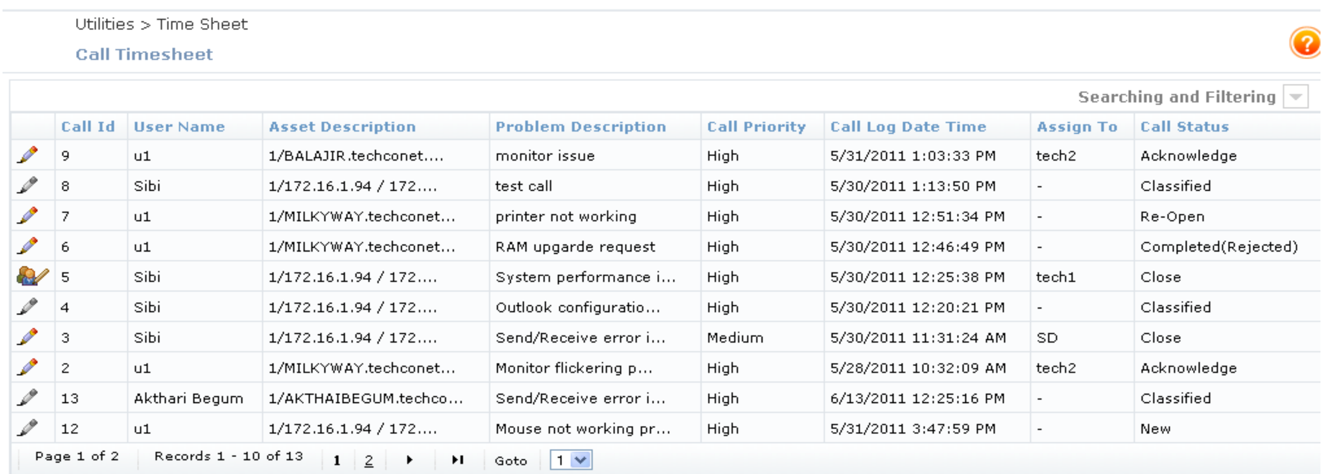
Operation

1. The technician troubleshoots the call assigned to him.
2. The actual complaint, action taken for the call and Action taken category should be entered.
3. The Technician updates the current status of the call
4. Browse and upload any file if required relating with the incident.
5. Use Remarks field to enter any additional description

6. Check-in and check-out dates are automatically updated if authorization is provided by the administrator.
7. Once the technician selects the call from the grid, the status will be Response and the check in time will be the same as the server time.
8. After troubleshooting the incident , the technician selects the particular call and based on the status the call is updated
9. Technician can provide a Plan start date and plan end date for each call and start working accordingly
10. Technician can even send an approval for the call if required.
11. Click Submit button to save the call

Call Timesheet

The call timesheet option is available for the Technician to update the duration taken for a particular activity assigned to him or to update on behalf of any other person on the same group.



Utilities > Time Sheet

Call Timesheet

Searching and Filtering

	Call Id	User Name	Asset Description	Problem Description	Call Priority	Call Log Date Time	Assign To	Call Status
	9	u1	1/BALAJIR.techconet....	monitor issue	High	5/31/2011 1:03:33 PM	tech2	Acknowledge
	8	Sibi	1/172.16.1.94 / 172....	test call	High	5/30/2011 1:13:50 PM	-	Classified
	7	u1	1/MILKYWAY.techconet...	printer not working	High	5/30/2011 12:51:34 PM	-	Re-Open
	6	u1	1/MILKYWAY.techconet...	RAM upgarde request	High	5/30/2011 12:46:49 PM	-	Completed(Rejected)
	5	Sibi	1/172.16.1.94 / 172....	System performance i...	High	5/30/2011 12:25:38 PM	tech1	Close
	4	Sibi	1/172.16.1.94 / 172....	Outlook configuratio...	High	5/30/2011 12:20:21 PM	-	Classified
	3	Sibi	1/172.16.1.94 / 172....	Send/Receive error i...	Medium	5/30/2011 11:31:24 AM	SD	Close
	2	u1	1/MILKYWAY.techconet...	Monitor flickering p...	High	5/28/2011 10:32:09 AM	tech2	Acknowledge
	13	Akthari Begum	1/AKTHAIBEGUM.techco...	Send/Receive error i...	High	6/13/2011 12:25:16 PM	-	Classified
	12	u1	1/172.16.1.94 / 172....	Mouse not working pr...	High	5/31/2011 3:47:59 PM	-	New

Page 1 of 2 Records 1 - 10 of 13 1 2 Goto 1

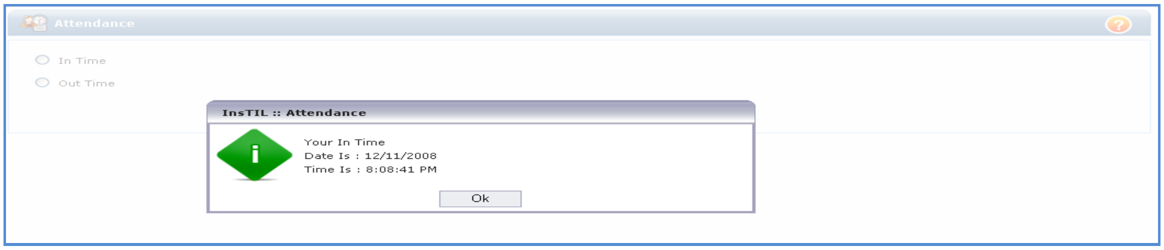
Utilities

Attendance

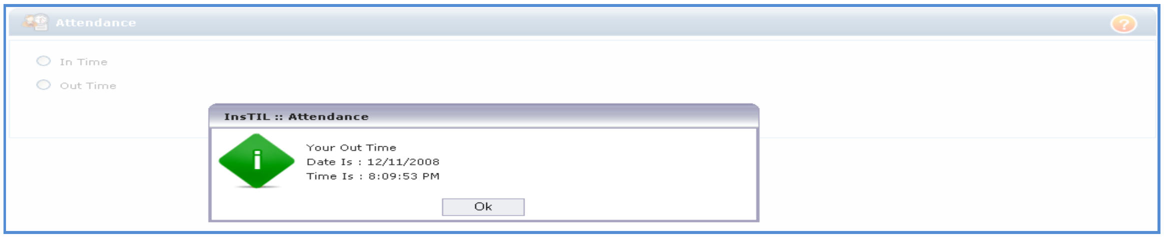
This feature enables the user to mark the Punch In time and Punch Out time for the particular day. This feature is made available for all the roles in InsTIL.

Operation

1. Select Punch In time and submit which marks the in time for the user

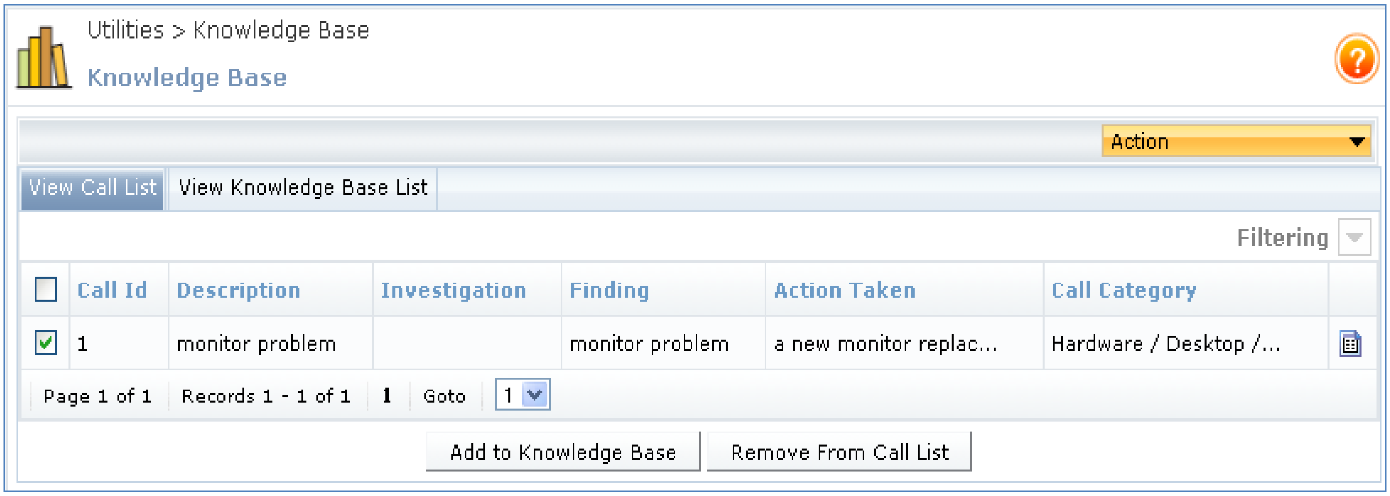


2. Similarly select Punch Out time and submit which marks the out time for the user.



Knowledge Base

The knowledge base is populated with the information from the incident data. All incidents with status as Completed or Closed will be displayed in the Grid. These incidents can be moved to the knowledge base. The administrator has the provision for updating the knowledge base or the administrator can be given the permission for viewing the knowledge base alone.

