

iServiceDesks

The Incident Management Software, Best Practice of ITIL Standard

version 1.1



Contacting iServiceDesks Software

You can access the iServiceDesks Software website at <http://www.iservicedesks.com> or <http://www.sscs.co.th>. From this website, you can obtain information about the company, its products, head office, special events, and career opportunities.

Thailand

Address: SSC Solutions Co., Ltd.25 Alma Link Building,

8th Floor, Chit Lom Alley, Lumpini,

Pathum Wan, Bangkok 10330

Phone: (+66)2 655 3953

Fax: (+66)2 655 3953

Email: info@sscs.co.th

© Copyright 2019-2020 iServiceDesks software.

iServiceDesks software is the exclusive properties of iServiceDesks software which is registered in Thailand, and may be registered or pending registration in other countries.

The information included in this documentation is the proprietary and confidential information of iServiceDesks software, its affiliates, or licensors. Your use of this information is subject to the terms and conditions of the applicable End User License agreement for the product and to the proprietary and restricted rights notices included in the product documentation.

Restricted rights legend

Thailand Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THAILAND. Use, duplication, or disclosure of any data and computer software by the Thailand Government is subject to restrictions, as applicable as amended from time to time. Any contract notices should be sent to this address.

Customer Support

You can obtain technical support by using the Support page on the iServiceDesks website or by contacting Customer Support by telephone or email. To expedite your inquiry, please see “Before Contacting iServiceDesks support team”.

Support website

You can obtain technical support from iServiceDesks on business day, working hour (8:30am – 5:30pm) at <http://www.iservicedesks.com>. Unless you have premium services, 24 hours a day and 7 days a week. From this website, you can:

- Read overviews about support services and programs that iServiceDesks software offers.
- Find the most current information about iServiceDesks software products.
- Order or download product documentation.
- Report a problem or ask a question.
- Subscribe to receive email notices when new product versions are released.
- Find local support center locations and contact information, including email addresses, fax numbers, and telephone numbers.

Support by telephone or email

In Thailand, if you need technical support and do not have access to the Web, call (+66) 2 655-3953 or send an email message to info@sscs.co.th (In the Subject line, enter CusID:<yourSupportContractID>, such as CusID:12345.)

Before contacting iServiceDesks support team

Have the following information available so that Customer Support can begin working on your issue immediately:

- Product information
 - Product name
 - Product version (release number)
 - License number and password (trial or permanent)
- Operating system and environment information
 - Machine type
 - Operating system type, version, and service pack
 - System hardware configuration
 - Serial numbers
 - Related software (web server, database and other application) including type, version, and service pack or maintenance level
- Sequence of events leading to the problem
- Commands and options that you used
- Messages received (and the time and date that you received them)
 - Product error messages
 - Messages from the operating system, such as file system full
 - Messages from related software
- Debug mode and logging for investigation
 - Turn on debug mode
 - Post the recent log files to developer

Chapter 1.....	8
Introducing iServiceDesks	8
<i>About iServiceDesks</i>	8
<i>What you can do with iServiceDesks</i>	9
<i>How iServiceDesks works</i>	17
<i>Document Resources</i>	19
Chapter 2.....	21
Understanding iServiceDesks concepts	21
<i>Components of iServiceDesks</i>	21
<i>How Process IDs work</i>	22
<i>About iServiceDesks licenses</i>	23
Chapter 3.....	24
Login Service	24
<i>About the Login Service</i>	24
<i>Requesting a password reset</i>	25
Chapter 4.....	26
Managing Service Request	26
<i>Introducing the Request Entry console</i>	26

<i>Submitting a service request (user method)</i>	30
<i>Submitting service requests (technician method)</i>	37
<i>Resolving service requests</i>	38
Chapter 5	40
Managing Incidents	40
<i>Introducing Incident Management</i>	40
<i>Submitting Incidents (user method)</i>	52
<i>Submitting incidents (technician method)</i>	60
<i>Resolving incidents</i>	63
Chapter 6	66
Managing Problems	66
<i>Introducing problem management</i>	66
<i>Submitting problems</i>	75
<i>Relating incidents to a problem ticket</i>	76
<i>Working a problem ticket</i>	76
<i>Creating a change request from a problem</i>	77
<i>Reviewing a proposed fix or workaround</i>	78
Chapter 7	80
Managing Changes	80
<i>Introducing Change Management</i>	80
<i>Submitting change requests</i>	92
<i>Approving and implementing changes</i>	100

Chapter 8.....	102
Managing your Organization’s Knowledge	102
<i>Introducing Knowledge Management.....</i>	<i>102</i>
<i>Processing requests for knowledge base entries.....</i>	<i>107</i>
<i>Managing the knowledge base</i>	<i>114</i>
<i>Using the knowledge base.....</i>	<i>116</i>
Chapter 9.....	119
Communicating in the Process Manager portal	119
<i>Emailing in the Process Manager portal</i>	<i>119</i>
Chapter 10	121
Viewing and Organizing Reports.....	121
<i>Introducing organizing reports.....</i>	<i>121</i>
<i>Viewing a report</i>	<i>122</i>
Chapter 11	124
Setting up and Managing iServiceDesks	124
<i>Configuring iServiceDesks.....</i>	<i>124</i>
<i>Managing security, users, roles, groups, and permissions</i>	<i>135</i>
<i>Managing the LDAP connections</i>	<i>145</i>
<i>Managing Application Programming Interface (API)</i>	<i>148</i>
<i>Managing Workflow Designer.....</i>	<i>150</i>
<i>Debug mode and logging.....</i>	<i>153</i>

Chapter 1

Introducing iServiceDesks

This chapter includes the following topics

- [About iServiceDesks](#)
- [What you can do with iServiceDesks](#)
- [How iServiceDesks works](#)
- [Document Resources](#)

About iServiceDesks

The iServiceDesks can help to improve your infrastructure's service management. It is best practice of ITIL standard includes all of the primary ITIL Service Management processes. These processes include Service Request, Incident Management, Problem Management, Change Management and Knowledge Management. It also includes an LDAP (Lightweight Directory Access Protocol) that lets users easily and securely reset password and access network shares.

iServiceDesks uses the pre-defined standard workflow to manage service tickets, provide reports, and integrate with the Knowledge Management Database (KMDB).

What you can do with iServiceDesks

iServiceDesks contains several pre-defined ITIL-based modules for managing your service environment. These modules can help you manage incidents, changes, problems and knowledge. In addition, iServiceDesks provides a module for managing your LDAP self-service request. When installing iServiceDesks.



Figure 1-1 iServiceDesks modules

An iServiceDesks web-based GUI is a collection of pre-defined standard workflow processes, administrative interfaces and portal extensions that address a specific business need for your environment. Each iServiceDesks module represents a core process in best practice of ITIL.

It contains the following modules to help you organize and manage your service environment:

Table 1-1 Modules in iServiceDesks

Module	Description
Service Request	<ul style="list-style-type: none"> ■ Contains an ITIL-based Service Request Management system. ■ Includes the Service Request Management pre-defined standard workflow process with request forms containing the following information.

Module	Description
	<ul style="list-style-type: none"> • Who raises the request? • Who opens the request? • Email of Requestor • Category or system name or service name • Request Type • Stage or Status • Assign to, person who take next action • Subject and Description to explain the request • Work done • Note or comment • Attachment <ul style="list-style-type: none"> ■ Lets the administrator to customize workflow design ■ Lets the authorized person to create, update the service request ticket. ■ Able to display the service request on tabular format. ■ Lets the user to search with keyword and display all associated request tickets. ■ Lets the user to download all list of service requests in CSV format with Thai language support. ■ Lets the service request ticket to relate with incident, problem and change and knowledge management. ■ Lets the user to write note records to communicate with support team. ■ Lets the user to upload images or associate files. ■ Lets the users submit requesting and lets the technical support workers respond to and work done the ticket. ■ Able to display history or audit trail of the request.

Module	Description
	<ul style="list-style-type: none"> ■ Lets the users to receive a notification via email or line chat. Then navigate the users to see the ticket detail immediately by using token, no login is required. ■ Lets the users to receive an email for customer satisfaction survey when the ticket is Closed. ■ Able to retrieve and save the Google geographic location.
Incident Management	<ul style="list-style-type: none"> ■ Contains an ITIL-based Incident Management system. ■ Includes the Incident Management pre-defined standard workflow process, submitting the incident ticket with containing the following information. <ul style="list-style-type: none"> • Who raises the incident? • Who opens the incident? • Email of Requestor • Category or system name or service name • Impact, Urgency and Priority • Stage or Status (active, resolved, closed, rejected) • Assign or escalate to, person who take next action • Subject and Description to explain the request • Investigation Result • Resolution • Note or comment • Attachment ■ Lets the administrator to customize workflow design ■ Lets the authorized person to create, update the incident ticket.

Module	Description
	<ul style="list-style-type: none"> ■ Able to display the incident ticket on tabular format. ■ Lets the user to search with keyword and display all associated incident tickets. ■ Lets the user to download all list of incident tickets in CSV format with Thai language support. ■ Lets the incident ticket to relate with service request, problem, change and knowledge management. ■ Lets the user to write note records to communicate with support team. ■ Lets the user to upload the image or associate files. ■ Lets the users submit incidents and lets the technical support workers respond to and resolve the incidents. ■ Able to display history or audit trail of the incident. ■ Lets the users to receive a notification via email or Line chat. Then navigate the users to follow up the ticket detail immediately by using token, no login is required. ■ Lets the users to receive an email for customer satisfaction survey when the ticket is Closed. ■ Able to retrieve and save the Google geographic location. ■ Able to transfer the incident ticket to the Helpdesk person automatically based on the group team who has the lowest work queue at the moment. ■ Able to creating a change request from an incident.

Module	Description
	<ul style="list-style-type: none"> ■ Email notification to submitter or the user on whose behalf someone submitted the incident when an incident exceeds SLA.
Problem Management	<ul style="list-style-type: none"> ■ Contains an ITIL-based Problem Management system. ■ Includes the Problem Management standard pre-defined workflow process, submitting the problem ticket with containing the following information. <ul style="list-style-type: none"> • Who raises the problem? • Who opens the problem? • Email of Requestor • Category or system name or service name • Impact, Urgency and Priority • Stage or Status • Assign to, person who take next action • Subject and Description to explain the request • Root Cause • Resolution ■ Lets the authorized person to create, update the problem ticket. ■ Able to display the problem ticket on tabular format. ■ Lets the support team to search and display all problem tickets. ■ Lets the support team to download all list of problem tickets in CSV format with Thai language support. ■ Lets the problem ticket to relate with service request, incident, change and knowledge management. ■ Lets the support team to write note records to communicate with support team.

Module	Description
	<ul style="list-style-type: none"> ■ Lets the support team to upload images or associate files. ■ Lets the support team submit problem tickets and lets the technical support workers respond to and resolve the problem ticket. ■ Able to creating a change request from a problem.
Change Management	<ul style="list-style-type: none"> ■ Contains an ITIL- based Change Management system. ■ Provides a process for standardizing the methods and procedures for handling changes in the organization to minimize the effect of those changes on services, submitting the change ticket with containing the following information. <ul style="list-style-type: none"> • Who raises the change? • Who opens the change? • Email of Requestor • Category or system name or service name • Impact, Urgency and Priority • Stage or Status (Active, Resolved, Closed, Rejected) • Assign to, person who take next action • Subject and Reason of Change to explain the request • Impact, Risk Information • Deployment and Rollback Activity • Downtime and Schedule • Customer approval • CAB decision and comment ■ Lets the authorized person to create, update the change ticket. ■ Able to display the change ticket on tabular format. ■ Lets the support team to search and display all change tickets.

Module	Description
	<ul style="list-style-type: none"> ■ Lets the support team to assign the ticket to CAB for approval or reject. ■ Lets the support team to download all list of change tickets in CSV format with Thai language support. ■ Lets the change ticket to relate with service request, incident, problem and knowledge management. ■ Lets the support team to write note records to communicate with support team. ■ Lets the support team to upload images or associate files. ■ Lets the support team submit problem tickets and lets the technical support workers respond to and resolve the problem ticket. ■ Able to display history or audit trail of the request.
Knowledge Base Management	<ul style="list-style-type: none"> ■ Provides a process for managing your knowledge base, which includes gathering, analyzing, storing, and sharing knowledge and information within an organization. ■ Provides a data repository that stores information on Forum & Community, Case Study and known errors. ■ Improves your efficiency by reducing the need to rediscover knowledge. ■ Lets the user to search with keyword and display all associated knowledge tickets ■ Lets the support team to review and approve before publishing.
Administrative	<ul style="list-style-type: none"> ■ Create a user id, group, title, department, etc. ■ User is able to login by user id or email address.

Module	Description
	<ul style="list-style-type: none"> ■ Able to comply the password policy standard. <ul style="list-style-type: none"> • Password contains complexity <ul style="list-style-type: none"> • Numeric • Small letter, Capital letter • Special character • Password length is configurable ■ Notification of Service Request and Incident to each user is configuration. ■ User is able to change their own profile such as avatar, password, font size apparent, title, department, email address and phone number. This is to reduce work by administrator on daily basis. ■ Fully Thai language support for display, input data and export data file. ■ Provide the access log such as login, logout records. ■ Contains a collection of self-service request processes for interacting with the Lightweight Directory Access Protocol (LDAP) domain. ■ Able to define the Incident Service Level Agreement (SLA) and enable/disable function ■ Able to interface with hardware or application to open an incident request. ■ Using Workflow Designer to customize a new workflow.
Organization Reports	<ul style="list-style-type: none"> ■ The Organization Reports on the Dashboard includes <ul style="list-style-type: none"> • Incident Report category by SLA (pass, fail, overdue)

Module	Description
	<ul style="list-style-type: none"> • Incident Report category by Stage • Incident Report category by Priority • Change Request category by Stage • Change Request category by Priority

Currently, the pre-defined workflow standard provides 3 tiers working group.

1st tier would be end-user, requestor, business user or manager for approval the request.

2nd tier would be Helpdesk or Service Desk who help to dispatch the ticker to the next level.

3rd tier would be Infrastructure team, Network team, Software team or other support team.

How iServiceDesks works

iServiceDesks is a bundling of ITIL-based core processes that run on the pre-defined standard workflow engine. This software helps you to manage both ITIL domains, Service Operation and Service Transitions.

Service Operation – Service Fulfillment, Incidents Management and Problem Management

Service Transition – Change Management and Knowledge Management

iServiceDesks has several key features to help you manage your service environment.

Table 1-2 Key features of iServiceDesks

Feature	Description
Ready-to-use ITIL-based process modules	<ul style="list-style-type: none"> ■ All iServiceDesks processes are ITIL-based, which lets you implement an ITIL solution.

Feature	Description
	<ul style="list-style-type: none"> ■ iServiceDesks includes a set of high-quality, ITIL-based processes that have undergone extensive testing and development effort.
Process-driven forms	<ul style="list-style-type: none"> ■ The default forms that iServiceDesks contains are process-driven rather than data-driven. ■ The user is not shown all of the available information for the form. Instead, the user is only shown what is relevant for the particular point they are at in the process. The user is only shown the information they need to see to move forward with the process. ■ This narrowing of focus helps ensure that the process is followed correctly, and makes following the processes easier for new users.
Business hours support	<ul style="list-style-type: none"> ■ Business hours support allows for accurate Service Level Agreement reporting and accurate reporting of average response time and resolution time. ■ Lets you define the normal business hours for your organization, which accounts for holidays and weekends.
Email templates and notifications	<ul style="list-style-type: none"> ■ The email notifications, which automation rule sets trigger, keep users aware of changes to ticket status, and allow users to verify that issues are resolved. ■ In any process, email notifications can be used to notify the contacts that are associated with a ticket, to assign tasks, and to send alerts.