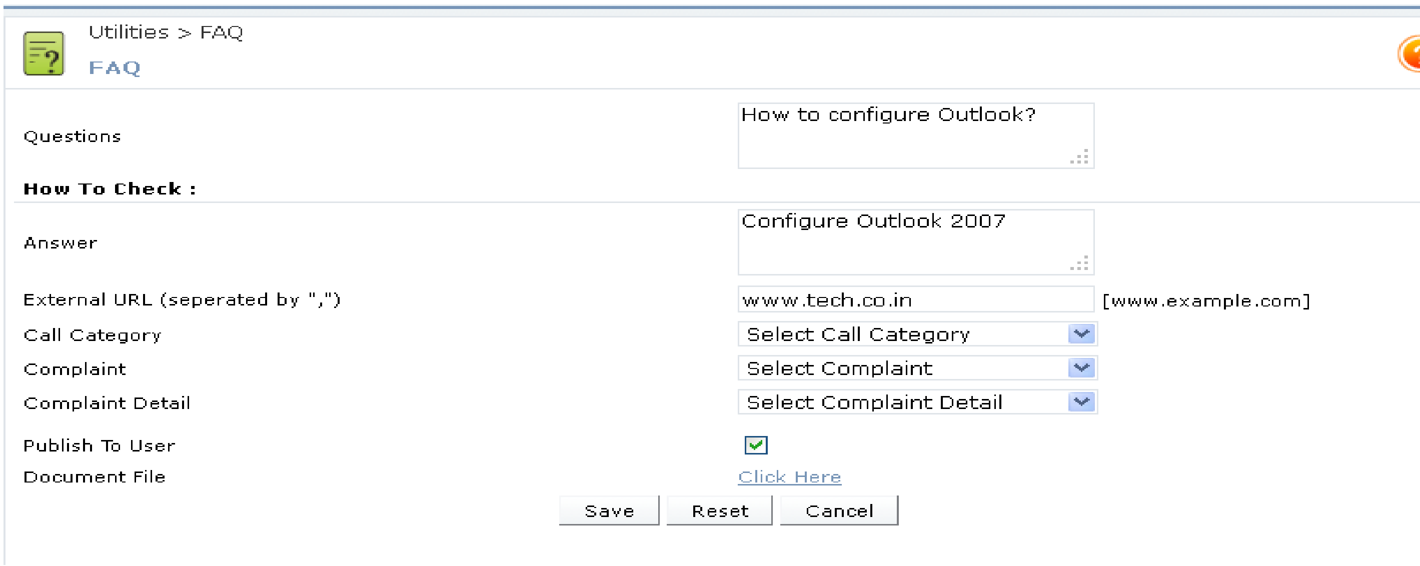


Operation

1. The calls with the status closed and completed will be displayed in the grid.
2. Click view to see the complete call history of the call.
3. Select the calls that has to be added to the knowledge base
4. Click Add to Knowledge base to add the call to the knowledge base.
5. Click View Knowledge base to see the calls that are added in the knowledge base
6. To remove a call from the database, select the call and click Remove button.
7. To search content from the knowledge base, type a keyword and click Search knowledge base

FAQ

The FAQ module is to use to gather some information related to the queries posted .The FAQ can be updated by the Service desk, Administrator, Technician and IT Manager if permissions are given by the Administrator in the settings menu.



Operation

1. Type the question for the FAQ (Search keyword)
2. Type the answer.
3. Type the Url(s) for providing the information.
4. Upload a document file.
5. Select the Call Category, Complaint and Complaint detail (if needed), to group the FAQ.

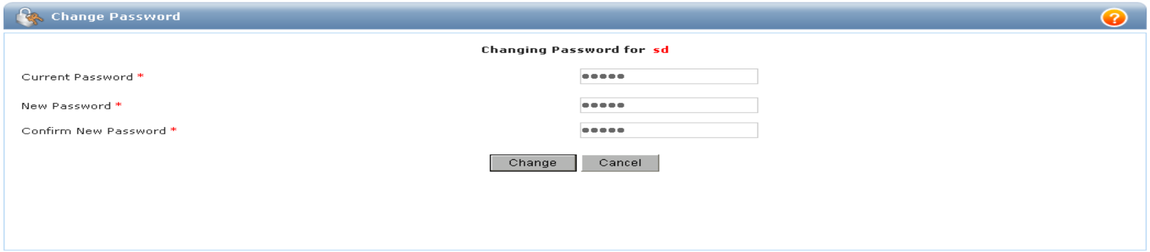
6. Enable Publish to user knowledge base to be viewed by the end user.
7. Click Submit to save the FAQ created.
8. To view a FAQ select search FAQ and type the keyword to be searched and click search.

Change Password

This screen is used to change the password. Only local user can change their password.

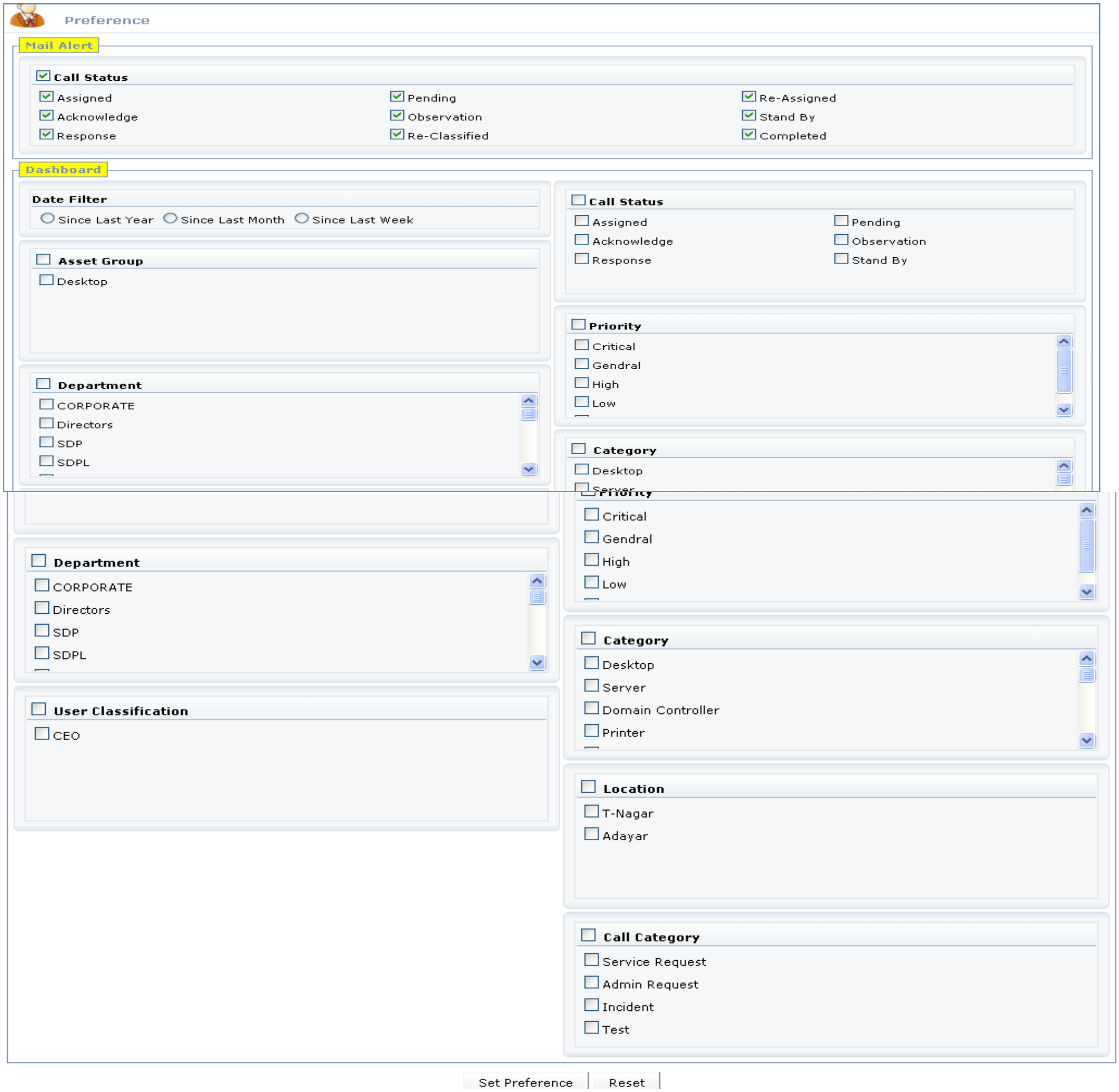
Operation

1. Enter your current password
2. Enter your new password and confirm password
3. Click change to change the password



Preferences

Preferences feature helps you to set mail alerts for particular status calls and dashboard preferences on home page depending on the call status, date filters, priority, asset group, category, department, location, user classification and call category. If the preferences are not set, the default settings will be used



Operation

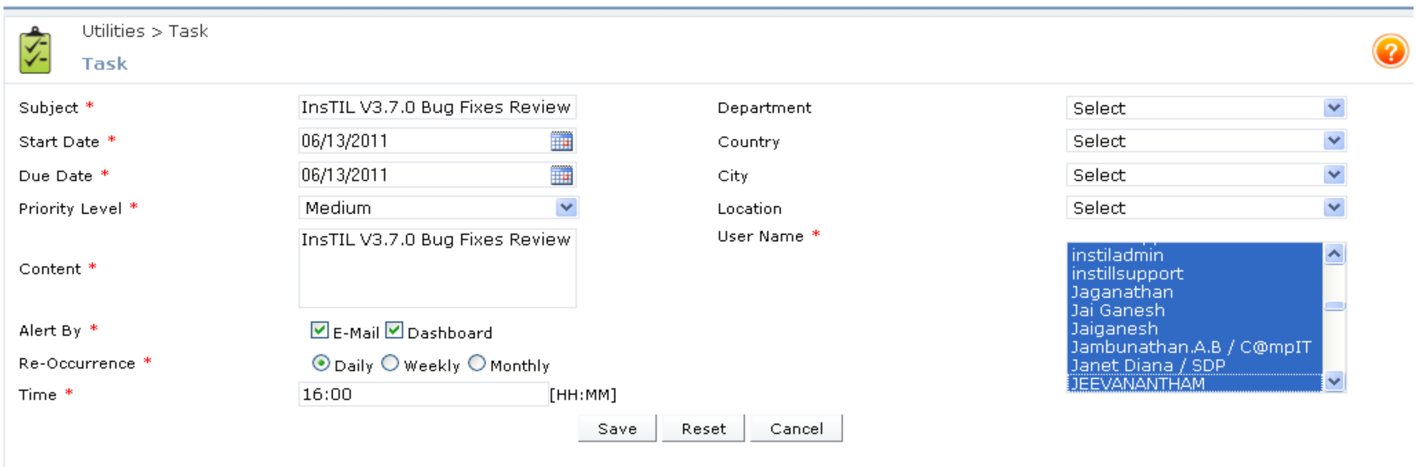
1. Click Preferences on the home page.
2. Click the required status calls for mail alerts.
3. Click the required status calls for dashboard preferences.
4. Select the date filter.
5. Select the priority.