Feature	Description
Line Chat notifications	<ul style="list-style-type: none"> ■ The Line Chat notifications, which automation rule sets trigger, keep users aware of changes to ticket status, and allow users to verify that issues are resolved. ■ In any process, line chart notifications can be used to notify the contacts that are associated with a ticket, to assign tasks, and to send alerts.
Service Level Agreement (SLA)	<ul style="list-style-type: none"> ■ Default SLA time frames can be established. ■ You can define the SLA time frames in iServiceDesks Administrator according to your corporate policy.
Customer Satisfaction Survey	<ul style="list-style-type: none"> ■ Lets the primary contact for an incident complete a Customer Satisfaction Survey to scoring the service and the resolution.
Reporting	<ul style="list-style-type: none"> ■ CSV report is provided as a report and download to your client PC. ■ Dashboard can show Active status and bar chart of ticket records.
Security at page level	<ul style="list-style-type: none"> ■ Secure processes, forms, and data at the group level to access each web page using pre-defined User Authorization Matrix (UAM).

Document Resources

Use the following documentation resources to learn about and use this product.

Table 1-3 Documentation resources

Document	Description	Location
----------	-------------	----------

Implementation Guide	Information about how to install, configure, and implement this product.	<ul style="list-style-type: none"> ■ The Documentation Library, which is available in iServiceDesks Manual menu.
User Manual	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	<ul style="list-style-type: none"> ■ The Documentation Library, which is available in iServiceDesks Manual menu.

Chapter 2

Understanding iServiceDesks concepts

This chapter includes the following topics:

- [Components of iServiceDesks](#)
- [How Process IDs work](#)
- [About iServiceDesks licenses](#)

Components of iServiceDesks

The components of iServiceDesks combine to let you use ITIL-based processes to manage service tickets and your organization's knowledge.

Table 2-1 Components of iServiceDesks

Component	Description
iServiceDesks solution software	<ul style="list-style-type: none">■ Installed on the iServiceDesks Management multiple platforms such as Microsoft Windows and Linux.■ Support mobile responsive on Safari browser (iOS) and Android browser.■ Cloud service 24x7 is also support.
iServiceDesks modules	<ul style="list-style-type: none">■ Contain the predefined, ITIL-based processes. These processes let you manage service request, incidents, problem, changes and knowledge.

Component	Description
	<ul style="list-style-type: none"> ■ After installation, you must configure these processes to meet the needs of your organization.
Process Manager Portal	<ul style="list-style-type: none"> ■ A Web-based interface that resides on the iServiceDesks server and provides access to the iServiceDesks processes. ■ Lets the users access the Process Manager portal from a Web browser to run the iServiceDesks processes.
Process Manager database	<ul style="list-style-type: none"> ■ Stores the Process Manager details such as groups, users, and permissions and stores persistent workflow data. ■ Must reside on the Database Server computer.
Knowledge Management Database (KMDB)	<ul style="list-style-type: none"> ■ A repository of the information that is related to all the components or resources of an information system. ■ In the ITIL context, the KMDB represents the repository of knowledge organization.

How Process IDs work

The process ID, sometimes called the incident ID, is a unique, numeric value that is generated when a process is first run. For example, when you create an incident, a process ID is created for that incident. When you create a problem, a process ID is created for that problem. You can search for process IDs. The process IDs let you view all the events and items that are associated with that process.

Table 2-2 Segments of the process ID

Segment	Description
Prefix	<p>Represents the process type.</p> <p>The prefixes that are used in the process ID are as follows:</p> <ul style="list-style-type: none"> ■ SR: Service Request ■ INC: Incident Management ■ PRB: Problem Management ■ CHG: Change Management ■ KM: Knowledge Management
Number	<p>A numerical value that is generated automatically and incremented for each subsequent process of the same type. The number is incremented every time the task is worked. For example, a new incident is assigned process ID INC-000009.</p>

About iServiceDesks licenses

The iServiceDesks licenses that you purchased determine the number of people who can work in the iServiceDesks portal at one time. A license is consumed when a logged-on user has an iServiceDesks **Process View** page open to work a ticket for any of the iServiceDesks processes.

The iServiceDesks licensing is IP-based. Therefore, a user can run one instance of iServiceDesks on one computer.

This software support both Thai and English language input with local time zone.

Login Service

This chapter includes the following topics:

- [About the Login Service](#)
- [Requesting a password reset](#)

About the Login Service

First of all, who going to use iServiceDesks must register by providing your name, email address to Administrator. Then Administrator will create a user account and sending a temporary password to that email address accordingly. With this security method, nobody knows the password even Administrator.

To achieve this, Administrator should decide which authentication must be used between LDAP (Lightweight Directory Access Protocol) and Native Authentication

LDAP user authentication is the process of validating a username and password combination with a directory server such MS Active Directory, OpenLDAP or OpenDJ. LDAP directories are standard technology for storing user, group and permission information and serving that to applications in the enterprise.

Authenticating users with an LDAP directory is a two-step process.

Step 1 – Resolving the username to a directory entry attribute

Step 2 – Validating the user password

Another way is using Native Authentication, iServiceDesks will store the user account and encrypted password to its own database. Then using it to validate the password while logging in.

iServiceDesks allow you to login by using your user account or email address for convenient purpose and allow you to change your email address by your own at any time.

Requesting a password reset

For LDAP Authentication, end-user must reset password on LDAP domain as usual before logging to iServiceDesks.

For Native Authentication, end-user can request on iServiceDesks Web Portal for a reset password, the system will send the new password to end-user's email address for using login and change the appropriate password later on.

To request a password reset

- 1 In the login page, click **forget password**.
- 2 Type in **your email** and **verification code** (captcha).
- 3 Click **reset password**.
- 4 You will receive an email with new password.
- 5 Go to login page and enter your email and **new** password.

Chapter 4

Managing Service Request

This chapter includes the following topics:

- [About the Request Entry console](#)

Introducing the Request Entry console

This chapter includes the following topics:

- [About the Service Request Management process](#)
- [Using the Request Entry console](#)
- [Popular Services view of the Request Entry console](#)
- [User scenario](#)

About the Service Request Management process

The goal of Service Request Management is to serve the operational request such as

- A new user account or VPN account
- A new email address
- Reset password
- Request a new PC or laptop

The Service Request Management process is initiated when user creates a ticket.

To initial a request, the user can take the following approaches:

Table 4-1 Service Request Management process

Step	Action	Description
Step 1	A service request is submitted.	<p>A service request is an iServiceDesks ticket that request something.</p> <p>A service request can originate from user help calls or emails, support technicians, and external systems.</p>
Step 2	The service request data is analyzed and assigned to a support technician for responding.	<p>When the service request is submitted, the following actions occur:</p> <ul style="list-style-type: none"> ■ Its data is stored. ■ Any configuration items that pertain to the service request are noted. For example, a specific computer or printer can be associated with the service request. ■ The Helpdesk team will receive the new ticket and assign to appropriate person.
Step 3	A support technician works the service request.	<p>The service request appears in the task list for the technician, group, or organization. If the service request is assigned to a specific technician, the technician receives an email notification.</p> <p>In addition to viewing and responding the service request, the technician can perform other actions.</p> <p>Examples of incident actions are as follows:</p> <ul style="list-style-type: none"> ■ Reassign the ticket back to Helpdesk or another person.

Step	Action	Description
		<ul style="list-style-type: none"> ■ Edit the service request. ■ Manage the related configuration items. ■ Reopen the service request.
Step 4	(Optional) A support technician escalates the service request.	<p>A service request can be escalated when it is close to missing its required resolution date or when it must be resolved at a higher level.</p> <p>A support technician can escalate an incident by assign to appropriate person.</p>
Step 5	The service request is resolved.	<p>The support technician is responsible to assess the requirement and contact the requestor for some more information. Once the service request is executed, the support technician can change the stage in iServiceDesks to Resolved with providing the detail and work done.</p>
Step 6	The user reviews the detail and confirms or re-opens the service request.	<p>The service request appears in the user's task list and the user receives an email notification. The user views the service request's history, comments, and other information.</p> <p>Then the user will check the result and mark the Stage in iServiceDesks as Closed when complete.</p> <p>If the action does not complete, the user re-opens the service request. The service request is re-assigned.</p>

iServiceDesks can be configured to send email notifications to users, helpdesk and support

technician when certain actions are taken in the Service Request Management process.

Using the Request Entry console

The Request Entry console serves as the front-end for the service request. You can use this console to view all service requests or your own requests depend on group level.

The Request Entry console provides an easy-to-use user interface in which you can:

- Search the service request
- Create, view, update, or cancel your service requests
- View the status of your service requests
- Enter requests on behalf of other users in the group level

In addition, the Request Entry console shows the newest service requests to reduce the time that you spend browsing the service request.

Sorting or Ordering Services view of the Request Entry console

The Request Entry console opens with the default sorting all service requests records in the table. Using the sorting or ordering Services view, you can select one of the service requests with a single click on top of the table column. For example, sorting by 'Raised by'.

The Services view lists services in the following order:

- Service Requests order by latest opened date.
- Service Requests can be ordered by other column such as Category or Request Type.
- By default, display 10 maximum records in role of the table.

User scenario

For example, on Monday, you must print presentation materials to distribute in an important meeting to be held in two hours, and require someone to install and setup the printer.

If the optional iServiceDesks Knowledge Management application is available, you can

search for articles in the knowledge base. If you find a solution to your printer problem, you do not need to open a service request.

If you do not have the iServiceDesks Knowledge Management application installed or you do not find a solution in the knowledge base, then you open a new Service Request.

You select the service, enter the required information, and submit the request. This request may go to your supervisor for approval or direct to helpdesk or service desk. You also receive an email notification when the request is assigned to the support technician and work on your request to install and setup the printer.

In the Request Entry console, you view your submitted request and see that its status is In Progress or Active.

When the support technician enters information indicating that the printer is installed, you will receive email notification alerting. You receive an email notification to response your request.

Submitting a service request (user method)

This chapter includes the following topics:

- [Create a New service request](#)
- [Attaching a file to a new service request](#)
- [Attach File to service request dialog box](#)
- [Finding and reviewing your service requests](#)
- [Confirming a service request's completely](#)
- [Reviewing and closing a resolved service request](#)
- [Reopening a service request](#)

Creating a service request

A user who has a requirement can create a request for services. The user creates the service request in iServiceDesks using the general service request form. This form contains the minimum amount of information that is required to create a service request.

When you create a service request, you can perform the following actions:

- 1 In the Request Entry console, click **Add**.
- 2 You can enter detail. The options are as follows.

Table 4-2 Options on the Create a New service request

Option	Description
Raise by	Lets you specify the name who report this service request.
Email	Lets you specify the email address who report this service request and be able to receive email notification when anyone update this ticket.
Request Type	<p>Lets you specify the type or urgency of the service. The options are as follows:</p> <ul style="list-style-type: none"> ■ 1 – Urgent: Require urgency actions. ■ 2 – No Urgent: Require actions as soon as possible. ■ 3 – Query: Require an answer. <p>Your organization or your manager might provide guidelines how to use each of these options.</p>
Category	<p>Lets you specify the category to serve the operational request such as.</p> <ul style="list-style-type: none"> ■ A new user account or VPN account ■ A new email address ■ Reset password ■ Request a new PC or laptop
Expected Date	<p>Lets you select the date on which this service request must be done.</p> <p>When you click this box, the calendar appears. It lets you select the date from a calendar pop-up.</p>

Option	Description
<p>What is your request?</p>	<p>Lets you type a brief description of the request. Make this description as specific as possible. For example, instead of “email problem,” you might type “Please create a new email address”.</p> <p>This description becomes the service request title, which identifies this service request in any service request lists in the Process Manager portal.</p>
<p>Details that might help identify this request</p>	<p>Lets you type additional information to describe the request. For example, you might describe the detail of your requirement or provide more information about what needed.</p>
<p>Location Affected</p>	<p>The iServiceDesks will detect your location by using Google geolocation location service. This can help the Support Technician to know where the incident occurs and be able to reach that place.</p>
<p>Attach File</p>	<p>Lets you attach one or more upload files that provide additional information about the request. For example, you can attach a sample file or a screen image that you captured.</p> <p>If you use mobile phone, the application will allow you to take screenshot and upload this image to the service request automatically.</p> <p>Any files that you attach appear in the Attachment list.</p>
<p>Note</p>	<p>Lets you provide note to the service request.</p> <p>The toolbar that appears in this section provides common text formatting tools.</p>

3 Click button Open Ticket.

- 4 The program will verify your information. If it's incomplete, you need to fill-in the mandatory fields and resubmit again.
- 5 If your account is able to receive notification, please check your mailbox or Line chat.

Attaching a file to a new service request

During service request entry, you can attach one or more files to a service request to provide additional information about the issue. For example, you can attach a sample file or a screen image that you captured. Files larger than 20 MB are not supported.

To attach a file to a service request.

- 1 On the bottom of new service request, click **Upload a File**.
- 2 In the upload file dialog box, select a single file or multiple files.
- 3 When you finish adding files, click **Open** button.
- 4 On the text editor, continue to enter information about the explanation as noted.

The files that you attach to a service request are added to the **Note** tab in the Request form. The files appear under your name and created date time.

You can also attach a file to a service request after it has been created by clicking the **Note** tab.

Attach File to Service Request dialog box

This dialog box lets you attach one or more files to a service request to provide additional information about the explanation. This dialog box appears when you choose to attach a file during the service request entry.

Table 4-3 Options in the Attach File to Incident dialog box

Option	Description
File to Add	Specify the file to add. You can add documents, spreadsheets, text files, logs, and many other file formats such as "jpg", "jpeg", "gif", "png", "tif", "doc", "docx", "wpd", "csv", "xls", "xlsx", "pdf", "pps", "ppt", "pptx", "pub", "txt", "log", "zip", "rar".
Current Attachments	Displays the files that are already attached to the ticket. To remove a file from the ticket, next to the file that you want to remove, click  icon to remove.
Add Another	Adds the file to the Current Attachments list and lets you specify another file to attach without leaving the Attach File to Service Request dialog box.
Add and Close	Adds the current attachments and closes the dialog box.

Finding and reviewing your service requests

You can review the service request that you created. Although you cannot edit a service request, you can perform other actions that are related to the service request.

If the service request is opened or in progress and you have the appropriate permissions, you can perform the following actions:

- Add a note or comment.
- Upload a single file or multiple files.

If the service request is closed, you can only view it.

To find and review a service request

- 1 On the left panel, you will find the Navigator menu, click **Service Request**.
- 2 (Optional) if the service request is not listed, type one or more keywords and click the **Search** symbol (magnifying glass).
- 3 On the table, select the service request by its ticket number.
- 4 On the service request's **Process View** page, view the service request or take whatever actions are necessary.
- 5 When you finish, close the service request 's **Process View** page.

Confirming a service request's work done

After a service request is resolved, it appears in the affected user's task list for review of its, comments, and other information about its work done.

Table 4-4 Confirming a service request's work done process

Step	Action	Description
Step 1	Review the task and if necessary, take any steps that the support technician recommends.	You might need to take steps to complete it by yourself if the support technician provided instructions for doing so. For example, you might be directed to a knowledge base article or a Service Request option that contains work done instructions.
Step 2	Test to confirm that the request is completed.	This step is important whether you complete testing by yourself, or somebody takes action for you.
Step 3	If the request is not	When you re-open the service request, it is returned to a

Step	Action	Description
	completed or if you are dissatisfied with the action taken, re-open the incident.	support technician. After you re-open the service request, wait for another task to notify you that it is resolved.
Step 4	If the request is completed, close the service request.	If you are satisfied with the action, the helpdesk or support technician can mark the service request as resolved. The service request is closed when you check the result and confirm to close this ticket.

Reviewing and closing a resolved

After a service request is resolved, it appears in the affected user's task list for review of its history, comments, and other information about its work done. If the work done is completed, you can confirm the close this ticket.

To review and close a resolved service request.