6. Select the required asset group, category, department, location, user classification, call category.
7. Click Set Preference to save the settings.
8. Click Reset button to reset the field entries.

Task

Task can be created and assigned to self and groups. Some of them include:

a. Backup Tasks.
b. Preventive maintenance task.
c. Information on meeting. Etc
d. Re-occurrence is set for Daily, Weekly and Monthly frequencies.



Operation:

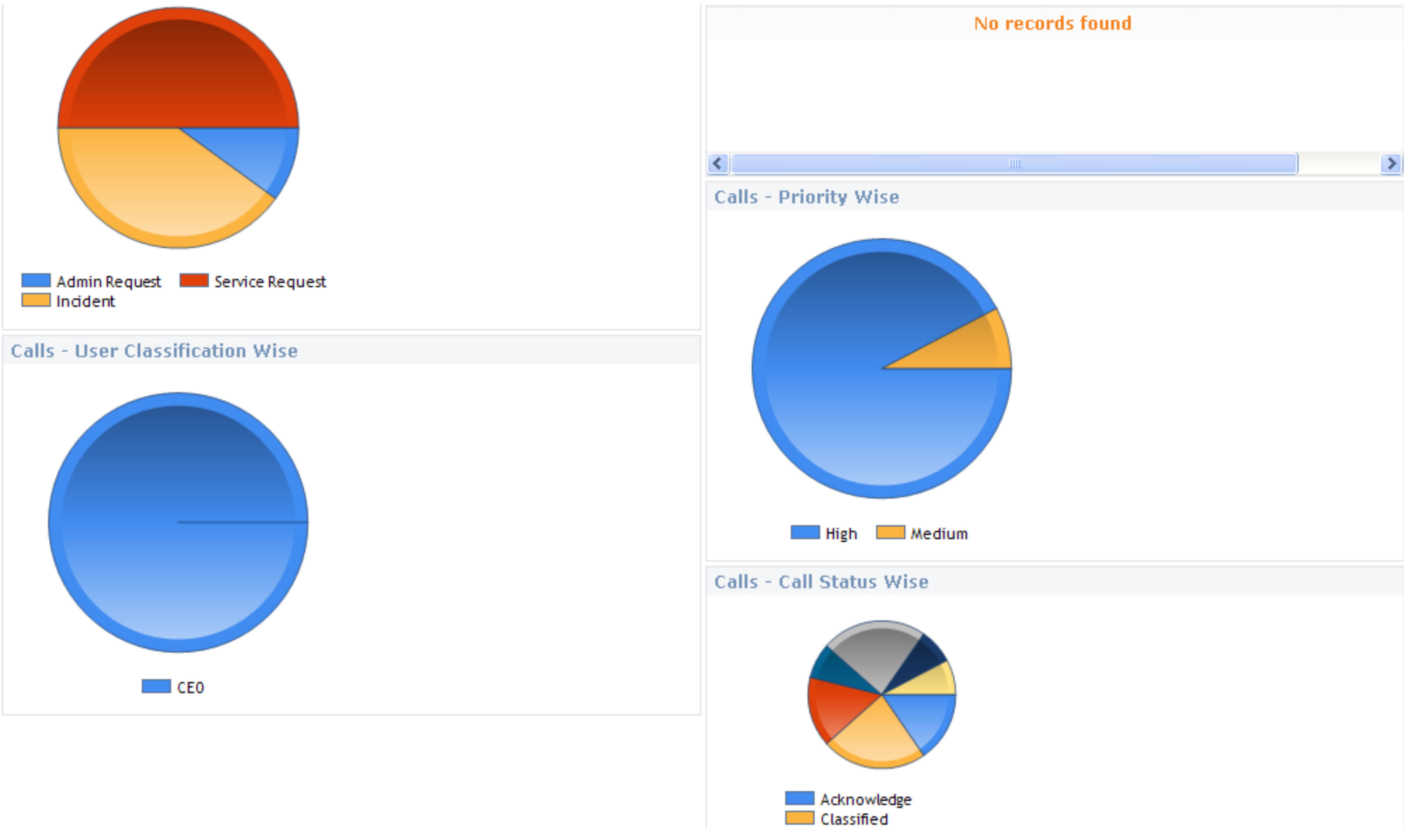
1. Click the Add New Task.
2. Enter the Subject – Brief outline of the task to be set
3. Enter the From Date – The task will be triggered starting from this date
4. Enter the Due Date of the task
5. Set the Priority level – High, Medium and Low
6. Enter the Content of the Task
7. Select Alert By - either through his dashboard or E-mail
8. Select the frequency of occurrence of the task- daily, weekly or monthly
9. Enter the time or day according to the re-occurrence
10. Select the user names whom the reminder has to be triggered
11. For selecting the department in a particular location:

12. Select the Department name.
13. Select the Country Name.
14. Select the City Name.
15. Select the Location name.
16. Click Save button to save the record created
17. Click Delete button to delete the record
18. Click Reset button to reset the entries.
19. Click Cancel button to cancel the process

8.0Logging in as IT Manager

InsTIL provides the flexibility of generating various reports related to Asset, Call Analysis, SLA Analysis. The IT Manager can generate reports like Asset detail, Reminders on Annual Maintenance Contract, Lapsed and Expired Warranty and Asset Transfer. IT Manager can generate reports analyzing on Calls received, response and resolution. IT Manager can analyze Incident based on Time wise, Day wise and Monthly reports.

Detail on total calls received, response and resolution provided can also be analyzed by the IT Manager. Most importantly, analysis report on Service Level Agreement provides critical information related to the response, resolution and uptime commitment and the deviation of the service provided. ITM can close or re-open the call on be-half of the user.



Incident

Call Update

Once the technician receives the call on his/her home page, technician can update the status for the call by finding the problem and providing a solution. The various call status provided for the technician while updating a call is as follows

a. Pending - This status tells about the call pending, where the same technician has to close and if it exceeds the SLA, it will be in the deviation.
b. Completed - This status tells about the completed call by Technician and the call will be in the customer's basket for his feedback.
c. Response - This status will provide an advantage to technician to give his responsiveness towards the call, meanwhile he shall attend the call as per the priority.
d. Re assigned - This status tells about the engineer is unable to complete the call and needs to reassign to the Service Desk, the SD the assigns call to another technician or a Vendor
e. Standby - There may be calls which cannot be closed by giving the resolution on the same machine, hence engineer has provided the standby in order maintain the SLA.

f. Observation - The engineer has completed the call but he wants to make the system under observation to complete the call satisfactorily

Operation

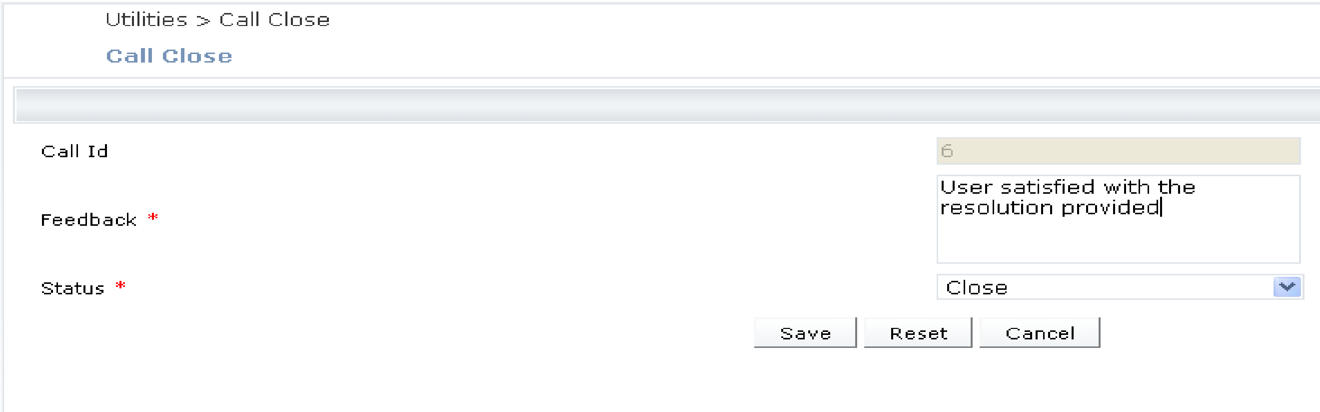
1. The technician troubleshoots the call assigned to him.
2. The actual complaint, action taken for the call and Action taken category should be entered.
3. The Technician updates the current status of the call
4. Browse and upload any file if required relating with the incident.
5. Use Remarks field to enter any additional description
6. Check-in and check-out dates are automatically updated if authorization is provided by the administrator.
7. Once the technician selects the call from the grid, the status will be Response and the check in time will be the same as the server time.
8. After troubleshooting the incident , the technician selects the particular call and based on the status the call is updated
9. Technician can provide a Plan start date and plan end date for each call and start working accordingly
10. Technician can even send an approval for the call if required.
11. Click Submit button to save the call

Call Close

The IT Manager has the provision to close or re-open the completed calls updated by the technician. This permission is also given to the user for the calls logged by him.

Operation

1. Select the call from the grid
2. Provide a feedback for the Incident raised
3. Select the status as Close/Re-open



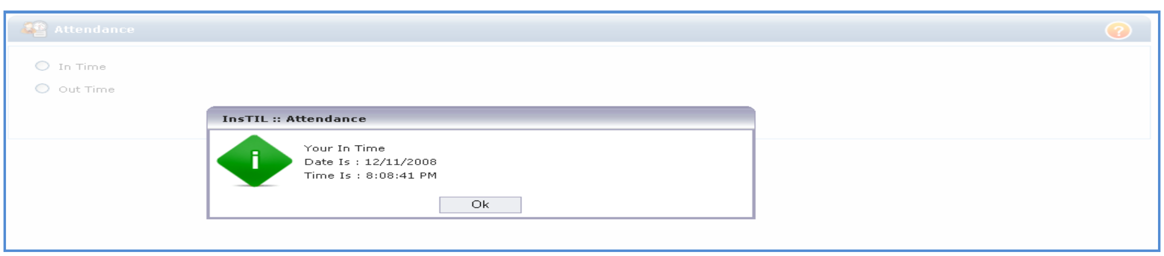
Utilities

Attendance

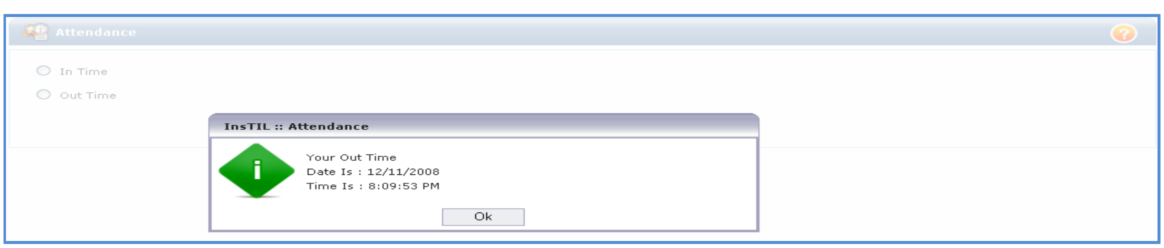
This feature enables the user to mark the Punch In time and Punch Out time for the particular day. This feature is made available for all the roles in InsTIL.

Operation

1. Select Punch In time and submit which marks the in time for the user

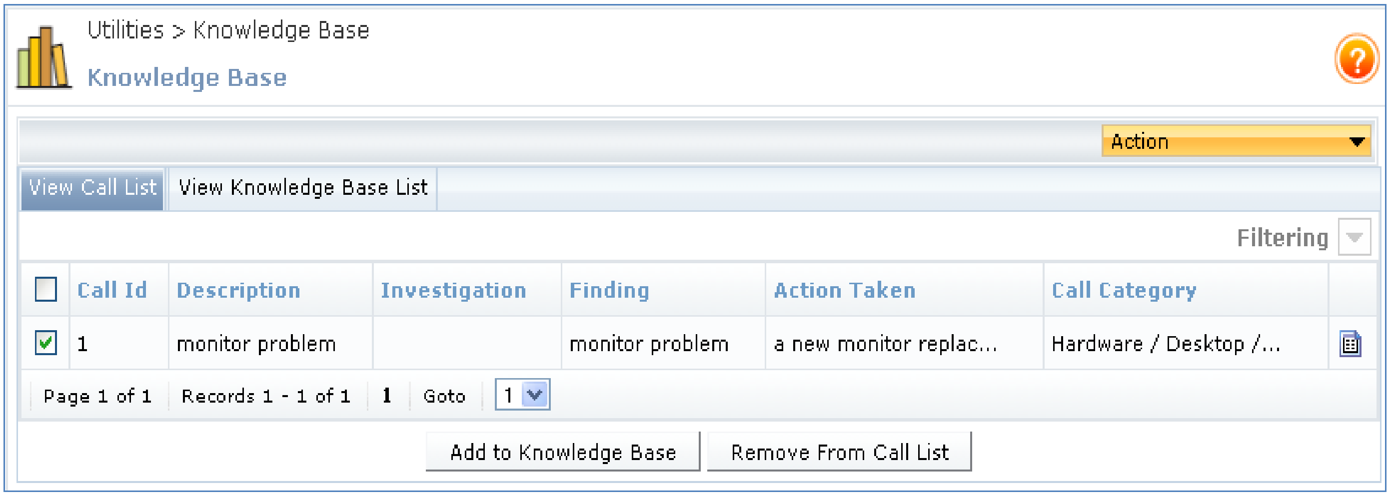


2. Similarly select Punch Out time and submit which marks the out time for the user.



Knowledge Base

The knowledge base is populated with the information from the incident data. All incidents with status as Completed or Closed will be displayed in the Grid. These incidents can be moved to the knowledge base. The administrator has the provision for updating the knowledge base or the administrator can be given the permission for viewing the knowledge base alone.

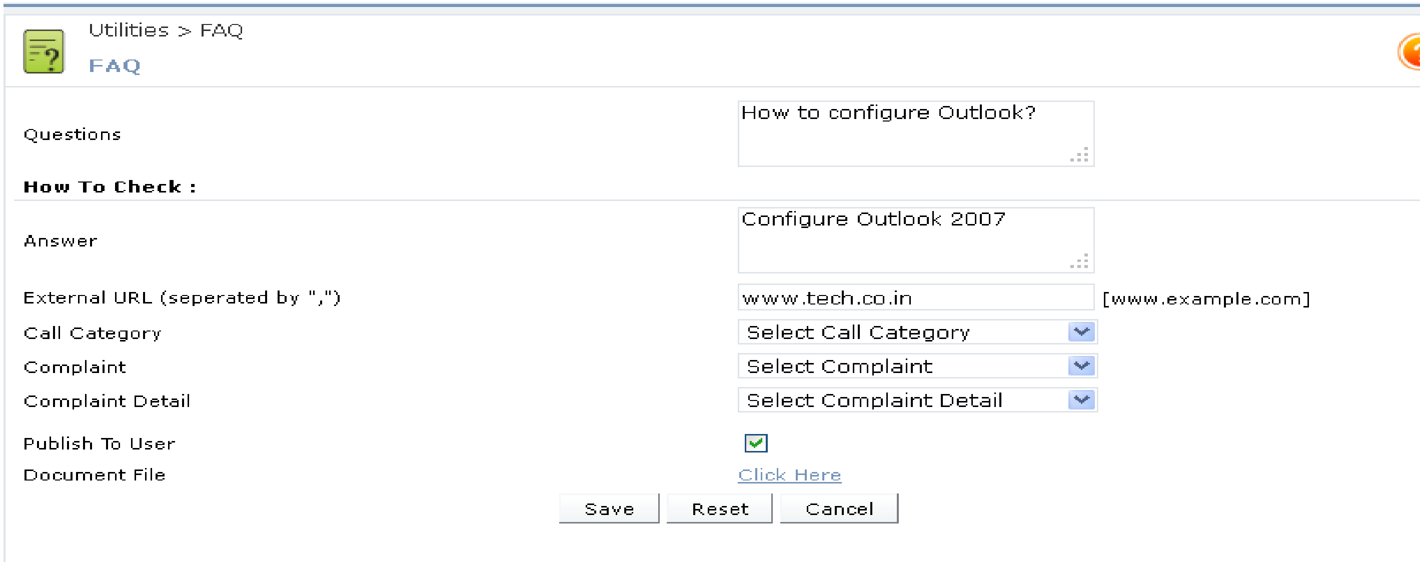


Operation

1. The calls with the status closed and completed will be displayed in the grid.
2. Click view to see the complete call history of the call.
3. Select the calls that has to be added to the knowledge base
4. Click Add to Knowledge base to add the call to the knowledge base.
5. Click View Knowledge base to see the calls that are added in the knowledge base
6. To remove a call from the database, select the call and click Remove button.
7. To search content from the knowledge base, type a keyword and click Search knowledge base

FAQ

The FAQ module is to use to gather some information related to the queries posted .The FAQ can be updated by the Service desk, Administrator, Technician and IT Manager if permissions are given by the Administrator in the settings menu.



Operation

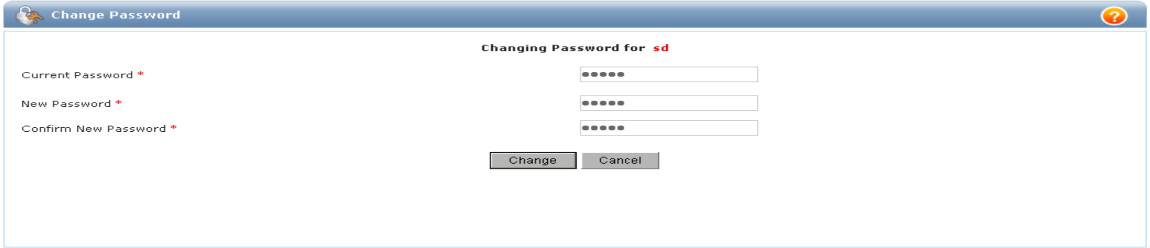
1. Type the question for the FAQ (Search keyword)
2. Type the answer.
3. Type the Url(s) for providing the information.
4. Upload a document file.
5. Select the Call Category, Complaint and Complaint detail (if needed), to group the FAQ.
6. Enable Publish to user knowledge base to be viewed by the end user.
7. Click Submit to save the FAQ created.
8. To view a FAQ select search FAQ and type the keyword to be searched and click search.