- 1 Check your mailbox, you should receive the notification when this ticket is **Resolved**.
- 2 To check the result and work done, you can go to the **Process View** page, review the details about the work done and if you are satisfied with the result.
- 3 If you are not satisfied with the actions performed on the service request, click Reopen the service request and add your explanation in **Note** tab.

Reopening a service request

After a service request is resolved, it appears in the affected user's task list for review of its

history, comments, and other information about its work done. If the request is completed, you confirm the work done. If the request is not completed or if you are dissatisfied with the work done, you can reopen the service request.

The service request is returned to a support technician. The technician either response to the request or escalates it to a higher level of support. When the service request is resolved again, you are asked to verify the work done.

To reopen a service request.

- 1 Contact your Helpdesk or reopen by yourselves based on pre-defined workflow process.
- 2 Helpdesk will open the Process Manager portal and change the stage from “Resolved” to “Active” again.
- 3 In the **Note** tab, type an explanation of why you need to reopen the service request.

Provide details about the steps that you took to test the fix and the results of your test.

- 4 (Optional) You can attach files to the service request to support your explanation. The

options are as follows:

Add File	Lets you attach one or more files that provide additional information about the service request. For example, you can attach a sample file or a screen image that you captured.
Remove	Lets you remove a file that is attached to the service request. The attached files are listed under Attachment .

- 5 In the Process View, click **Update** to submit the reopened service request.

Submitting service requests (technician method)

This chapter includes the following topics:

- [Search for Process page](#)

Search for Processes page

This Process page lets you search or sorting all service requests. It performs an automatic search of all the other service requests that are associated with the keyword. You can select from those service requests or search for additional ones.

When you select one of the displayed service requests, it will navigate you to view and edit that service request.

Table 4-5 Options on the Search for Related Processes page

Option	Description
Search for	Lets you type the search keyword and find all related service requests.
Advanced Search	Lets you specify additional search criteria to help find the service request.
Search Results	Displays the service requests and lets you select one on your search result.

Resolving service requests

This chapter includes the following topics:

- [Resolving a service request](#)

Resolving a service request

In response to a telephone call or email from a user, a support technician can record the service request on the service request form. If the service request is resolved immediately, the support technician can resolve the service request at the same time as the service request entry.

For example, a user calls the Helpdesk or Service Desk if require someone to setup a share

drive. During the call, the support technician takes the user through the process of setting up a share drive. When the call is over, the support technician creates and resolves the service request on the service request form.

If you cannot complete the service request, you might need to escalate it to another worker.

To complete a service request form.

- 1 In the Service Request Entry, update the service request on standard form.

Table 4-6 Options on the Service Request page

Option	Description
Work done	<p>Lets you type the work done result for the request.</p> <ul style="list-style-type: none"> ■ What action taken ■ What guideline or instruction to the user? ■ What assumption ■ What is next action
Stage	Lets you select the stage for Resolved or Closed .

- 2 When you finish entering information about the service request, click **Resolved**.
- 3 On the Resolution page, type in the necessary information about the **Work done Result**, Guideline or Instruction.

Note that you can search a knowledge base article or other content be created based on this guideline or instruction by checking Create a Knowledge Base Article after Stage is **Closed**.

- 4 When you finish entering details about the request, on the Resolution page, click **Update** ticket.

Chapter 5

Managing Incidents

This chapter includes the following topics:

- [Introducing Incident Management](#)
- [Submitting incidents \(user method\)](#)
- [Submitting incidents \(technician method\)](#)
- [Resolving incidents](#)

Introducing Incident Management

This chapter includes the following topics:

- [About Incident Management](#)
- [About the Incident Management process](#)
- [Incident Status](#)
- [Roles in Incident Management](#)
- [Sources of incidents](#)
- [Email notifications from Incident Management](#)
- [Process View page for incidents](#)

About Incident Management

Incident Management is one of the core ITIL-based processes, and one that iServiceDesks users work with the most frequently. With the Incident Management process, users can manage and

quickly resolve incidents and analysts can manage, track, and prioritize issues.

The goal of Incident Management is to recover from incidents and restore service to users as quickly as possible.

Incident Management includes the following key features:

- The pre-defined standard workflow lets you execute actions based on potential decision points.
- An intuitive form for users to submit incidents from the self-service portal.
- The ability to include information about the user and the user's assets in the incident data in the incident form.
- The inclusion of specialized tasks that help the technician diagnosing the issue and provide opportunities to either resolve or escalate the issue.
- Opportunities to use the knowledge base to help the technician resolve an incident and to provide additional information to the user.
- The inclusion of the user in the Incident Management process, by letting the user decide if an issue is resolved to their satisfaction. The user can also provide feedback on their service experience.
- The Incident Management process provides information to the other iServiceDesks processes as follows:
 - A collection of incidents that can be used in Problem Management to identify root causes of incidents. When the root causes are identified, they can be resolved to prevent further incidents from occurring.
 - Information from the incidents, which is used in Change Management to determine how to standardize methods and procedures for efficient handling of all changes.

About the Incident Management process

The goal of Incident Management is to recover from incidents and return the user to an operational state as quickly as possible.

iServiceDesks can be configured to send email notifications to users and other workers when certain actions are taken in the Incident Management process.

Table 5-1 Incident Management process

Step	Action	Description
Step 1	An incident is submitted.	An incident is an iServiceDesks ticket that reports an issue. Incidents can originate from user help calls or emails, support technicians, and external systems.
Step 2	The incident data is analyzed and assigned to a support technician for resolution.	When the incident is submitted, the following actions occur: <ul style="list-style-type: none"> ■ Its data is stored. ■ Any configuration items that pertain to the incident are noted. For example, a specific computer or printer can be associated with the incident. ■ Its priority is calculated based on impact and urgency. ■ Its assigned to the Default Incident Queue that is associated with the helpdesk group. ■ The Helpdesk team will receive the new ticket and assign to appropriate person.
Step 3	A support technician	The incident appears in the task list for the technician,

Step	Action	Description
	works the incident.	<p>group, or organization. If the incident is assigned to a specific technician, the technician receives an email notification.</p> <p>In addition to viewing and resolving the incident, the technician can perform other actions.</p> <p>Examples of incident actions are as follows:</p> <ul style="list-style-type: none"> ■ Reassign the ticket. ■ Edit the incident. ■ Manage the related configuration items. ■ Reopen the incident. ■ Submit a knowledge base article when it's closed.
Step 4	(Optional) A support technician escalates the incident.	<p>An incident can be escalated when it is close to missing its required resolution date or when it must be resolved.</p> <p>A support technician can escalate an incident by assign to appropriate person.</p>
Step 5	The incident is resolved.	<p>The support technician is responsible to investigate and diagnose the symptom. These processes take place during troubleshooting when the initial incident hypothesis is confirmed as being correct. Once the incident is diagnosed, the support technician can apply a solution, such as changing software settings, applying a software</p>

Step	Action	Description
		<p>patch, or ordering new hardware.</p> <p>For resolution and recovery, when the support technician confirms that the user's service is restored within the stipulated SLA time, the incident ticket can be changed stage to Resolved and provide the detail of resolution.</p>
Step 6	<p>The user reviews the resolution and confirms or re-opens the incident.</p>	<p>The incident resolution appears in the user's task list and the user receives an email notification. The user views the incident's history, comments, and other information. If the support technician provided instructions for self-service or for testing, the user follows the instructions.</p> <p>If the resolution fixes the issue, the user confirms the fix and provides customer feedback. The incident is marked as Closed.</p> <p>If the resolution does not fix the problem, the user re-opens the incident. The incident is re-assigned.</p>
Step 7	<p>(Optional) The support technician performs the post-resolution activities.</p>	<p>The user's response appears in the support technician's task list and the technician receives an email notification.</p> <p>If the user closes the incident, the support technician can take any of the following actions:</p> <ul style="list-style-type: none"> ■ Submit the resolution details to the knowledge base team to be integrated into an Incident article or FAQ.

Step	Action	Description
		<ul style="list-style-type: none"> ■ Open a Problem ticket to find the root cause. ■ Re-open the incident ticket. <p>If the user or the technician re-opens the incident, the resolution steps are repeated.</p>

Incident status

The incident status accurately reports the progression and outcome of the stages of the Incident Management process. The percentage represents the level of completion that the process has reached. For example, if the time consume of percentage is 60, it means that the process is 60 percent completion against SLA.

The status and percentage appear in the Process Manager portal. For example, they appear in the table of the incident tickets.

Table 5-2 The Default Incident status

Status	Description
Received	The incident was submitted and is ready to be worked.
Assigned to	The incident was assigned to a designated person or group for resolution.
Hold or Pending	<p>The incident is scheduled for later and is placed on hold.</p> <p>Typically, this status means that more research or analysis needs to be performed.</p>
Working	In the process of diagnosing and analyzing the problem And complete corrections Including informing relevant persons To proceed to the next step.

Status	Description
Resolved	A resolution for the entire incident was provided and the incident is ready for the user's approval. The resolution must apply to the entire incident, not to a single subtask.
Rejected or Cancelled	In case of misunderstandings or opening a wrong type of request. The incident should be rejected or cancelled.
Closed	All manual actions and automated actions within the process are complete and the incident is closed.

Roles in Incident Management

iServiceDesks employs roles to define responsibilities for and assign owners to the tasks and other activities within the ITIL processes.

The roles in the Incident Management process are tasked with submitting incidents and resolving them as quickly as possible.

Table 5-3 Roles in Incident Management

Role	Description
User	The user can be anyone inside or outside the organization who submits an incident. The user typically has limited access to the iServiceDesks processes.
Support Technician	The support technician is a worker in the organization's support department who manages incidents. Organizations can set up their own levels of technicians.

Role	Description
	<p>For example, first-level technicians can monitor incoming incidents, take support calls, and resolve incidents. If the incident cannot be resolved immediately or if it requires research or escalation, the technician can assign the incident to a second-level technician. The second-level technicians can perform incident analysis and resolve or escalate incidents.</p> <p>An incident can be assigned to a user, group, or organization. When an incident is assigned to a user or a group, it is added to a queue from which workers can select it.</p> <p>Some organizations might use a third level of support. Typically, this level represents an external vendor or a manufacturer of hardware or software.</p>
Helpdesk	<p>A typical help desk performs a single point of contact for users to gain assistance in troubleshooting, and to ensure that end users are receiving the appropriate assistance with high levels of customer service. A helpdesk generally manages its requests through the use of iServiceDesks such as issue tracking systems. This iServiceDesks allows the helpdesk to track and sort user requests with the help of a unique number, and can frequently classify problems by user, computer program, or similar categories. Then assign the appropriate ticket to Support Technician.</p>
Administrator	<p>To use iServiceDesks at the first time, many configurations need to be setup by the Administrator as follows.</p> <ul style="list-style-type: none"> ● Create and update a user account and group

Role	Description
	<ul style="list-style-type: none"> ● System Name (must be added or update for 1st use) ● Impact (pre-defined default configuration) ● Urgency (pre-defined default configuration) ● Priority (pre-defined default configuration) ● Stage (pre-defined default configuration) ● Notification by email and Line Chat ● Service Level Agreement (SLA) ● LDAP configuration
Guest	Role to access the application from the self-service portal. Only viewing purpose, no ability to update or create a new ticket.

Sources of iServiceDesks incidents

The creation of an incident triggers the Incident Management process. An incident can originate from several sources.

Table 5-4 Sources of iServiceDesks incidents

Source	Description
User	A user inside or outside organization reports an issue by creating an incident in the Process Manager portal.
Helpdesk	Typically, helpdesk is able to create an incident in response to a request from a user, either by telephone or email.

External systems	<p>Your organization can make a web service call (RESTful) to Incident Management and pass in the data that is required to create an incident in iServiceDesks.</p> <p>For example, you might send a message from Microsoft SharePoint, Microsoft InfoPath, Lotus Notes, Microsoft Systems Management Server (SMS), Adobe LifeCycle, and HP OpenView to iServiceDesks system via RESTful protocol for opening a new ticket.</p>
------------------	---

Email notifications from Incident Management

iServiceDesks can send email notifications about incident events. Any action that is taken to create or work an incident ticket can be used as a trigger. You must configure Incident Management to send email notifications.

You can setup email notification to the members when an incident is submitted automatically.

Some examples of incident events that you can use to trigger email notifications are as follows:

Table 5-5 Email notification of iServiceDesks incidents

Event	Email recipient
An incident is submitted.	The submitter or the user on whose behalf someone submitted the incident.
An incident assigned to a specific Support Technician or group.	The assigned technician or group members.

The Support Technician updates the ticket.	The ticket is updated to Resolved stage and provide the detail of resolution.
An incident exceeds SLA	The submitter or the user on whose behalf someone submitted the incident.

Process View page for incident tickets

The **Process View** page is the primary interface for working a task. The **Process View** page appears when you select a task from your **Task List** or from another list in the Process Manager portal.

In addition to the common actions that you can perform for all tasks, the incident **Process View** page contains additional, incident-specific actions. The actions that are available depend on your permissions and the state of the incident. For example, if the incident has been escalated to a higher level, the **Resolve Incident** action is no longer available to you.

The support group of actions on an incident's **Process View** page:

Table 5-6 Incident actions

Action	Description
Reassign Ticket	Lets you assign an incident to a person. For example, a level-one support technician starts to work on an incident but leaves for lunch before the incident is resolved. The incident must be resolved before the technician is due to return. Another worker who is at the same level or higher can open the incident, select this option, and resolve the incident.
Work Incident	Lets you begin the incident resolution process. Also lets you change the incident's details, including any extended classifications.

Action	Description
Remove from Hold	Lets you reopen an incident that has been postponed so that it can be worked.

Table 5-7 Related to Problem and Change Management

Action	Description
Create or Relate to a Problem	<p>Lets you create a problem ticket based on the incident if the incident represents a recurring issue.</p> <p>Lets you search for and view existing problem tickets. Then associate the incident with an existing problem ticket, if you find a problem ticket that addresses your incident.</p>
Request Change	Lets you create a change request based on the incident if the incident represents a recurring issue.

Table 5-8 Smart Tasks

Action	Description
Edit Incident	Lets you update the incident details such as investigation result, resolution, fixed date and change stage to Resolved .
Relate to	Lets you tight another incidents, changes, and problems to this incident.
Hold Management	<p>Lets you change the stage to Hold or Pending.</p> <p>When you hold or pending an incident, it is no calculating the SLA until you turn it on Active running again.</p>

Action	Description
Reopen Incident	Lets you reopen a closed incident.
Note	Lets you leave note to appropriate person for taking action or evident purpose.
Upload file or picture	Lets you take picture or upload image file to iServiceDesks.
Knowledge Management	Lets you post to a knowledge base article or a FAQ that contains resolution instructions.

Submitting Incidents (user method)

This chapter includes the following topics:

- [Create a New Incident](#)
- [Attaching a file to a new incident](#)
- [Attach File to Incident dialog box](#)
- [Finding and reviewing your incidents](#)
- [Confirming an incident's resolution](#)
- [Reviewing and closing a resolved incident and submitting feedback on an incident resolution](#)
- [Reopening an incident](#)

Creating an incident

A user who has an issue can create an incident to report the problem. The user creates the incident in iServiceDesks using the general incident form. This form contains the minimum amount of information that is required to create an incident.

When you create an incident, you can perform the following actions:

- 1 In the Incident Management portal, click **Add**.
- 2 You can enter detail. The options are as follows.

Table 5-9 Options on the Create a New Incident

Option	Description
Raise by	Lets you specify the name who report this incident.
Email	Lets you specify the email address who report this incident
What is your issue?	<p>Lets you type a brief description of the issue in the Subject field. Make this description as specific as possible. For example, instead of “email problem,” you might type “Cannot receive external email”.</p> <p>This description becomes the incident title, which identifies this incident in any incident lists in the Process Manager portal.</p>
Details that might help resolve this issue	Lets you type additional information to describe the issue. For example, you might describe the steps to reproduce the issue or provide more information about what happened.
Needed by Date	<p>Lets you select the date on which this issue must be resolved.</p> <p>When you check this check box, a drop-down list appears. It lets you select the date from a calendar pop-up.</p>
Location Affected	The iServiceDesks will detect your location by using Google geolocation location service. This can help the Support Technician to know where the incident occurs and be able to reach that place.
Impact, who is affected?	Lets you specify impact how many people this issue affects. This information is combined with the urgency information to determine the incident’s priority.