Change Password

This screen is used to change the password. Only local user can change their password.

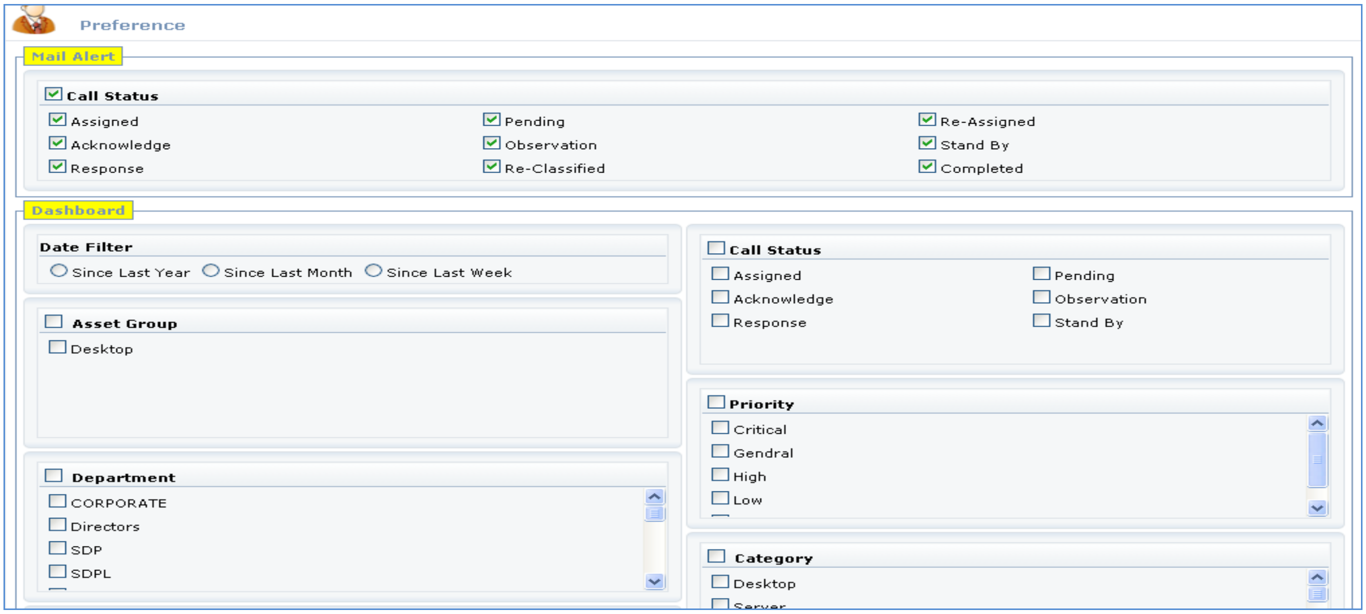
Operation

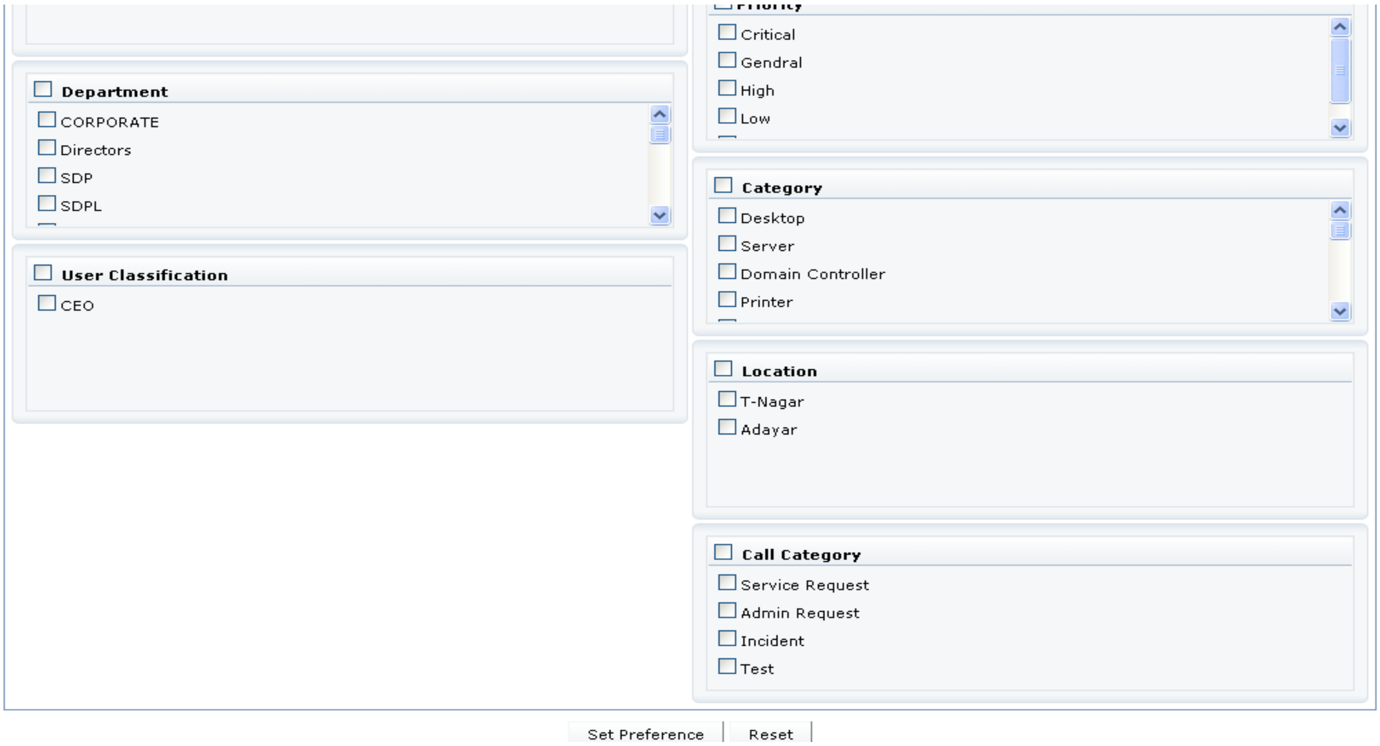
1. Enter your current password
2. Enter your new password and confirm password
3. Click change to change the password



Preferences

Preferences feature helps you to set mail alerts for particular status calls and dashboard preferences on home page depending on the call status, date filters, priority, asset group, category, department, location, user classification and call category. If the preferences are not set, the default settings will be used





Operation

1. Click Preferences on the home page.
2. Click the required status calls for mail alerts.
3. Click the required status calls for dashboard preferences.
4. Select the date filter.
5. Select the priority.
6. Select the required asset group, category, department, location, user classification, call category.
7. Click Set Preference to save the settings.
8. Click Reset button to reset the field entries.

Task

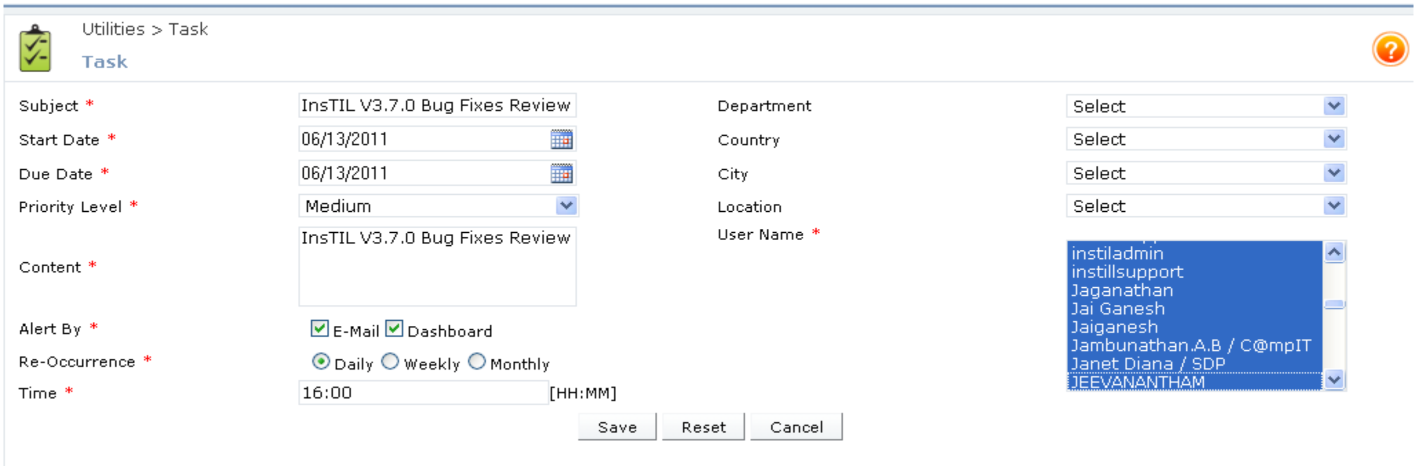
Task can be created and assigned to self and groups. Some of them include:

1. Backup Tasks.

2. Preventive maintenance task.

3. Information on meeting. Etc

4. Re-occurrence is set for Daily, Weekly and Monthly frequencies.



Operation:

1. Click the Add New Task.
2. Enter the Subject – Brief outline of the task to be set
3. Enter the From Date – The task will be triggered starting from this date
4. Enter the Due Date of the task
5. Set the Priority level – High, Medium and Low
6. Enter the Content of the Task
7. Select Alert By - either through his dashboard or E-mail
8. Select the frequency of occurrence of the task- daily, weekly or monthly
9. Enter the time or day according to the re-occurrence
10. Select the user names whom the reminder has to be triggered
11. For selecting the department in a particular location:
12. Select the Department name.
13. Select the Country Name.
14. Select the City Name.
15. Select the Location name.
16. Click Save button to save the record created
17. Click Delete button to delete the record
18. Click Reset button to reset the entries.
19. Click Cancel button to cancel the process

Reports

InsTIL application has the option to generate reports related to the Asset, Call Details, Escalation and Alerts and Notifications. These reports can be customized and viewed in detail for various types of grouping which are provided in the application. The available reports can be scheduled in Reoccurrence type of Daily, Weekly and monthly and reports triggered to various roles in the application.

The reports related to Assets includes

Asset

1. Asset detail

- Asset linking
- Asset group
- Brand
- Department
- Category
- Location
- User classification
- User linking
- Vendor

2. AMC Reminder

- Asset group
- Category
- Brand
- Department
- Location
- Vendor

3. Warranty Expiry

- Asset group
- Category
- Brand
- Department

- Location
- Vendor

4. Asset Transfer

5. Asset Physical verification report

6. Baseline report

User

User Detail – The user details can be viewed using this group

Call Analysis

1. Call Details

The reports related to Call Analysis includes

1. Incident – Time wise -Based on priority, call type and user

2. Incident – Day wise - Based on priority, call type and user

3. Incident – Monthly - Based on priority, call type and user

4. Call Detail

- Asset
- Call category
- Call origin
- Call status
- Technician status
- Call analysis
- Technician performance
- FLS report
- Maximum Calls – Asset
- Maximum Calls– Call category
- Maximum Calls – Duration

- Maximum Calls – Engineer
- Maximum Calls – User
- Re-occurrence
- Wrong classification
- User
- Time sheet
- Call Summary
- Call Priority Summary
- Technician Pending calls
- Technician call summary
- Category based calls
- SLA Report
- Deviated/Pending calls – Engineer wise
- Incident at a glance report
- Summary reports
- Location wise call report
- Periodical call report

SLA Analysis

1. SLA analysis

IT –Organization

1. Attendance report

Alerts and Notification

1. AMC/Warranty and SLA reminders
2. Task reminders
3. Escalation Details
4. SMS

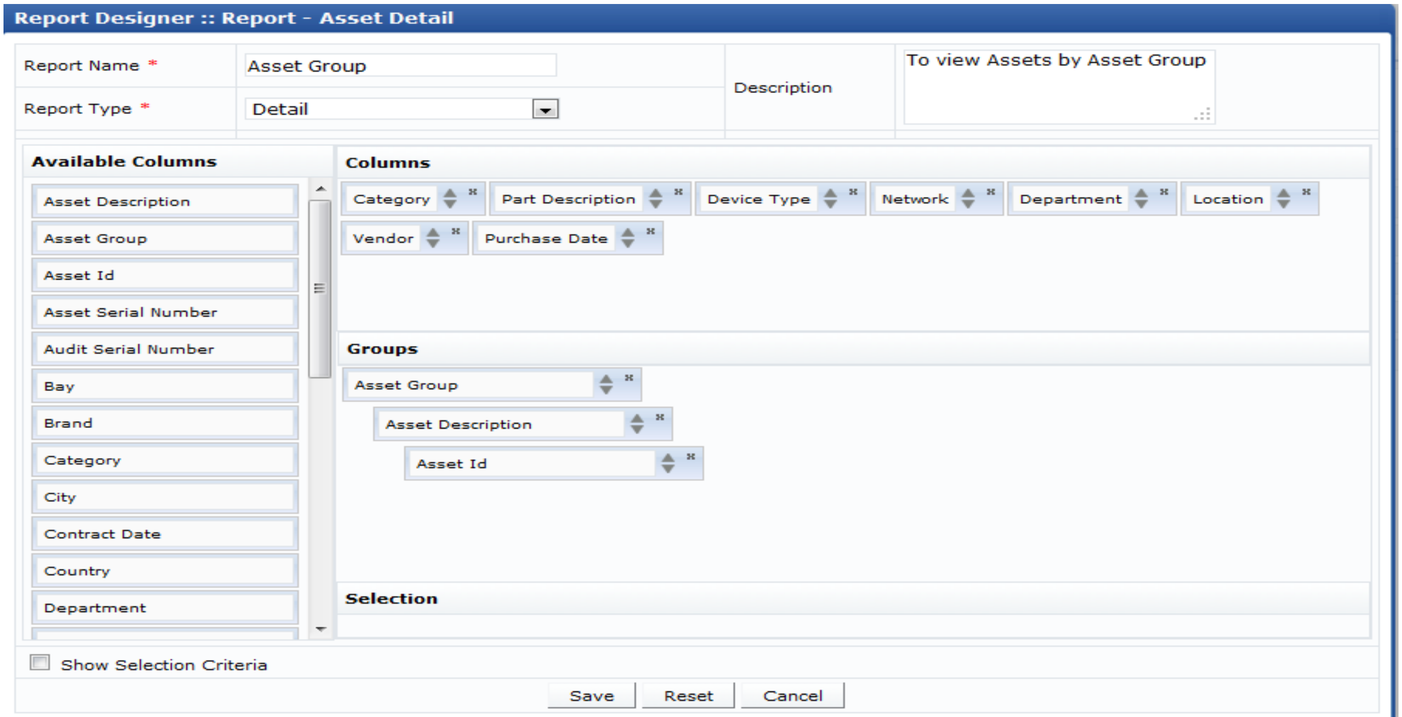
Custom Reports:

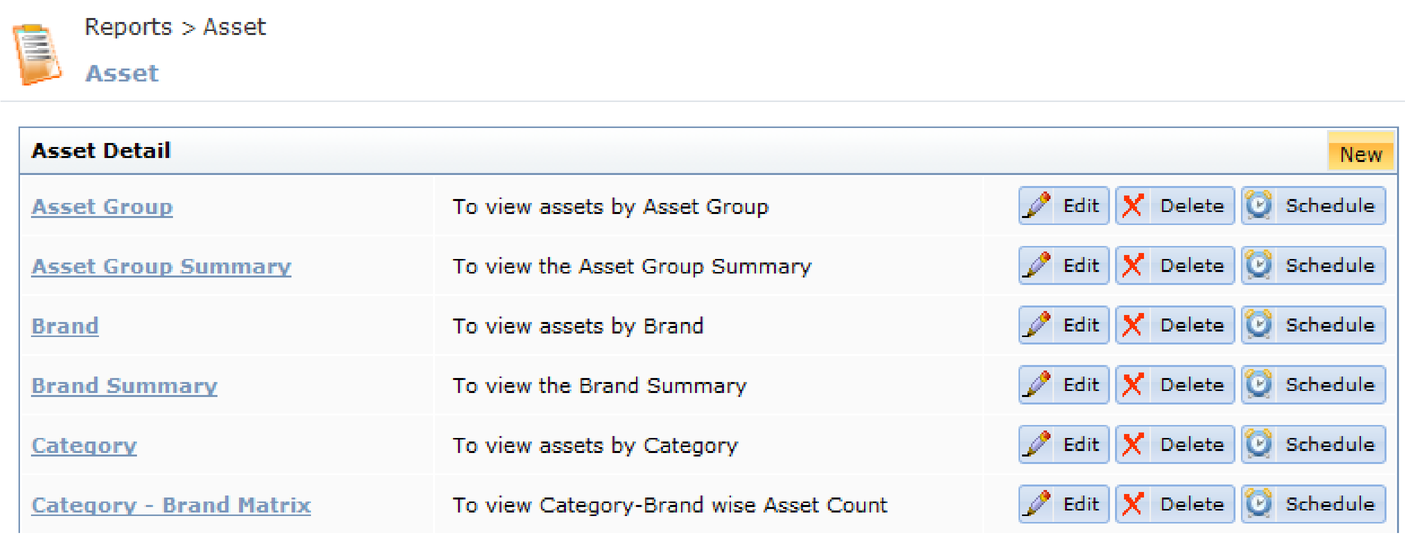
Sample Custom report is shown below

Report Type: Detail

Operations

Select the report type as **Detail** adds the required fields and save the report