Option	Description
	<p>The options are as follows:</p> <ul style="list-style-type: none"> ■ 1 – High: Potentially damaging service impact to customers or all users impacted. ■ 2 – Medium: A significant service is unavailable to the public or some missing functionality. ■ 3 – Low: Single-user business impact, general break/fix issue with no or little business impact.
Urgency	<p>Lets you specify the severity of the issue. The options are as follows:</p> <ul style="list-style-type: none"> ■ 1 – High: Require urgency fixed. ■ 2 – Medium: Require fixed as soon as possible. ■ 3 – Low: Not urgent due to non-financial impact. <p>Your organization or your manager might provide guidelines how to use each of these options.</p>
Attach File	<p>Lets you attach one or more upload files that provide additional information about the incident. For example, you can attach an error log file or a screen image that you captured.</p> <p>If you use mobile phone, the application will allow you to take screenshot and upload to this incident automatically.</p> <p>Any files that you attach appear in the Attachment list.</p>
Note	<p>Lets you provide note to the incident.</p> <p>The toolbar that appears in this section provides common text formatting tools.</p>

Option	Description
Search the Knowledge Base	Lets you search the knowledge base for any articles that are related to your issue. You might find an article that answers your question and eliminates the need to submit an incident.

- 3 Click button Open Ticket.
- 4 The program will verify your information. If it's incomplete, you need to fill-in the mandatory fields and resubmit again.
- 5 If your user account is able to receive notification, please check your mailbox or Line chat.

Attaching a file to a new incident

During incident entry, you can attach one or more files to an incident to provide additional information about the issue. For example, you can attach an error log file or a screen image that you captured. Files larger than 20 MB are not supported.

To attach a file to an incident.

- 1 On the Create a **New** Incident page, click **Upload a File**.
- 2 In the upload file dialog box, select a single file or multiple files.
- 3 When you finish adding files, click **Open** button.
- 4 On the Create a New Incident page, continue to enter information about the incident.

The files that you attach to an incident are added to the **Note** tab in the Process Manager portal. The files appear in a folder whose name is the incident number.

You can also attach a file to an incident after it has been created by clicking the **Note** tab.

Attach File to Incident dialog box

This dialog box lets you attach one or more files to an incident to provide additional information about the issue. This dialog box appears when you choose to attach a file during the incident entry.

Table 5-10 Options in the Attach File to Incident dialog box

Option	Description
File to Add	Specify the file to add. You can add documents, spreadsheets, text files, logs, and many other file formats such as "jpg", "jpeg", "gif", "png", "tif", "doc", "docx", "wpd", "csv", "xls", "xlsx", "pdf", "pps", "ppt", "pptx", "pub", "txt", "log", "zip", "rar".
Current Attachments	Displays the files that are already attached to the ticket. To remove a file from the ticket, next to the file that you want to remove, click  icon to remove.
Add Another	Adds the file to the Current Attachments list and lets you specify another file to attach without leaving the Attach File to Incident dialog box.
Add and Close	Adds the current attachments and closes the dialog box.

Finding and reviewing your incidents

You can review the incidents that you create . Although you cannot edit an incident, you can perform other actions that are related to the incident.

If the incident is open or in progress and you have the appropriate permissions, you can perform the following actions:

- Add a note or comment.
- Upload a single file or multiple files.

If the incident is closed, you can only view it.

To find and review an incident.

- 1 In the Process Manager portal, click **Incident** menu on the left panel.
- 2 (Optional) if the incident is not listed, type one or more keywords and click the **Search** symbol (magnify glass).
- 3 On the **Incident Management** page, select the incident by its ticket number.
- 4 On the incident's **Process View** page, view the incident or take whatever actions are necessary.
- 5 When you finish, close the incident's **Process View** page.

Confirming an incident's resolution

After an incident is resolved, it appears in the affected user's task list for review of its history, comments, and other information about its resolution.

Until you complete the confirmation task, the incident is considered to be completed and require a final action for the Customer Satisfaction Survey.

Table 5-11 Confirming an incident's resolution process

Step	Action	Description
Step 1	Review the task and if necessary, take any steps that the	You might need to take steps to resolve the issue yourself if the support technician provided instructions for doing so. For example, you might be directed to a knowledge base article

Step	Action	Description
	support technician recommends.	or a Service Catalog option that contains resolution instructions.
Step 2	Test to confirm that the issue is fixed.	This step is important whether you resolved the issue, or it was resolved for you.
Step 3	If the issue is not fixed or if you are dissatisfied with the resolution, re-open the incident.	When you re-open the incident, it is returned to a support technician. After you re-open the incident, wait for another task to notify you that it is resolved.
Step 4	If the issue is fixed, close the incident.	If you are satisfied with the resolution, you can mark the incident as resolved. The incident is closed when you confirm that an incident is resolved. Then you might be asked to complete a Customer Satisfaction Survey.

Reviewing and closing a resolved incident and submitting feedback on an incident resolution

After an incident is resolved, it appears in the affected user's task list for review of its history, comments, and other information about its resolution. If the resolution fixes the issue, you can confirm the fix. If the Customer Satisfaction Survey appears to your mailbox, you can also provide feedback on the incident resolution.

To review and close a resolved incident and submit feedback on an incident resolution

- 1 Check your mailbox, you should receive the Customer Satisfaction Survey for your rating

by clicking the number below.

- 5 star – Very Good
 - 4 star – Good
 - 3 star – Satisfy or meet expectation
 - 2 star – Poor, please put your comment for future improvement
 - 1 star – Unsatisfaction, please put your comment for future improvement
- 2 To check the investigation result and resolution, you can go to the **Process View** page, review the details about the resolution and if you are satisfied with the resolution.
 - 3 If you are not satisfied with the actions performed on the incident, click Reopen the incident and add your explanation in **Note** tab.

Reopening an incident

After an incident is resolved, it appears in the affected user's task list for review of its history, comments, and other information about its resolution. If the issue has been resolved you confirm the incident's resolution. If the issue is not fixed or if you are dissatisfied with the resolution, you can request Helpdesk to reopen the incident.

The incident is returned to a support technician. The technician either resolves the issue or escalates it to a higher level of support. When the incident is resolved again, you are asked to verify the resolution and provide feedback.

To reopen an incident

- 1 Contact your Helpdesk
- 2 Helpdesk will open the Process Manager portal and change the stage from “Closed”

to “Active” again.

- 3 In the **Note** tab, type an explanation of why you need to reopen the incident.

Provide details about the steps that you took to test the fix and the results of your test.

- 4 (Optional) You can attach files to the incident to support your explanation. The options are as follows:

Add File	Lets you attach one or more files that provide additional information about the incident. For example, you can attach an error log file or a screen image that you captured.
Remove	Lets you remove a file that is attached to the incident. The attached files are listed under Attachment .

- 5 In the Process View, click **Update** to submit the reopened incident.

Submitting incidents (technician method)

This chapter includes the following topics:

- [Search for Process page](#)
- [Hold and Pending the incident](#)
- [Creating a change request from an incident](#)

Search for Processes page

This Process page lets you search or sorting all incidents. It performs an automatic search of all the other incidents that are associated with the keyword. You can select from those incidents or search for additional ones.

When you select one of the displayed incidents, it will navigate you to view and edit that

incident.

Table 5-12 Options on the Search for Related Processes page

Option	Description
Search for	Lets you type the search keyword and find all related incidents.
Advanced Search	Lets you specify additional search criteria to help find the incident.
Search Results	Displays the incidents that result from your search and lets you select one to attach the email information to.

Hold or Pending the incident

You can hold the assignment and resolution of an incident by changing the stage to **Hold** or **Pending**. When you hold an incident, the SLA duration will not be computed.

If you are ready to work the incident before the hold date, you can change the stage back to **Active**.

What you should do when you hold an incident.

- The status is changed to **Hold** or **Pending**.
- You should add a note to explain why you consider to hold this incident.
- The system will record your update to **History** section.
- The incident is stopped clocking SLA clock temporary.

What you should do when you change to **Active** again.

- The status is changed to **Active**.
- You should add a note to explain why you turn back to **Active** stage.
- The incident is turned back to the SLA clock at its original level. It is not re-

evaluated.

To **Hold** or **Pending** the incident.

- 1 In the Process Manager portal, click **My Task List**.
- 2 On the My Task List page search for and open the incident that you want to hold.
- 3 On the incident's **Process View** page, under **Stage**, change the stage to **Hold** or **Pending**.
- 4 (Optional) In the **Note** dialog box, type a reason for holding the incident.
- 5 Click **Update** button.

Creating a change request from an incident

A support technician or other worker who works an incident can create a change request.

Creating a change request is a step in the Change Management process.

To create a change request from an incident

- 1 In the Incident Request portal, go to bottom of the page.
- 2 Find the button to open a new Change Request and click.
- 3 All information on Incident Request will copy to the new Change Request.
- 4 The system will create **Related Ticket** between this Incident Request and Change Request automatically.

Note that if this action is not available, the Incident Request is probably not finish opening yet. To enable this action, you need to complete opening this incident request first.

- 1 Update information in your incident.
- 2 Click button Update.

- 3 Select this ticket again, then this action would enable to you for opening a new change request.

Resolving incidents

This chapter includes the following topics:

- [Resolving an incident](#)

Resolving an incident

In response to a telephone call or email from a user, a support technician can record the incident on the incident form. If the incident is resolved immediately, the support technician can resolve the incident at the same time as the incident entry.

For example, a user calls the Helpdesk or Service Desk because of a printer jam. During the call, the support technician talks the user through the process of clearing the printer jam. When the call is over, the support technician creates and resolves the incident.

If you cannot resolve the incident, you might need to escalate it to another worker.

To resolve an incident from the incident form.

- 1 In the Process Manager portal, create an incident with the advanced form.

Table 5-13 Options on the Incident Response page

Option	Description
Investigation Result	Lets you type the investigation result for the incident. <ul style="list-style-type: none">■ Suspicion or detection of a cause of one or more incidents■ How to analysis and detect or simulate the problem■ What cause of problem

Option	Description																														
	<ul style="list-style-type: none"> What impact to 																														
Resolution	Lets you type information in the text box about appropriate solution and action taken how to fix.																														
Impact	Lets you define the extent of the issue by specifying how many people the issue affects.																														
Urgency	Lets you specify the urgency of the issue by specifying which service the issue affects.																														
Priority	<p>Automatic calculation the priority of this incident.</p> <table border="1"> <thead> <tr> <th>Impact</th> <th>Urgency</th> <th>Priority</th> </tr> </thead> <tbody> <tr> <td>1 - High</td> <td>1 - High</td> <td>1 - Critical</td> </tr> <tr> <td>1 - High</td> <td>2 - Medium</td> <td>2 - High</td> </tr> <tr> <td>1 - High</td> <td>3 - Low</td> <td>3 - Moderate</td> </tr> <tr> <td>2 - Medium</td> <td>1 - High</td> <td>2 - High</td> </tr> <tr> <td>2 - Medium</td> <td>2 - Medium</td> <td>3 - Moderate</td> </tr> <tr> <td>2 - Medium</td> <td>3 - Low</td> <td>4 - Low</td> </tr> <tr> <td>3 - Low</td> <td>1 - High</td> <td>3 - Moderate</td> </tr> <tr> <td>3 - Low</td> <td>2 - Medium</td> <td>4 - Low</td> </tr> <tr> <td>3 - Low</td> <td>3 - Low</td> <td>5 - Planning</td> </tr> </tbody> </table>	Impact	Urgency	Priority	1 - High	1 - High	1 - Critical	1 - High	2 - Medium	2 - High	1 - High	3 - Low	3 - Moderate	2 - Medium	1 - High	2 - High	2 - Medium	2 - Medium	3 - Moderate	2 - Medium	3 - Low	4 - Low	3 - Low	1 - High	3 - Moderate	3 - Low	2 - Medium	4 - Low	3 - Low	3 - Low	5 - Planning
Impact	Urgency	Priority																													
1 - High	1 - High	1 - Critical																													
1 - High	2 - Medium	2 - High																													
1 - High	3 - Low	3 - Moderate																													
2 - Medium	1 - High	2 - High																													
2 - Medium	2 - Medium	3 - Moderate																													
2 - Medium	3 - Low	4 - Low																													
3 - Low	1 - High	3 - Moderate																													
3 - Low	2 - Medium	4 - Low																													
3 - Low	3 - Low	5 - Planning																													
Stage	Lets you select the stage for Hold , Pending or Resolved .																														

- When you finish entering information about the incident, click **Resolved**.
- On the Resolution page, type in the necessary information about the **Investigation Result** and **Resolution**.

Note that you can search a knowledge base article or other content be created

based on this resolution by checking Create a KB Article after Stage is **Closed**.

- 4 When you finish entering details about the resolution, on the Resolution page, click **Update** ticket.

Chapter 6

Managing Problems

This chapter includes the following topics:

- [Introducing problem management](#)
- [Submitting problems](#)
- [Relating incidents to a problem ticket](#)
- [Working a problem ticket](#)
- [Reviewing a proposed fix or workaround](#)

Introducing problem management

This chapter includes the following topics:

- [About Problem Management](#)
- [About the Problem Management process](#)
- [Problem statuses](#)
- [Roles in Problem Management](#)
- [Sources of problem tickets](#)
- [Email notifications from Problem Management](#)
- [Process View page for problem tickets](#)

About Problem Management

The Problem Management process looks at the root causes of the problems that cause multiple incidents. Problem Management then seeks to take actions to fix the situation and prevent it from recurring. The goal of the process is to minimize the effect of incidents and problems on the business.

To manage problems successfully, you need the ability to perform the following actions:

- Track problems.
- Diagnose the problems.
- Fix the problems through change requests.
- Publish known errors to help with future resolutions.

Part of the Problem Management process is to group related incidents for additional analysis and discovery of root causes. This analysis and discovery let Problem Management take Incident Management a step further. Incident Management seeks to resolve the single issue at hand, so that a user can get up and running again. Problem Management goes deeper and seeks to take the actions that prevent that issue from happening again. When the problem is identified, a change request can be created or a knowledge base article can be requested.

In general, Problem Management deals with the issues that multiple users have encountered. For example, multiple users may experience an issue with a certain software program. Each of these issues can be resolved individually through the Incident Management process. However, the Problem Management process might suggest a Service Pack update for all users of that software. This solution would solve the individual incidents and prevent other users from encountering the issue and creating new incidents.

Problem Management includes the following key features:

- The ability to group incidents so that the root cause that is common to all the incidents

can be analyzed.

- The knowledge base can be used as part of a resolution for a problem, and problems can provide information for the knowledge base.

The Problem Management process provides information to the other iServiceDesks processes as follows:

- Obtains the initial context of a problem from the Incident Management process.
- Provides the context that is related to the problem to assist in the decision making during the Change Management process.
- Provides the documentation from problems to the knowledge base.

About the Problem Management process

The goal of Problem Management is to minimize the effect of problems and known errors that result from systemic issues within the IT infrastructure. The Problem Management process lets you track and diagnose problems, propose actions to resolve the problems, and take action on the problem resolutions.

The Problem Management process is initiated when someone creates a problem ticket.

To identify problems, iServiceDesks workers can take the following approaches:

Table 6-1 The Problem Management process

Step	Action	Description
Step 1	Someone creates a problem ticket.	A problem analyst reviews incidents to find the errors that reoccur frequently and creates a problem ticket for those errors.