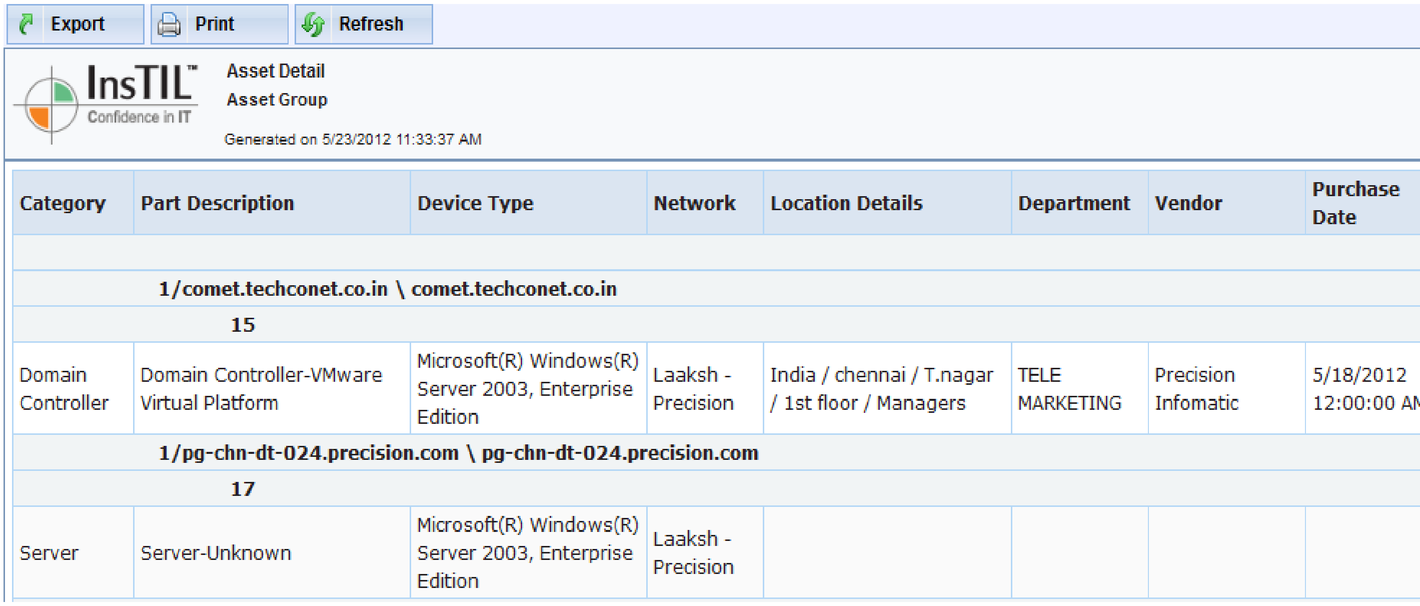




After saving the report, it enables to **Edit, Delete, Schedule**. Click the saved report to view the detail report.

Output:

It displays the fields of **Column**, **Group** and **Selection** which is dragged and dropped from the available columns

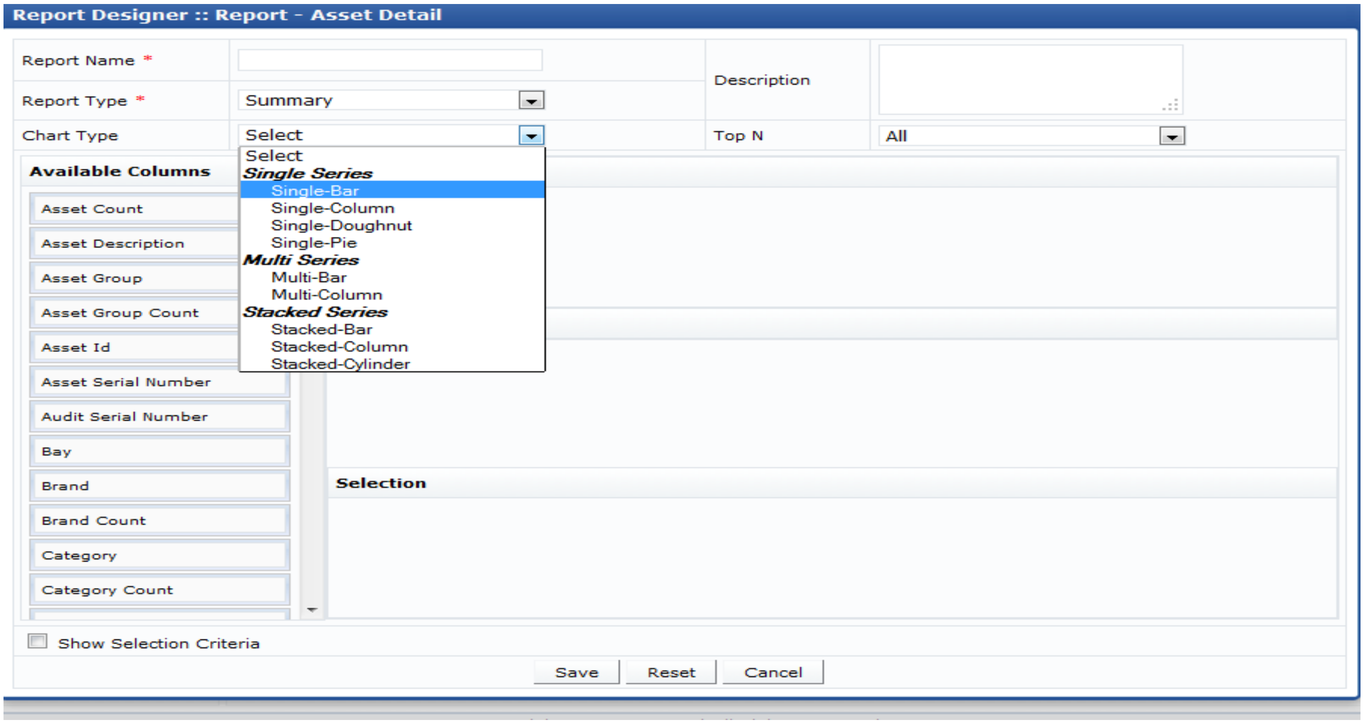


Category	Part Description	Device Type	Network	Location Details	Department	Vendor	Purchase Date
1/comet.techconet.co.in \ comet.techconet.co.in							
15							
Domain Controller	Domain Controller-VMware Virtual Platform	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	Laaksh - Precision	India / chennai / T.nagar / 1st floor / Managers	TELE MARKETING	Precision Infomatic	5/18/2012 12:00:00 A
1/pg-chn-dt-024.precision.com \ pg-chn-dt-024.precision.com							
17							
Server	Server-Unknown	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	Laaksh - Precision				

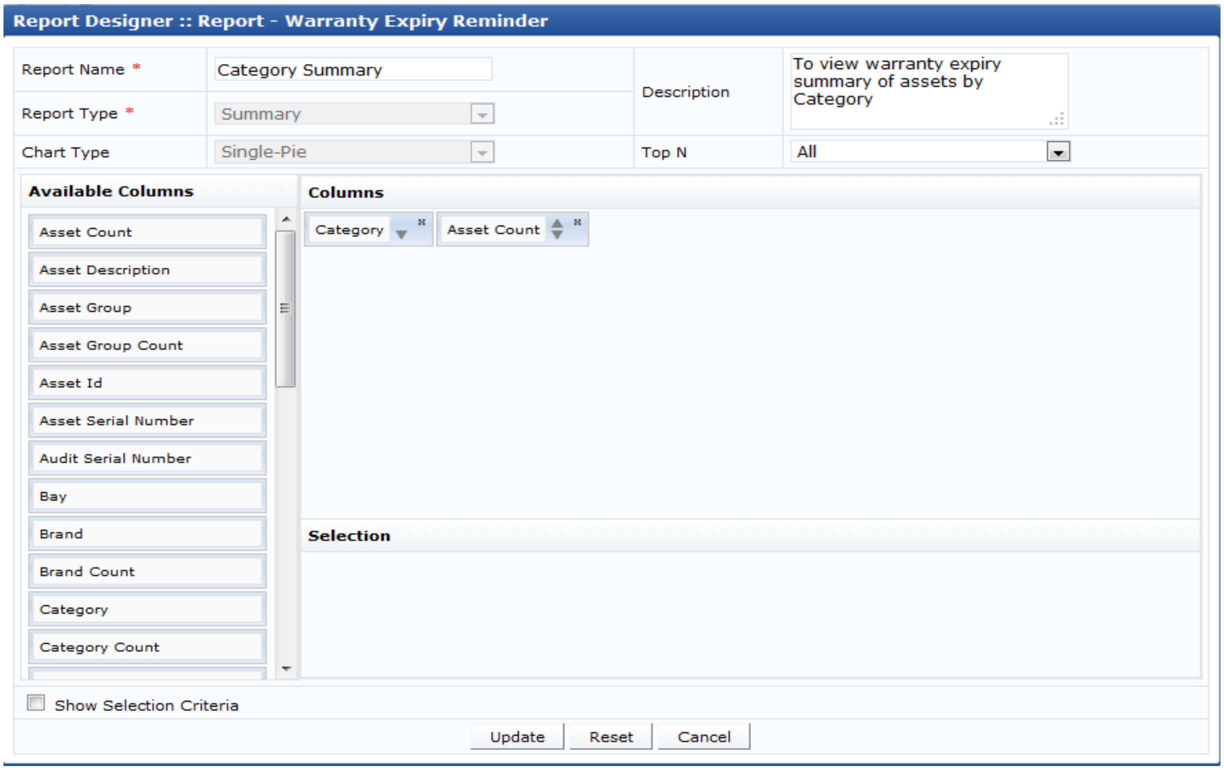
Report Type: Summary

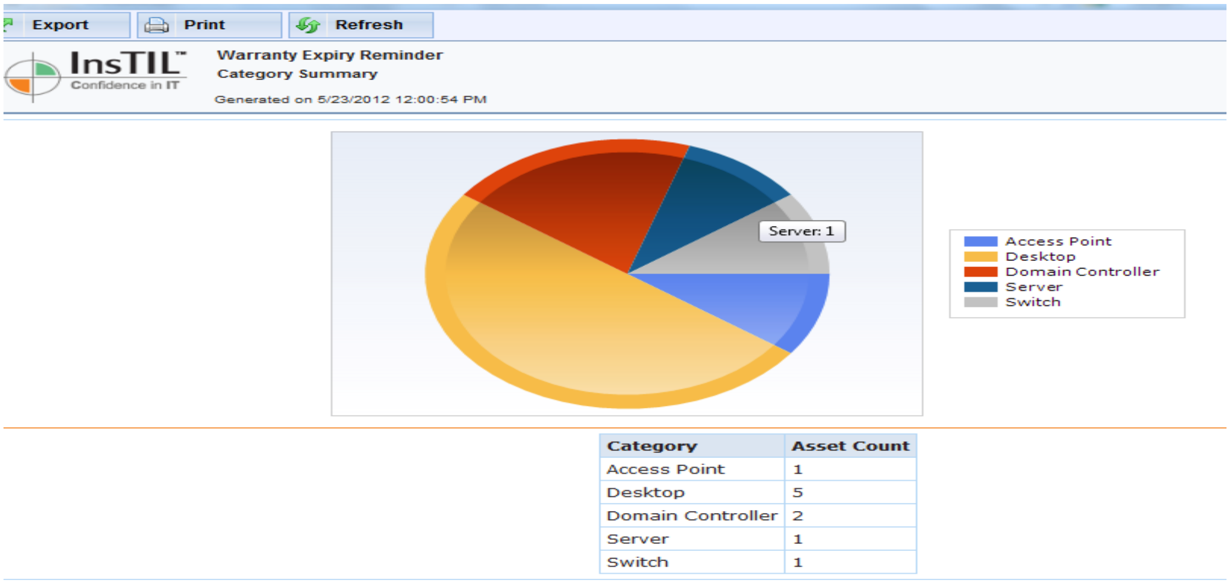
On selecting report type as summary, it displays various chart type namely

- **Single Series**
- Single bar
- Single column
- Single doughnut
- Single pie
- **Multi Series**
- Multi bar
- Multi column
- **Stacked series**
- Stacked Bar
- Stacked Column
- Stacked Cylinder



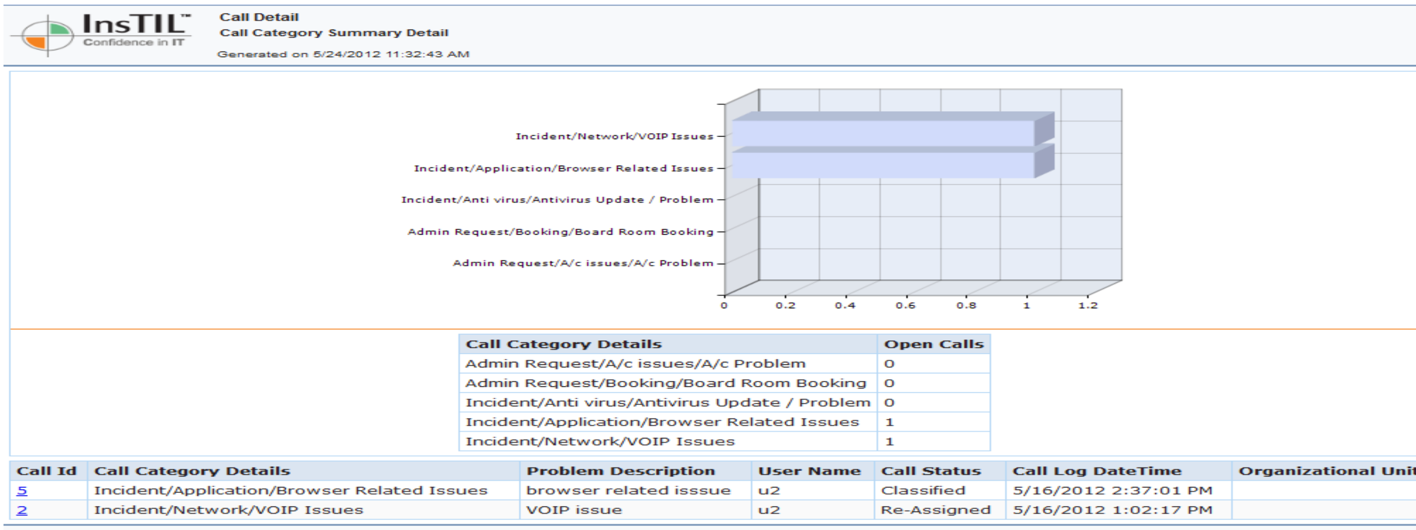
Depending on the chart type it displays the output.





Report Type: Summary Detail

The summary detail report is similar to the summary report but the output displays in detailed manner.



InsTIL™ Confidence in IT

Call Detail

Call Category Summary Detail

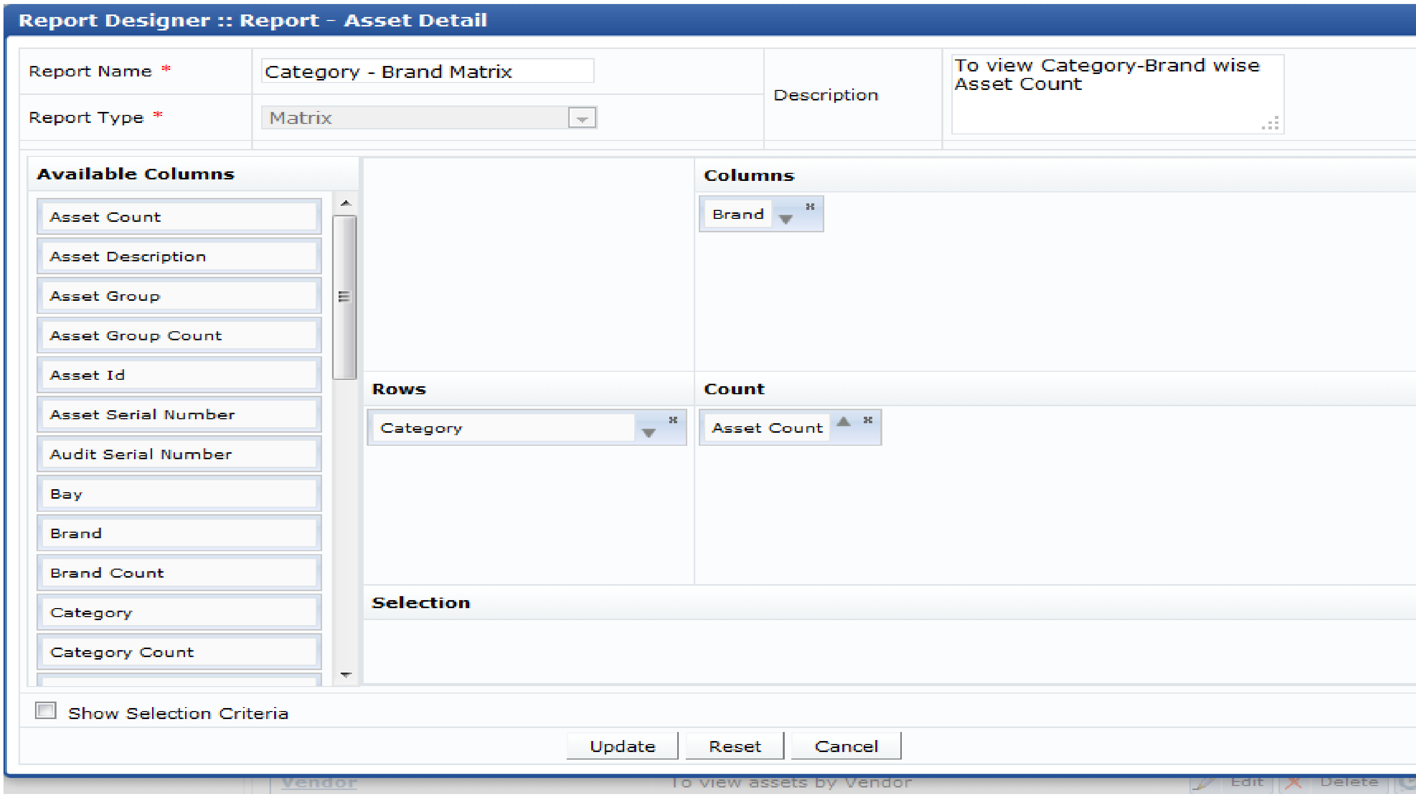
Generated on 5/24/2012 11:32:43 AM

Call Category Details	Open Calls
Admin Request/A/c issues/A/c Problem	0
Admin Request/Booking/Board Room Booking	0
Incident/Anti virus/Antivirus Update / Problem	0
Incident/Application/Browser Related Issues	1
Incident/Network/VOIP Issues	1

Call Id	Call Category Details	Problem Description	User Name	Call Status	Call Log DateTime	Organizational Unit
5	Incident/Application/Browser Related Issues	browser related isssue	u2	Classified	5/16/2012 2:37:01 PM	
2	Incident/Network/VOIP Issues	VOIP issue	u2	Re-Assigned	5/16/2012 1:02:17 PM	

Report Type: Matrix

On selecting the report type as **Matrix**, drag and drop the required fields from the available column to row, column and count.



The results are displayed as per the selection criteria made in row, column and count.

Export | Print | Refresh

InsTIL™ Confidence in IT

Asset Detail

Category - Brand Matrix

Generated on 5/24/2012 11:42:38 AM

	Hewlett-Packard	Lenovo	VMware, Inc.	Total
Access Point	1	0	0	1
Desktop	7	0	0	7
Domain Controller	0	0	2	2
Laptop	0	1	0	1
Server	1	0	0	1
Switch	2	0	0	2
Total	11	1	2	14