Step	Action	Description
Step 2	The problem analyst works the problem ticket.	<p>The problem analyst views the ticket and researches the problem. After the analysis is finished, the analyst updates the problem ticket with additional details, proposes a fix or workaround, and submits the problem for review.</p> <p>When the problem is submitted, a task is created for the problem reviewer.</p>
Step 3	(Optional) A problem worker can add incidents to the problem ticket.	<p>If the problem is related to one or more incidents, they can be associated with the problem ticket. The incidents can help to uncover root causes.</p> <p>Incidents can be added to a problem ticket at any time before the problem reviewer approves the fix or workaround.</p>
Step 4	The problem reviewer reviews the proposal.	<p>The problem reviewer reviews the proposed fix or workaround and decides how to handle it.</p> <p>When the proposal is accepted, the problem reviewer decides whether to create a change request, request the creation of a knowledge base article, or both.</p> <p>When the proposal is rejected, the problem reviewer provides a reason for the rejection. A task is created for the problem analyst, who can decide to rework the problem by repeating Step 2.</p>
Step 5	If the problem reviewer	The change manager reviews the change request and

Step	Action	Description
	requests a change, the problem process waits for the change process.	approves or rejects it.
Step 6	The problem is closed.	<p>The problem ticket can be closed in the following ways:</p> <ul style="list-style-type: none"> ■ The problem reviewer accepts the problem proposal, chooses to request a knowledge base article, and closes the problem ticket.

Problem Status

The problem status accurately reports the progression and outcome of the stages of the Problem Management process.

The status appears in the ticket's **Process View** page.

Table 6-2 Problem Status

Status	Description
Analyze New Problem	The problem ticket is in a waiting state for the problem analyst to review the ticket and propose a resolution.
Awaiting proposal review	The problem analyst proposed a resolution and submitted the problem ticket, which is in a waiting state for the problem reviewer to review the ticket.
Waiting on Change	A change was requested to resolve the problem, which is in a waiting state for the completion of the change process.

Status	Description
Management	
Closed	The problem process is complete. The closure occurs when the problem analyst or reviewer closes the problem.
Schedule Change has been submitted	A change request is submitted to resolve the problem.
Create Document	A fix or workaround for the problem is submitted as a new knowledge base article request.
Solution was rejected	The problem reviewer rejected the problem and returned it to the problem analyst. The problem ticket is in a waiting state for the problem analyst to rework or cancel the problem ticket.

Roles in Problem Management

Depending on their structure, some organizations might have different hierarchy levels and multiple roles for Problem Management. iServiceDesks contains two default groups for Problem Management: Problem Analyst and Problem Reviewer.

Table 6-3 Roles in Problem Management

Role	Description
Problem analyst	<p>Analyzes the root cause of the problem, proposes a solution, and submits the proposal. The proposal can be in the form of a fix or a workaround. Analysts can also remove the problem.</p> <p>In many organizations, the same person fills both the problem analyst and the problem reviewer roles. However, in larger organizations the problem analyst role is assigned to one or more people other than the problem reviewer.</p>
Problem reviewer	<p>Approves the proposed fix or workaround and decides how to handle the problem, or returns the problem to the problem analyst for rework.</p>

ITIL recommends that the same person should not be involved in both Problem Management and Incident Management. The priorities of those processes are not always consistent with each other.

Sources of problem tickets

The creation of a problem ticket triggers the Problem Management process. A problem ticket can originate from several sources.

Table 6-4 Sources of problem tickets

Source	Description
Helpdesk or Service Desk	<p>A typical helpdesk performs a single point of contact for everyone and able to open a problem ticket through the iServiceDesks as you request.</p> <p>Helpdesk also can help to assign the appropriate ticket to Support</p>

Source	Description
	Technician and track the problem until its closed.
Process Manager portal	A problem analyst or other iServiceDesks worker creates a problem ticket and Relate to incidents.
Incident Management	A support worker creates a problem from the Create or Relate to a Problem Ticket action in an incident's Process View page.

Email notifications from Problem Management

iServiceDesks sends email notifications at various stages of the Problem Management process. In this context, a problem event is any action that is taken to create or work a problem ticket. The type of event and the iServiceDesks configurations determine the recipients of the email notifications.

Replies are processed in the following situations:

- The email notification is sent from a process. Such emails contain an identifier to trigger the response.
- The email notification is sent with a default template.

Table 6-5 Default problem events that trigger email notifications

Event	Email recipient
A problem ticket is created.	The submitter and the primary contact, if they are not the same person
A problem worker decides to handle the	The knowledge base editor. The email message requests an article that describes how to handle

Event	Email recipient
problem by creating a knowledge base article.	the problem.

Process View page for problem tickets

The **Process View** page is the primary interface for working a task. The **Process View** page appears when you select a task from your **Task List** or from another list in the Process Manager portal.

In addition to the common actions that you can perform for all tasks, the problem **Process View** page contains additional, problem-specific actions. The actions that are available depend on your permissions and the state of the problem ticket. For example, the **Review Fix or Workaround** action appears only after the problem ticket is reviewed and analyzed.

Table 6-6 Actions on the problem ticket's Process View page

Action	Description
View Problem	Lets you view the details of the problem ticket and select the options or tab that appear. For example, select Note tab and write down a sentence to communicate with technician team.
Assignments	Lets you assign the ticket to another user, group, or organization.
Change Priority	Lets you change the problem ticket's priority. For example, after a problem is created, many incidents that are related to the problem are submitted. In this situation, you might change the problem's priority to a higher level.
Edit Description	Lets you describe the problem accurately.

Action	Description
	For example, when you create a problem from an incident, the problem inherits the incident's description. However, the incident's description is likely to be user-specific while the problem typically represents a more general issue.
Work Problem	Update a problem ticket to provide the cause and a detailed description of the problem. You can also categorize the problem and propose a workaround or a fix.
Review permanent fix	Lets you review the proposed permanent fix, determine how to handle the problem, and approve the problem or return it to the analyst.
Relate to Incident	Lets you add one or more incidents that are related to the problem.

Submitting problems

Report a problem to create a problem ticket to initiate the process of taking measures to prevent an issue that can lead to incidents. Reporting a problem to create a problem ticket is the first step in the Problem Management process.

A problem ticket can also be created from an incident manually, which creates an association between the incident and the problem.

After the problem ticket is created, the problem analyst works the ticket by entering the results of the analysis and proposing a fix or workaround.

To report a problem.

- 1 In the Process Manager portal, click **Problem** menu on left panel.

- 2 On the right side of the page, you will see all list of problem sorting by current date.
- 3 In the Search for field, type the search text to evaluate against incident descriptions, and then click the Search symbol (magnifying glass).
- 4 On the **Create Problem** page, click **Create a New Problem**.
- 5 On the **Submit a New Problem** page, define the problem, and then click **Continue**.

Relating incidents to a problem ticket

If a problem is related to one or more incidents, you can associate the incidents with the problem ticket. You might add the incidents that triggered the problem process, or you might add the related incidents that you discover during the problem analysis.

Relating incidents to a problem ticket is an optional step in the Problem Management process. You can add incidents to a problem ticket at any time before the proposed fix or workaround is approved.

To add incidents to an existing problem ticket

- 1 In the Process Manager portal, click **Relate to** tab.
- 2 In the **Related Ticket** page, select type of service you want to relate to.
- 3 Enter the incident ticket number link to this problem
- 4 When you finish adding incidents, click **Add**.
- 5 When the ticket's Process View page reappears, you can see the relation of incident and problem tickets.

Working a problem ticket

After you analyze a problem, you update the problem ticket to provide the cause and a

detailed description of the problem. You also categorize the problem and propose a fix or a workaround.

Working a problem ticket is a step in the Problem Management process.

After you propose a resolution for the problem, the problem reviewer views the proposal and then takes action.

To work a problem ticket

- 1 In the Process Manager portal, click **Problem** menu on the left panel.
- 2 On the **Problem View** page, record the results of your analysis.

Table 6-7 Problem View page

Action	Description
Root Cause	Lets you describe what you think is the cause of the problem. This option defaults to the text from the problem entry and lets you type additional text.
Propose a Workaround Propose a Fix	Lets you document a workaround or a fix to a problem.

Creating a change request from a problem

A support technician or other worker who works an problem can create a change request.

Creating a change request is a step in the Change Management process.

To create a change request from an problem

- 1 In the Problem Request portal, go to bottom of the page.

- 2 Find the button to open a new Change Request and click.
- 3 All information on Problem Request will copy to the new Change Request.
- 4 The system will create **Related Ticket** between this Problem Request and Change Request automatically.

Note that if this action is not available, the Problem Request is probably no authorized opening yet. To enable this action, you need your admin to grant permission for you.

Reviewing a proposed fix or workaround

After a problem analyst proposes a solution to a problem, you can review the proposal and accept or reject it. When you accept a proposal, you can decide whether to create a change request, request the creation of a knowledge base article, or both. When you reject a proposal, you return the problem to the problem analyst, who can provide additional information and resubmit it.

Reviewing a fix or workaround is a step in the Problem Management process.

If you submit a change request after your review, a problem task with the status **Waiting for Change Request to Complete** appears in the task list.

To review a fix or workaround

- 1 In the Process Manager portal, click **Problem** menu on the left panel.
- 2 On the **Review Proposal** page, review the information about the proposed workaround or fix.
- 3 Select one of the following options:
 - Return Problem to Analyst
 - Approve proposal
- 4 Enter Fix date as same as deployment date

- 5 If you chose to return the problem to the analyst, on the Return to Analyst page, provide the reason for returning the problem, and then click Submit.
- 6 If you chose to create a change request, on the Submit Change Request page, provide the information for the change ticket, and then click Submit Change Request.
- 7 Click Update bottom to saves the information and closes the page.

Chapter 7

Managing Changes

This chapter includes the following topics:

- [Introducing Change Management](#)
- [Submitting change requests](#)
- [Approving and implementing changes](#)

Introducing Change Management

This chapter includes the following topics:

- [About Change Management](#)
- [About the Change Management process](#)
- [Change Management process: Planned state](#)
- [Change Management process: Received State](#)
- [Change Management process: Reviewed state](#)
- [Change Management process: Closed state](#)
- [Actions in the Change Management process states](#)
- [Configuring Change Management](#)
- [About the roles in Change Management](#)

About Change Management

The goal of Change Management is to standardize methods and procedures to ensure the most efficient handling of the changes that an organization requires. An effective Change Management process minimizes how changes affect service and improves the reliability and responsiveness of IT services and processes. This improvement leads to a quicker turnaround on changes and reduces unplanned work, rework, and duplicated efforts.

Change Management includes the following key features:

- Problems can be escalated to a change request or change requests can be initiated independently.
- The change approval board analyzes the risk that is associated with the change as part of the process.
- Supports multiple change managers, each with their own customized rights to tickets and actions.
- All participants review the proposed schedule.
- When the plans are finalized, the change approval board provides final approval, and the implementation task is assigned based on the scheduled date and time.
- When a change request is completed, the problems and incidents that are associated with that change request must be updated with a resolution and closed.

The Change Management process interacts with the other iServiceDesks processes as follows:

- Obtains incident information from the Incident Management process.
- Obtains the documentation of the proposed change from the Problem Management process.
- Serves as a source of information for future knowledge base articles.

About the Change Management process

The Change Management process ensures that standardized methods and procedures are used to handle all changes efficiently and promptly. The process minimizes the effect of any related incidents upon service. Using Change Management improves the reliability and responsiveness of IT services and processes, leading to a higher turnaround of changes. It also reduces rework and the duplication of effort. Standard or common change requests can be expedited. The process includes the ability to define and use templates for quickly completing a change plan.

The Change Management process is initiated when someone requests a change.

The change manager who provides the initial approval of a change request also selects the change type. The change type determines the number of steps that the change implementation requires. It also determines the number of workers who must be involved in each step.

The Change management process consists of the following states:

- Received
- Plan
- Review
- Closed

During the planning phase, the change manager can select one of two variations to tailor the process to the request: Standard or Emergency.

A standard plan change is commonly requested and performed, meaning that procedures, risk and cost are well-understood and CAB approval is not necessary. Essentially, the Planned state is skipped. For example, once a computer has become obsolete, it experiences a standard change

of repurposing or disposal. A standard change is usually scheduled for a later time to coincide with maintenance windows or a release. Typically, an organization has a one-to-one mapping between standard plans and plan templates. This one-to-one mapping is so that if the Standard type is selected, the change manager can find the matching template, and load the plan details.

An emergency change cannot be scheduled for later. If it is designated as an emergency, then it should be implemented immediately following approval by the E-CAB. Like the Standard plan type, the plan details are not required before submission to the CAB.

Change Management process: Planned state

The Planned state is a state in the Change Management process.

The Change Manager has submitted the change plan to the CAB for approval. The change manager selects the CAB during the Received state. The CAB can either approve or reject the plan. The CAB can opt to schedule it for a later time. This state is skipped if the Change Manager chooses the Standard plan type.

The table describes the details of the Planned state in the Change Management process.

Stage	Planned
Brief description:	Change Manager submits the change plan to the CAB for approval.
Initiated by:	Change Manager completes and submits change plan
Players:	Change Approval Board (CAB/ECAB)
Available stage:	<ul style="list-style-type: none"> ■ CAB Options: Approved ■ CAB Options: Rejected ■ Process Action: Edit Change Plan.

	<ul style="list-style-type: none"> ■ Process Action: Manage CABs ■ Process Action: Manage Related Configuration Items ■ Process Action: Manage Related Processes ■ Process Action: Search Knowledge Base
--	--

Change Management process: Received State

The Received state is a state in the Change Management process.

In this state, the Change Manager receives the change request and is ready for planning.

During this state, the Change Manager can delegate portions of the planning to others.

The table describes the details of the Received state in the Change Management process.

Stage	Received
Brief description:	The request has been received and the Change Manager reviews it.
Initiated by:	Change request submitted
Outcome/Next status:	<ul style="list-style-type: none"> ■ Plan completed and submitted to CAB for review (Planned) ■ CAB approval is bypassed and change is scheduled (Reviewed) ■ Request denied Change Management
Players:	Change manager, selected delegates
Available actions:	<ul style="list-style-type: none"> ■ Task: Approve/Deny Change Plan ■ Planning Tasks: Delegate Implementation Plan. ■ Planning Tasks: Delegate Test Plan ■ Planning Tasks: Delegate Backout Plan ■ Planning Tasks: Delegate Other Task

	<ul style="list-style-type: none"> ■ Planning Tasks: Manage Planning Tasks ■ Process Action: Edit Change Plan ■ Process Action: Manage CABs ■ Process Action: Manage Related Configuration Items ■ Process Action: Manage Related Processes ■ Process Action: Search Knowledge Base
--	---

Change Management process: Reviewed state

The Reviewed state is a state in the Change Management process.

In this state, CAB approval was either provided or was not needed. During this phase the change is implemented, either immediately or at the scheduled time.

The table describes the details of the Reviewed state in the Change Management process.

Stage	Reviewed
Brief description:	The change plan has been approved and is scheduled for implementation
Initiated by:	CAB approves Change plan or the Change Manager initiates change directly (for Standard plan)
Outcome/Next status:	<ul style="list-style-type: none"> ■ Change successfully implemented (Closed: Success) ■ Change cannot be implemented (Closed: Failure)
Players:	Implementer is selected during the planning phase
Available actions:	<ul style="list-style-type: none"> ■ Task: Cancel Change ■ Task: Implement Right Away ■ Task: Complete Task ■ Implementation Options: Delegate Implementation Plan

	<ul style="list-style-type: none"> ■ Implementation Options: Manage Implementation Tasks ■ Process Action: Edit Change Plan ■ Process Action: Manage CABs ■ Process Action: Manage Templates ■ Process Action: Manage Related Configuration Items ■ Process Action: Manage Related Processes
--	--

Change Management process: Closed state

The Closed state is a state in the Change Management process.

To reach this state, a close code must be provided. It can be one of the following:

- Success – The change was implemented.
- Failure – The change cannot be implemented for some reason.
- Denied by CM – Change manager denies Request.
- Denied by CAB – CAB denies the plan.

The table describes the details of the Closed state in the Change Management process.

Stage	Closed
Brief description:	No further action is taken on the ticket
Initiated by:	Change Manager denies change request, CAB denies change plan, or Implementer marked change as Completed
Outcome/Next status:	N/A
Players:	N/A
Available actions:	<ul style="list-style-type: none"> ■ Process Action: Edit Change Plan ■ Process Action: Manage CABs ■ Process Action: Manage Templates ■ Process Action: Manage Related Configuration Items

	<ul style="list-style-type: none"> ■ Process Action: Manage Related Processes
--	--

Actions in the Change Management process states

In each state in the Change Management process, specific types of actions are available. Each action is associated with a specific user role.

The following types of actions are available in the Change Management process:

- **Task**

A **Task** is an actual pre-defined workflow step. The completion of a task moves the process along.

- **Planning Tasks, Implementation Options, and CAB Options**

Planning Tasks, Implementation Options, and CAB Options are additional actions, which are specific to a user or a group at a specific moment in the process.

- **Process Action**

A **Process Action** is an action that anyone with the appropriate access level to the process can perform, regardless of process state. This action can be used to edit ticket data directly, and so forth. It may or may not provide an alternative to completing the main task or advancing the process along.

Table 7-1 Change Management process actions

Action	Initiator of Action	Type	Description
Approve/Deny Change Plan	Change Manager	Task	<ul style="list-style-type: none"> ■ Provide state-sensitive elements of the change plan, such as the designated CAB, the change type, and the implementer. ■ Submit the change plan to the CAB, moving

Action	Initiator of Action	Type	Description
			the process to the Planned state.
Delegate Implementation Plan Delegate Test Plan Delegate Backout Plan	Change Manager	Planning Tasks	<ul style="list-style-type: none"> ■ Create tasks for selected delegates to complete portions of the change plan, like the implementation plan or the testing plan. Sets the status for the affected plan elements to Assigned. ■ Remove delegated tasks or change their assignments.
Delegate Other Task	Change Manager	Planning Tasks	<ul style="list-style-type: none"> ■ Provide a generic tasking ability for the Change Manager to use to assign tasks like testing a change ahead of implementing it. These tasks are not bound to the process state, so they do not delay the main process.
Edit Change Plan	Change Manager, selected delegates, CAB	Process Action	<ul style="list-style-type: none"> ■ Provide non-state-sensitive elements of the change plan, such as the risk, cost, and plan elements (implementation, testing, and backout). ■ Implemented as a Process Action to allow editing of a change plan at any process state. Also, anyone with administrative or edit rights to the process can edit the plan.

Action	Initiator of Action	Type	Description
			<ul style="list-style-type: none"> Used by the plan element delegates to provide details for their plan element.
Manage CABs	Change Manager	Process Action, Service Catalog Item	<ul style="list-style-type: none"> Add, remove, and edit CABs (available only to those with administrative rights to the process).
Manage Related Configuration Items	Change Manager	Process Action	<ul style="list-style-type: none"> Associate configuration items from the CMDB with the change request.
Manage Related Processes	Change Manager	Process Action	<ul style="list-style-type: none"> Lets you add or remove the incidents that are associated with the change request. Adding incidents to a change request creates a cascading relationship. Lets you add or remove the problems that are associated with the change request. Adding problems to a change request creates a cascading relationship, whereby the successful completion of the change triggers the closure of any associated incidents.
Approve Change	CAB/ECAB	Task	<ul style="list-style-type: none"> Used by the CAB to move the process to the

Action	Initiator of Action	Type	Description
Plan			<p>next state.</p> <ul style="list-style-type: none"> Can approve or deny change plan. Can add process documents
Complete Task (Fulfill Request)	Implementer	Task	<ul style="list-style-type: none"> Used by the implementer to indicate that the task is complete. Can choose close code of Success or Failure. Must enter comments if close code is Failure.

Configuring Change Management

To configure change management, you define the change manager group. Next you configure access to the change request process view.

Table 7-2 Process for configuring Change Management

Step	Action	Description
Step 1	Define your Change manager group or groups	Your organization may have several different groups responsible for managing incoming change requests. Which group manages the incoming change may depend on the category, location, or other attributes of the request. You must create these groups in the portal and add people to them as needed.

Step	Action	Description
Step 2	Configure Access to the Change Request Process View	The process view page for Change Management is very robust. The page contains a full description of the request. It also contains the current implementation plan, history of the ticket, current assignments, etc. You can grant access to other users or groups to the full view in the User Authorization Matrix inside the database.

About the roles in Change Management

iServiceDesks employs roles to define responsibilities for and assign owners to the tasks and other activities within the ITIL processes. The roles in the Change Management process are tasked with efficiently managing all changes to minimize the effect of any related incidents on service quality.

Table 7-3 Roles in Change Management

Role	Description
Submitter	The submitter is any worker who can request a change. Typically, the submitter is a support technician or manager, a change worker, or a problem manager.
Change Manager (CM)	The change manager can be anyone who is assigned to the Change Manager group. The change manager is responsible for the daily activities of the Change Management process. The change manager authorizes and documents all changes in the IT

Role	Description
	infrastructure and its components (configuration items) to reduce the amount of unplanned downtime.
Change Approval Board (CAB)	The change advisory board (CAB) is a group of people who can advise the change manager in the assessment, prioritization, and scheduling of changes.

Submitting change requests

This chapter includes the following topics:

- [Sources of change requests](#)
- [Requesting a change](#)

Sources of change requests

The creation of a change request triggers the Change Management process. A change request can originate from several sources.

Table 7-4 Sources of change requests

Source	Description
Helpdesk or Service Desk	A typical helpdesk performs a single point of contact for everyone and able to open a change request ticket through the iServiceDesks as you request. Helpdesk also can help to assign the appropriate ticket to Support Technician and track the problem until its closed.
Incident	A support technician or manager can create a change request as follows:

Source	Description
Management	<ul style="list-style-type: none"> From the Submit Request portal page <p>Typically, support technicians create change requests when they see a pattern of similar incidents.</p>
Problem Management	If the resolution of a problem requires a fix or change, the problem manager can create a change request from a problem ticket.
Change Management	A change worker can create a new change request but, in most cases, the change worker works on the change requests that other workers submit.

Requesting a change

A change worker or incident technician can create a change request that is not associated with other process tickets.

Creating a change request is a step in the Change Management process.

Change requests can also be created from incidents and from problem tickets.

To request a change.

- 1 In the Process Manager portal, click **Change** menu on the left panel.
- 2 On the right side of the page, click **New Change**.
- 3 In the Request a Change, enter information about the change.

Table 7-5 Options on the Create a Change Request

Option	Description
Raise by	Lets you specify the name who report this change.

Option	Description																														
Department	Lets you specify department of the requestor																														
Implement Date	Lets you specify the proposed implementation date																														
System	Lets you specify the system name which require the change																														
Assign to	Lets you specify the group or user who will response next to you																														
Impact	Lets you define the extent of the issue by specifying how many people the issue affects.																														
Urgency	Lets you specify the urgency of the issue by specifying which service the issue affects.																														
Priority	<p>Automatic calculation the priority of this incident.</p> <table border="1"> <thead> <tr> <th>Impact</th> <th>Urgency</th> <th>Priority</th> </tr> </thead> <tbody> <tr> <td>1 - High</td> <td>1 - High</td> <td>1 - Critical</td> </tr> <tr> <td>1 - High</td> <td>2 - Medium</td> <td>2 - High</td> </tr> <tr> <td>1 - High</td> <td>3 - Low</td> <td>3 - Moderate</td> </tr> <tr> <td>2 - Medium</td> <td>1 - High</td> <td>2 - High</td> </tr> <tr> <td>2 - Medium</td> <td>2 - Medium</td> <td>3 - Moderate</td> </tr> <tr> <td>2 - Medium</td> <td>3 - Low</td> <td>4 - Low</td> </tr> <tr> <td>3 - Low</td> <td>1 - High</td> <td>3 - Moderate</td> </tr> <tr> <td>3 - Low</td> <td>2 - Medium</td> <td>4 - Low</td> </tr> <tr> <td>3 - Low</td> <td>3 - Low</td> <td>5 - Planning</td> </tr> </tbody> </table>	Impact	Urgency	Priority	1 - High	1 - High	1 - Critical	1 - High	2 - Medium	2 - High	1 - High	3 - Low	3 - Moderate	2 - Medium	1 - High	2 - High	2 - Medium	2 - Medium	3 - Moderate	2 - Medium	3 - Low	4 - Low	3 - Low	1 - High	3 - Moderate	3 - Low	2 - Medium	4 - Low	3 - Low	3 - Low	5 - Planning
Impact	Urgency	Priority																													
1 - High	1 - High	1 - Critical																													
1 - High	2 - Medium	2 - High																													
1 - High	3 - Low	3 - Moderate																													
2 - Medium	1 - High	2 - High																													
2 - Medium	2 - Medium	3 - Moderate																													
2 - Medium	3 - Low	4 - Low																													
3 - Low	1 - High	3 - Moderate																													
3 - Low	2 - Medium	4 - Low																													
3 - Low	3 - Low	5 - Planning																													
Stage	Lets you specify the stage, Active, Resolved, Closed or Rejected																														
Project Name	Lets you specify the project name																														
Reason for Change	Lets you specify detail of this change request																														

Option	Description				
Impact / Risk	<p data-bbox="400 239 736 267">Change and Risk Assessment</p> <p data-bbox="400 309 1255 399">A change manager should reflect on, and communicate, the risks they identify to those involved in sponsoring, supporting, and putting a change into effect.</p> <p data-bbox="400 440 626 468">The Scoring System</p> <p data-bbox="400 510 1209 725">The scoring system can start very simply, where each response has five possible answers. Starting at 2 for the best possible scenario and answer, and increasing in increments of 2 to 10 for the worst. The scores for each question are then totaled to arrive at a final 'total risk factor' score.</p> <p data-bbox="400 767 650 795">The Number of Teams</p> <p data-bbox="400 836 1249 1052">The number of teams involved (in a change) can suggest complexity, and difficulty, from the perspective of the tasks involved, the challenge of maintaining communications, and coordinating the collaborative effort. Thus, the more teams involved, the greater the risk that one of these facets may fail.</p> <p data-bbox="400 1093 774 1121">The range can be straightforward.</p> <p data-bbox="400 1163 1255 1433">In terms of possible scoring ranges, an example is that one team involved scores just 2 points. If there are two teams involved it's 4 points, and so on until five or more teams involved equates to a score of 10 points. Such that the score increases as the number of teams involved, and thus the associated risks, increase.</p> <p data-bbox="400 1475 784 1503">This example can be visualized as:</p> <table border="1" data-bbox="489 1534 1244 1621"> <thead> <tr> <th data-bbox="489 1534 873 1621">Number of teams involved</th> <th data-bbox="873 1534 1244 1621">Score</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Number of teams involved	Score		
Number of teams involved	Score				

Option	Description
--------	-------------

1	2
2	4
3	6
4	8
5 or more	10

The Prior Experience

As an example, if the type of change has been performed before, successfully, it scores a 2. Previously successful after encountering issues, 4 points. Unsuccessful after issues, 6 points, through to 10 points for no previous experience. You might also wish to expand on these levels.

This example can be visualized as:

Level of prior experience/change success	Score
Previously successful	2
Previously successful after encountering issues	4
Unsuccessful after issues	6 (or 8)
No previous experience	10

Option	Description
--------	-------------

The Level of Testing

Testing is of course a major factor in success/failure, but sometimes circumstances mean that a change must progress absent of any serious chance to test. An example scoring mechanism is that an untested change scores 10 points. Only unit tested, 8 points. Unit tested and quality assured, 6 points, and one that is unit, quality assured, and user-acceptance tested, 2 points. Again, extra levels (and possible scores) can be added to suit your organization.

This example can be visualized as:

Level of testing	Score
Unit tested, quality assured, and UA tested	2
Unit tested and quality assured	6 (or 4)
Unit tested	8
Untested	10

The Expected Service Outage

It's always worth asking whether a service outage is required to implement a change, or whether it can be implemented without interruption.

In the example scoring system, no outage scores best at just 2 points. Less

Option	Description
--------	-------------

than 2 hours, 4 points. Between 2 and 3 hours, 6 points. Between 3 to 5 hours, 8 points, and more than 5 hours scores the maximum of 10 points.

This example can be visualized as:

Expected service outage	Score
No outage	2
< 2 hours	4
2-3 hours	6
3-5 hours	8
> 5 hours	10

The Reversal Time

Finally, for now, can the change be reversed out (backed out) should issues arise? When asking about this, it’s also important to check how long any backout effort might last.

An example scoring system is: No outage and less than an hour to back out scores the minimum 2 points – which is good. No outage but more than an hour to reverse the change scores 4 points. An outage of less than one hour scores 6 points. An outage of more than one hour score 8 points, and no back out option scores the maximum 10 points.

This example can be visualized as:

Option	Description	
	Reversal time	Score
	No outage and less than an hour to back out	2
	No outage but more than an hour to reverse	4
	Outage of less than one hour with minimal reversal time	6
	Outage of more than one hour with significant reversal time	8
	No back out option	10
Deployment Activity	Lets you specify the deployment activity or you can refer to the deployment document which attach to the Note tab after the change is created.	
Rollback Activity	Lets you specify the rollback activity or you can refer to the rollback document which attach to the Note tab after the change is created.	
Downtime	Lets you specify the downtime YES/NO	
Schedule	<p>Lets you specify the date/time of implementation.</p> <p>The change requestor provides a required by date for the change request.</p> <p>You can use the needed by date to schedule when the change request should be implemented. Typically, you schedule the implementation of a</p>	

Option	Description
	change plan after the planning tasks are completed. For example, 10 March 2020 @ 20:00 – 22:00.
Customer Approve	Lets you specify if Customer wants to approve or reject this change.
CAB Decision	Lets you specify if CAB decides to approve or reject this change.
CAB Comment	Lets you specify the comment by CAB in case of rejected or approve with condition.

- 4 Click **Update** if you are finished.

Approving and implementing changes

This chapter includes the following topics:

- [Approving a change \(change manager\)](#)
- [Closing a change request ticket](#)

Approving a change (change manager)

The change manager can approve or deny a change plan after the CAB votes to approve or deny the change plan.

Approving a change is part of the Change Management process.

To approve a change.

- 1 In the Process Manager portal, click **Change** menu on the left panel.
- 2 Under **Process View** page, search the Change Request by entering the change number
- 3 Click the specific change number to open the change request ticket

- 4 Review **Assign to** (implementer)
- 5 Review **Impact / Risk**
- 6 Review **Deployment Activity**
- 7 Review **Rollback Activity**
- 8 Review **Downtime** and change **Schedule**
- 9 Review **Customer Approval**
- 10 In the **CAB Decision** dialog box, select **Approve** or **Reject**
- 11 Click **Update** button.

Closing a change request ticket

After you implement the change request, you must close the change request ticket. Closing the ticket lets you fulfill the request. Fulfilling the change request is part of the Change Management process.

To close a change request ticket

- 1 In the Process Manager portal, click **Change** menu on the left panel.
- 2 Under **Process View** page, search the Change Request by entering the change number
- 3 Click the specific change number to open the change request ticket
- 4 In the **Stage** dropdown list, select **Closed** ticket.

Chapter 8

Managing your Organization's Knowledge

This chapter includes the following topics:

- [Introducing Knowledge Management](#)
- [Processing requests for knowledge base entries](#)
- [Managing the knowledge base](#)
- [Using the knowledge base](#)

Introducing Knowledge Management

This chapter includes the following topics:

- [About Knowledge Management](#)
- [Types of knowledge base items](#)
- [About the Bulletin Board](#)
- [Knowledge base statuses](#)
- [Email notifications from Knowledge Management](#)
- [About permissions in the knowledge base](#)

About Knowledge Management

The Knowledge Management process gathers, analyzes, stores, and shares knowledge and information within an organization. The goal of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge. Collecting information in the knowledge base lets

organizations match new incidents against previous ones and reuse established solutions and approaches.

When the knowledge base is implemented correctly, it can significantly improve incident resolution time and customer satisfaction. The knowledge base can contain information about the best practices that address the most common issues that users encounter. Instead of having to solve the same customer issues repeatedly, incident technicians can search the knowledge base for information about similar issues. Providing established methods for addressing common incidents reduces response time.

Users can access the knowledge base to obtain self-service resolution of common problems. By providing users with the knowledge resources to solve problems on their own, you can greatly reduce the number of incidents that they submit. When a user submits an incident, they can search the knowledge base to determine if there is a solution to the incident. If the user finds a solution, they might be able to implement the solution on their own. This self-service reduces the number of incidents that are submitted to the iServiceDesks.

In iServiceDesks, the Knowledge Management process provides a means to submit, review, approve, and post information to the knowledge base. The process increases the reliability of the knowledge base so that it can be used to improve the other processes in your organization.

The Knowledge Management process includes the following key features:

- The FAQ or Forum Community, which facilitates proactive notification of important issues.
For example, if the Internet access is down, you can let users know that IT is aware of the problem. As a result, you minimize further incident submissions for that issue.
- The ability to set up a category to organize knowledge base items and make them easier for users to find.

- A knowledge base approval process that helps to ensure that the content is relevant and accurate before publication.
- A fully-audited content management system that stores the knowledge base content. You can run reports to analyze this content. For example, you can report the number of times a knowledge base item was viewed and how recently it was viewed.
- The accessibility of the knowledge base information from within the iServiceDesks processes. Easy access from processes lets users take full advantage of the knowledge base, as well as easily add new content to the knowledge base.

Types of knowledge base items

The iServiceDesks knowledge base can contain several types of items. These items help organize the information and provide users with different levels of information to meet a variety of needs.

Table 8-1 Types of knowledge base items

Knowledge base item	Description
Article	A general-purpose, informational document. The article format provides the most flexibility. In addition to text, an article can contain images, formatted HTML, and links. An article has no size limitations.
FAQ (frequently asked question)	Provides the information in a question-and-answer format. FAQ items typically provide self-service information but can be used for other purposes as well.
Forum & Community	A message that provides users with time-sensitive, critical information.

	Bulletin board items have date restrictions and a priority.
Case Study	A group of related articles, entries, or other documents and files about a specific topic.

About the Forum and Community

The Forum & Community is a Web part that appears on most of the main pages in the Process Manager portal. A Forum & Community message provides users with time-sensitive, critical information.

The Forum & Community messages are components of the iServiceDesks knowledge base. However, the Forum & Community provides a proactive way to display the time-sensitive messages to iServiceDesks users without requiring them to access the **Knowledge Base** page.

Examples of how you can use the Bulletin Board are as follows:

- Inform users about critical, known issues.

For example, if email access is down, you can let users know that IT is aware of the problem. As a result, you minimize further incident submissions for that issue.

- Inform users about upcoming outages and planned disruptions in service.
- Leave public or private messages for specific users, groups, or organizational units.

Like the other items in the knowledge base, you can set permissions on Forum & Community messages. Therefore, you can create messages for certain segments of your organization. You can also provide creation permissions so that others can create messages for the members of their groups or departments.

Forum & Community messages can be created as a result of the Knowledge Management process or outside the process on the **Knowledge Base** page. Forum & Community messages can also be created and appear on the **Process View** pages of the iServiceDesks process.

Knowledge base Status

The knowledge base request status accurately reports the progression and outcome of the stages of the knowledge base process.

The status and percentage appear in several places in the Process Manager portal. For example, they appear at the top of the ticket's **Process View** page.

Table 8-2 Knowledge base statuses

Status	Description
Closed	The process is complete as a result of either of the following actions: <ul style="list-style-type: none"> ■ A knowledge base article was created. ■ The knowledge base article was removed.
Create Article	The creation of the knowledge base article is underway.
Review Proposed KB Article	A request for a knowledge base article was submitted and is ready to be worked.
Review Request to Remove the KB Submittal	The knowledge base request was rejected and is in a waiting state for the knowledge base approver to remove it.
Review Request to Create KB Entry	The knowledge base request was accepted and edited and is ready for the final review, or the review is underway.

About permissions in the knowledge base

Access to knowledge base items is controlled through permissions. Permissions can be set

on the knowledge base categories and on the individual knowledge base items. Permissions can be granted to users, groups, and organizational units.

The knowledge base items that are created through the Knowledge Management process contain default group permissions. Those default permissions can be edited from the **Knowledge Base** page. The knowledge base items that are created outside the process do not have default permissions. The permissions must be assigned during or after the item creation.

Typically, only the administrator or other user with the appropriate permissions can set permissions on knowledge base items and categories.

Processing requests for knowledge base entries

This chapter includes the following topics:

- [Processing requests for knowledge base entries](#)
- [Roles in Knowledge Management](#)
- [Sources of knowledge base requests and entries](#)
- [Submitting a request for a knowledge base entry](#)
- [Accepting or rejecting a knowledge base request](#)
- [Create KB Article dialog box](#)
- [Reviewing a knowledge base entry for final resolution](#)

Processing requests for knowledge base entries

In iServiceDesks, the Knowledge Management process provides a means to submit, review, approve, and post information to the knowledge base. The process increases the reliability of the knowledge base so that it can be used to improve the other processes in your organization.

Table 8-3 Process for submitting and reviewing requests for knowledge base entries

Step	Action	Description
Step 1	A request for a knowledge base entry is submitted.	Requests for a knowledge base entry can originate from the incidents or problems. When the request is submitted, a task to review the knowledge base request is assigned to the knowledge base editor.
Step 2	The knowledge base editor reviews the request.	After a knowledge base request is submitted, a knowledge base editor reviews the request and accepts or rejects it. When the request is accepted, the editor can categorize the entry and edit it to improve usability. When the knowledge base editor finishes working with the request, a task is assigned to the knowledge base approver.
Step 3	The knowledge base approver reviews the request and determines how to handle it.	The knowledge base approver makes the final decision to post or remove a proposed knowledge base item. The approver can also return the request to the knowledge base editor for further editing or reconsideration.
Step 4	The knowledge base approver posts the entry to the knowledge base.	After the knowledge base entry is posted, it is available to all users.
Step 5	(Optional) The knowledge base	The knowledge base items that are created through the Knowledge Management process contain default group

Step	Action	Description
	approver sets additional restrictions on the entry.	permissions. If access to the entry needs to be restricted further, the knowledge base approver can edit the entry and its permissions from the Knowledge Base page.

An administrator or other user with the appropriate permissions can create knowledge base items in the Knowledge Management process.

Roles in Knowledge Management

iServiceDesks employs roles to define responsibilities for and assign owners to the tasks and other activities within the ITIL processes.

The roles in the Knowledge Management process are tasked with editing, approving, and categorizing knowledge base entries.

Table 8-4 Roles in Knowledge Management

Role	Description
Knowledge Base editor	Reviews a knowledge base request and approves or rejects it. The editor can categorize the entry and edit the title or content to improve usability.
Knowledge Base approver	Reviews the proposed entry and provides a final approval for posting the entry to the knowledge base.

Sources of knowledge base requests and entries

The creation of a knowledge base request triggers the Knowledge Management process for approving and creating knowledge base items. A knowledge base request can originate from several

sources.

The administrator or other user with the appropriate permissions can also create knowledge base entries outside the approval process.

Table 8-5 Sources of knowledge base requests for the Knowledge Management process

Source	Description
Process Manager portal	A user requests the creation of a knowledge base entry by creating a knowledge base request in the Process Manager portal.
Incident resolution	During the incident resolution process, on the Create Incident Details page, the support technician selects the option to create a knowledge base entry. This option lets the support technician request an entry that can provide help for the same kind of issue in the future. For example, if the issue was resolved by training the user, the technician can request a knowledge base article that contains the same information. Users who encounter that issue in the future can find and read the knowledge base article instead of creating an incident.
Problem Management	During the problem review, on the Review Proposal page, the problem manager selects the option to create a knowledge base entry. Creating a knowledge base entry is one way to resolve a problem. For example, if the problem cannot be fixed but a workaround exists, the workaround can be documented in a knowledge base article.

Table 8-6 Sources of knowledge base items outside the process

Source	Description
Knowledge Base page	On the Knowledge Base page, the administrator or other user with the appropriate permissions selects any of the following options:
Process View page of Process View page of	On the Process View page of an incident, change request, or problem ticket, process workers can create Bulletin Board messages. They can

Source	Description
an incident, change request, or problem ticket	use the Add Forum & Community Entry and Create Forum & Community Entry Process Type Actions to create these messages.

Submitting a request for a knowledge base entry

Before it can be added to the knowledge base, most new content must go through the knowledge base approval and review process.

This task is a step in the process for creating a knowledge base entry.

The knowledge base article request is created, and a confirmation screen displays the process ID for the entry request. The proposed knowledge base entry now goes to a knowledge base editor, who approves or denies the request. Click **Close** to close the dialog.

To submit a request for a knowledge base entry.

- 1 In the Process Manager portal, click **Knowledge**.
- 2 On the Create Knowledge Management page, click **New**.
- 3 In the Entry Request dialog box, define the entry as follows:

Select a **Tag** to identify this entry in any article lists or search results in the Process Manager portal. When you type the **Tag**, make it as specific as possible so that it quickly conveys the purpose of the entry. For example, instead of “printer jam,” you might type “Clearing a printer jam”.

Select and format the content for the proposed entry.

- 4 In the **Entry Request** dialog box, click **Submit** button.

Accepting or rejecting a knowledge base request

After a knowledge base request is submitted, a knowledge base editor reviews the request and accepts or rejects it. The editor can categorize the entry and edit it to improve usability.

This task is a step in the process for creating a knowledge base entry.

Whether the request is accepted or rejected, a task is created for the knowledge base reviewer to review it and take final action.

To review a knowledge base request

- 1 In the Process Manager portal, click **Knowledge** menu on the left panel.
- 2 On the **My Task List** page, under **Tasks Viewer**
- 3 In the list of tasks, find and open a request that has the status **Review Proposed KB Article**.
- 4 On the ticket's **Process View** page, under **My Actions**, click **Review KB Request**.
- 5 Close the article's view page.
- 6 In the **Create KB Article** dialog box, review the entry submission, and then take one of the following actions:

To reject a knowledge base request

- 1 In the **Create KB Article** dialog box, click **Reject Submission**.
- 2 In the **Close Request** dialog box, provide a reason for rejecting the entry, and then click **Submit**.
- 3 When you are returned to the task's **Process View** page, you can close it.

To accept a knowledge base request

- 1 In the **Create KB Article** dialog box, categorize and enter additional information about the knowledge base entry.
- 2 When you are satisfied with the information, click **Preview**.
- 3 In the **Preview Post** dialog box, review the entry in its final format, and then click **Submit**.
- 4 When you are returned to the task's **Process View** page, you can close it.

Create KB Article dialog box

This dialog box lets you review a request for a knowledge base entry, edit it, categorize it, and accept or reject it. It appears when a knowledge base editor clicks **Review KB Request** on the request's **Process View** page.

Table 8-7 Options in the Create KB Article dialog box

Option	Description
Tag	Lets you select the type of knowledge base group that the submission should be created as. The knowledge base item types are as follows: <ul style="list-style-type: none"> ■ FAQ ■ Forum & Community ■ Case Study
Category	Lets you select the category in which to place the knowledge base entry. You can also create a new category by clicking New Category .
Headline	Lets you add the title of the knowledge base.
Description	Lets you provide a description of the article or a more detailed explanation of the question. This description appears under the title of the knowledge base item on the Knowledge Base page.
Stage	Lets you specify the stage of Submission, Reviewed, Published, Closed,

Option	Description
	Reject.

Reviewing a knowledge base entry for final resolution

After a knowledge base editor accepts or rejects a knowledge base request, the knowledge base approver receives a task to make a final decision.

The knowledge base approver can take the following actions:

- Edit the entry before approving it.
- Approve and submit the entry.
- Reject the entry.
- Return the request to the knowledge base editor for further editing or reconsideration.

The knowledge base approver can review the tasks that have the following statuses:

Review Request to Create KB Entry	This status represents a request that the knowledge base editor accepted. You can return it for further editing, reject it, edit it, or approve it.
Review Request to Remove the KB Submittal	This status represents a request that the knowledge base editor accepted. You can return it for further editing, reject it, edit it, or approve it.

Managing the knowledge base

This chapter includes the following topics:

- [About knowledge base categories](#)

- [Adding a knowledge base category](#)
- [Add knowledge Tag](#)

About knowledge base categories

iServiceDesks uses categories to classify its knowledge base items. The knowledge base categories help the iServiceDesks workers and users find the information that they need.

iServiceDesks contains a pre-defined knowledge base category. You can add categories and manage the existing ones on the **Knowledge Base** page in the Process Manager portal.

You can set permissions for the knowledge base categories in the User Authorization Matrix which reside in the database. The permissions determine who can access a knowledge base category and all the items that it contains.

Adding a knowledge base category

Knowledge base categories help you organize all the knowledge base items in iServiceDesks.

Organizing the items in categories helps users find the items they need more easily.

To add a knowledge base category

- 1 Login as Administrator
- 2 On the left panel, click the **Setting** menu.
- 3 On the right panel, find the **Knowledge** section and click **Category**.
- 4 Under Knowledge Category, click **Add New**.
- 5 Type a knowledge base category.

- 6 When you finish defining the category, click **add**.

Adding a knowledge Tag

Knowledge base Tag help you group all the knowledge base items in iServiceDesks

This dialog box lets you create knowledge base Tag in the Knowledge Management process.

To add a knowledge base Tag.

- 1 Login as Administrator
- 2 On the left panel, click the **Setting** menu.
- 3 On the right panel, find the **Knowledge** section and click **Category**.
- 4 Under Knowledge Category, click **Add New**.
- 5 Type a knowledge base category.
- 6 When you finish defining the category, click **add** button.

Using the knowledge base

This chapter includes the following topics:

- [Searching the knowledge base](#)
- [Viewing an item in the knowledge base](#)

Searching the knowledge base

You can search for knowledge base items on the **Knowledge Base** page. The knowledge base searches are performed as follows:

- The search is performed on the article title, text, and description fields.
- The search evaluates the items in all the knowledge base categories.

When you find a knowledge base item, you can open and view it or perform other actions.

To search the knowledge base.

- 1 In the Process Manager portal, click **Knowledge Base**.
- 2 On the **Knowledge Base** page, under **Search Articles**, type the text to search for, and then click the **Search** symbol (a magnifying glass).

Viewing an item in the knowledge base

You view knowledge base items on the **Knowledge Base** page

To view an item in the knowledge base

- 1 In the Process Manager portal, click **Knowledge Base**.
- 2 On the **Knowledge Base** page, take one of the following actions:
 - Under **Search Articles**, type the text to search for, and then click the **Search** symbol (magnifying glass).
 - Under **Article Category List**, select a category that is likely to contain the item.
 - Under **Tag Cloud**, select a tag that is likely to contain the item.
- 3 Under **All Articles**, scroll through the list of knowledge base items to find one that might provide the information you need.

If you cannot find what you need, you can repeat step 2.

- 4 To open an item, click its article name or click the **Open** symbol (a magnifying glass)

that appears at the far right of its name.

- 5 If the item contains multiple entries, you can expand and collapse them to view their information.
- 6 (Optional) Take any other actions that you need.

Your permissions determine what you can do with a knowledge base item. For example, typical actions are to view the item's history, print it, or export it.

Chapter 9

Communicating in the Process Manager portal

This chapter includes the following topics:

- [Emailing in the Process Manager portal](#)

Emailing in the Process Manager portal

This chapter includes the following topics:

- [About automatic email notifications](#)

About automatic email notifications

iServiceDesks can send email notifications at various stages of a process, based on one or more events that occur within the process. The type of event determines the contents and the recipients of the email notifications.

iServiceDesks contains default notifications for the following core processes:

- Service Request
- Incident Management
- Problem Management
- Change Management

The default notifications are ready to use. You can receive the email notifications if

Administrator setup this alert for you. The email content is created from a default email template.

To send an email by setting email notify on each user account

- 1 Login as Administrator.
- 2 On menu left panel, click on **Edit User**.
- 3 Find the user account you want to receive email notification.
- 4 Click the user name in the table.
- 5 Then find and checkbox the **Receive ticket status emails?**
- 6 When you are finished, click **update**.

These automatic email notifications occur on specific items within the Process Manager portal. For example, the process notifications can be sent when a document or an incident entry is added, edited or deleted.

Email notifications for Service Request and Incident Management are handled through the Automation Rules.

Chapter 10

Viewing and Organizing Reports

This chapter includes the following topics:

- [Introducing organizing reports](#)

Introducing organizing reports

This chapter includes the following topics:

- [About iServiceDesks reporting](#)

About iServiceDesks reporting

iServiceDesks includes predefined reports that provide easy access to the iServiceDesks data. The pre-defined reports are extracted all records which it contains almost default columns from database table into a single file as CSV format. Then you can use Excel program to generate the desired graphical chart.

To download the iServiceDesks reports in the following ways:

- Login to iServiceDesks.
- On menu left panel, click the following menu.
 - Service Request
 - Incident

- Problem
- Change
- Under the table, click **CSV** hyperlink to download the report.

Viewing a report

You can view reports in the Organization Reports on the Dashboard. Those reports are for Incident and Change Request.

Your permissions determine the reports that you can view.

To view a report on the Summary Reports page

- 1 Login to iServiceDesks.
- 2 On menu left panel, click the Dashboard. There are pre-defined monthly reports below.
 - Incident Report category by SLA
 - Number of tickets which Pass for each month
 - Number of tickets which Fail for each month
 - Number of tickets which Overdue for each month
 - Incident Report category by Stage
 - Number of tickets which Active for each month
 - Number of tickets which Resolved for each month
 - Number of tickets which Closed for each month
 - Number of tickets which Rejected for each month
 - Incident Report category by Priority

- Number of tickets which Critical for each month
- Number of tickets which High for each month
- Number of tickets which Moderate for each month
- Number of tickets which Low for each month
- Number of tickets which Planning for each month
- Change Request category by Stage
 - Number of tickets which Active for each month
 - Number of tickets which Resolved for each month
 - Number of tickets which Closed for each month
 - Number of tickets which Rejected for each month
- Change Request category by Priority
 - Number of tickets which Critical for each month
 - Number of tickets which High for each month
 - Number of tickets which Moderate for each month
 - Number of tickets which Low for each month
 - Number of tickets which Planning for each month

Chapter 11

Setting up and Managing iServiceDesks

This chapter includes the following topics:

- [Configuring iServiceDesks](#)
- [Managing security, users, roles, groups, and permissions](#)
- [Managing the LDAP connections](#)

Configuring iServiceDesks

This chapter includes the following topics:

- [About configuring iServiceDesks](#)
- [Before you configure iServiceDesks](#)
- [Configuring iServiceDesks](#)
- [About the incident priority](#)
- [Default priority, urgency, and impact values](#)
- [How the incident priority is calculated](#)
- [Creating and Editing Service Level Agreements \(SLAs\)](#)
- [Default SLA levels](#)
- [Configuring business hours](#)

About configuring iServiceDesks

The installation of iServiceDesks modules includes an initial configuration of iServiceDesks

and the Process Manager portal. The initial configuration lets you select the parts of iServiceDesks to install and configure communication settings.

Before you use iServiceDesks in your production environment, you must configure iServiceDesks to meet your needs. First, you must add users and groups and set up their permissions. Also, iServiceDesks comes with a default set of business of hours. You need to configure the business hours and add holidays to meet your schedule.

Before you use the Service Request and Incident Management processes, you may want to modify the email notifications and personalize using menu of **Add User** and **Edit User**.

For Service Request Management, you must setup **Category**, **Request Type** and **Stage**. Or using default pre-defined configuration.

For Incident Management, you must setup **Priority**, **Stage** and **SLA**. Or using default pre-defined configuration.

Out-of-the-box, Incident Management provides a default Service Queue, preconfigured routing rules, and default Service Level Agreement levels. When you open a new incident ticket, it will route to Helpdesk group first because Helpdesk can identify the Support Technician who can help to investigate and solve the problem.

For Problem Management and Change Management, you must setup **Priority** and **Stage**. Or using default pre-defined configuration.

Examples of some of the tasks you must perform to configure the Change Management process are as follows:

- Create your Change Manager.
- Create your Change Approval Boards (CAB).

Before you configure iServiceDesks

Before you use iServiceDesks in your production environment, you must configure iServiceDesks to meet your needs.

Configuring iServiceDesks

Before you use iServiceDesks in your production environment, you must configure iServiceDesks in the Process Manager portal and require administrator permissions.

Depending on your needs, you may want to perform some advanced customizations before you introduce iServiceDesks into your production environment.

Table 11-1 iServiceDesks configuration tasks

Action	Description
LDAP server connection.	If you use LDAP authentication for iServiceDesks, you can set up LDAP server connections.
Add users, groups, and organizational units, and assign permissions.	If you use Native Authentication for iServiceDesks, you must add the users in the Process Manager portal. iServiceDesks contains predefined groups and permissions, which you can use or modify. Assign the new users to the appropriate groups.
Configure the common settings.	The common settings determine the behavior of iServiceDesks and the portal. <ul style="list-style-type: none">■ Impact (common use for incident, problem management)■ Urgent (common use for incident, problem management)■ System Name (common use for service request) You can use the default settings or you can edit them as necessary. iServiceDesks recommends that you review the settings and become familiar with them and before you edit the master settings.
Configure your	Business hours are the hours during which your business is commonly

Action	Description
business hours.	<p>conducted. iServiceDesks provides a set of default business hours.</p> <p>The default business hours are Monday thru Friday, 8:00 A.M. to 5:00 P.M. You can modify the default business hours or add your own business hours configurations.</p>
Configure Service Level Agreement (SLA) levels.	<p>A Service Level Agreement (SLA) is a contract between an organization and its service provider, which sets the expectations and requirements for service delivery. The SLA includes the allowable time frame for the service delivery.</p> <p>Incident Management provides default Service Level Agreement levels. You can use the default settings or you can configure SLA levels to meet your needs.</p>
Configure incident categories.	<p>Categories are used to classify iServiceDesks incidents. iServiceDesks contains pre-defined incident categories, which you can use immediately or edit to meet your organization's requirements. Review the existing categories and edit or add to them if necessary.</p>
Verify or edit the default impact, urgency, and priority values.	<p>During incident entry, the submitter specifies the incident's impact and urgency. Support technicians can also specify the priority. When a user submits an incident, the priority level is assigned based on the impact and the urgency that the user specified.</p> <p>iServiceDesks contains default values for the impact, urgency, and priority settings. You can change the available impact and urgency values and the priority that is assigned to the combination of the two values.</p>
Create change team groups for Change Management.	<p>In the Change Management process, a change team is a group of people who can assess, plan, authorize, schedule, implement, and test a change request. The change team includes the change advisory board (CAB). The members of the CAB advise the change manager in the</p>

Action	Description
	<p>assessment, planning, and authorization of changes.</p> <p>During the initial approval phase of the Change Management process, the change manager selects the members of the change team. You can create predefined change team groups to facilitate the team selection.</p>

About the incident priority

Every incident that is submitted to the iServiceDesks is assigned a priority. This priority lets you determine how the incident is routed and when it is escalated. The prioritization of incidents helps you manage Service Level Agreements (SLA) and comply with the concepts of ITIL service management.

A user who submits an incident can specify the urgency and the impact. You can use these values to calculate the incident's priority and to create routing rules for its initial routing. This automatic calculation eliminates guesswork and prevents the user from assigning a high priority to every incident. The support technician who works the incident can change the urgency values and impact values as well as the calculated priority.

A support technician who uses the advanced incident form can specify the urgency, impact, and priority. The priority is not calculated automatically because the support workers can assess an incident's priority better than the users can.

To change these values and make them available in your Incident Management process, you need to modify different areas of the process as follows:

- Login as Administrator
- On the menu left panel, click **Setting**

- Find the Main Configuration section, you can disable / enable the impact and urgency values.
- Find the Incident section, you have no need to enable / disable the incident priority values because it calculates from Impact and Urgent

Default priority, urgency, and impact values

During incident entry, the submitter specifies the urgency and impact. When a user submits an incident, the priority is assigned based on the urgency and the impact that the user specified. The support technicians can change an assigned priority. Support technicians who create new incidents can specify the priority.

iServiceDesks contains default values for the priority, urgency, and impact settings.

Table 11-2 Default priority, urgency, and impact values

Setting	Default values
Impact	<p>Defines the extent of the issue by specifying how many people are affected. The users and support technicians can select from the following values:</p> <ul style="list-style-type: none"> ■ 1 – High (Customer or All services in Department/LOB/Branch) (LOB means line of business) ■ 2 – Medium (Small group or VIP or some components) ■ 3 – Low (Single User or report)
Urgency	<p>Represents an assessment of how much the issue affects the submitter or the primary contact. The end users and support technicians can select from the following values:</p> <ul style="list-style-type: none"> ■ 1 – High (Core Business Service) ■ 2 – Medium (Support Service) ■ 3 – Low (Non-urgent Services)

Setting	Default values
Priority	<p>Determines how the incident is routed and when it is escalated. This setting is available on the advanced incident form only.</p> <p>The default values are as follows:</p> <ul style="list-style-type: none"> ■ 1 – Critical (emergency) ■ 2 – High ■ 3 – Medium ■ 4 – Low ■ 5 – Planning

How the incident priority is calculated

When a user submits an incident, the incident is assigned a priority based on the impact and the urgency that the user specified. This automatic calculation can eliminate guesswork and prevents the user from assigning a high priority to every incident.

On the **Create a New Incident** page that the user sees, the option to specify the impact is named **Who is Affected?**

The pre-defined configuration of impact and urgency values combine to arrive at the priority.

Table 10-3 How the incident priority is calculated

Impact	Urgency	Calculated priority
1 - High	1 - High	1 - Critical
1 - High	2 - Medium	2 - High
1 - High	3 - Low	3 - Medium
2 - Medium	1 - High	2 - High
2 - Medium	2 - Medium	3 - Medium
2 - Medium	3 - Low	3 - Low

Impact	Urgency	Calculated priority
3 - Low	1 - High	3 - Medium
3 - Low	2 - Medium	3 - Low
3 - Low	3 - Low	5 – Planning

Creating and Editing Service Level Agreements (SLAs)

A Service Level Agreement (SLA) is a contract between an organization and its service provider. It sets the expectations and requirements for service delivery. The SLA can be between an external customer and your customer support team or between your organization’s employees and your IT department. The corporate policy typically defines the overall SLA. The SLA formally defines the agreed-upon services, priorities, and responsibilities that are required to support the customers and users.

SLAs use a Business Hours Configuration to determine if an SLA is late or not. The predefined SLAs are configured to use the Default Business Hours. Before you create an SLA, you should configure your business hours.

To create or edit Service Level Agreements (SLAs)

- 1 Login as Administrator.
- 2 On the menu left panel, click **Setting**.
- 3 Under Incident section, click **SLA**.
- 4 Type workhour to each priority and decide workday is **YES** or **NO**.

In the SLA Level Editor, provide information for the following items:

Incident Priority	SLA level.
-------------------	------------

Business Hour	Select the Business Hours Configuration that you want to associate with this SLA level to determine when a service is considered as Warning, Critical, Overdue, Pass or Fail .
Work Hour	To calculate SLA in working hour, select YES . Otherwise program will calculate 24 hour a day continually.

- 5 When finish, click **Update** button.

Service Level Agreement (SLA) Result and Definition

When you create or edit SLA levels, iServiceDesks will can calculate SLA for each incident based on your configuration and display the SLA life time on the incident table.

Table 11-4 The SLA Result has the following options:

SLA Status	Description	Color
SLA percentage (%)	It shows the time consume since open an incident based on each priority as configuration by Administrator	No color
60%-79%	It shows warning SLA	Yellow
80%-100%	It shows nearly deadline SLA	Red
Overdue	It shows status whether this incident still remain open and past its due date SLA condition.	Gray
Pass	It shows status whether this incident is closed and pass SLA condition.	No color
Fail	It shows status whether this incident is closed and not pass SLA condition.	No color

Default SLA levels

A Service Level Agreement (SLA) defines the expectations and requirements for delivering a service, including the allowable time frame for the response and resolution.

A default SLA is built in to the Incident Management process. The SLA levels are configured according to the default business hours, which are set up for nine hour a day, 8:00 A.M. - 5:00 P.M. You can edit the default business hours and SLA levels to comply with your organization's business hours and SLAs.

Table 11-5 Default SLA levels

SLA level	Description	Time frames
Resolution time	The resolution level monitors how much time a worker is allowed to resolve an incident according to its priority.	The default SLA Levels for resolution are as follows: <ul style="list-style-type: none">■ Critical: 4 hours■ High: 8 hours■ Medium: two business days■ Low: five business days■ Planning: fifteen business days

Configuring business hours

Business hours are the hours during which your business is conducted. Typical business hours can vary by location.

You can define multiple sets of business hours and holidays depending on your business locations and your SLA policy, such as the following:

- Default

The default business hours are included with iServiceDesks. The hours are set from Monday through Friday, 8:00 A.M. to 5:00 P.M.

You can edit the default business hours to meet your organizations requirements. You can define the beginning and ending business hours, holidays, and weekend days.

To configure business hours:

- 1 It is configurable in the configuration file.
- 2 On the configuration file, find the following pre-defined variables:

WORKDAY_START	'08:00:00'
WORKDAY_FINISH	'17:00:00'

- 3 On the routine function program, find the following pre-defined variables:

\$holidays	"New Year's Day"	=> date('Y', \$date) .'-01-01',
	"National Children's Day"	=> date('Y', \$date) .'-01-12',
	"Teachers' Day"	=> date('Y', \$date) .'-01-16',
	"Chinese Lunar New Year's Day"	=> date('Y', \$date) .'-02-05',
	"Second day of Chinese Lunar New Year"	=> date('Y', \$date) .'-02-06',
	"Third day of Chinese Lunar New Year"	=> date('Y', \$date) .'-02-07',
	"Valentine's Day"	=> date('Y', \$date) .'-02-14',
	"Makha Bucha"	=> date('Y', \$date) .'-02-19',
	"March Equinox"	=> date('Y', \$date) .'-03-21',
	"Chakri Day"	=> date('Y', \$date) .'-04-06',
	"Chakri Day observed"	=> date('Y', \$date) .'-04-08',
	"Songkran observed"	=> date('Y', \$date) .'-04-12',
	"Songkran"	=> date('Y', \$date) .'-04-13',
	"Songkran"	=> date('Y', \$date) .'-04-14',
	"Songkran"	=> date('Y', \$date) .'-04-15',
	"Songkran observed"	=> date('Y', \$date) .'-04-16',
	"Labor Day"	=> date('Y', \$date) .'-05-01',
	"Special Holiday"	=> date('Y', \$date) .'-05-06',
"Royal Ploughing Ceremony Day"	=> date('Y', \$date) .'-05-09',	

"Visakha Bucha"	=> date('Y', \$date) .'-05-18',
"Day off for Visakha Bucha"	=> date('Y', \$date) .'-05-20',
"Queen Suthida's Birthday"	=> date('Y', \$date) .'-06-03',
"June Solstice"	=> date('Y', \$date) .'-06-21',
"Asalha Bucha"	=> date('Y', \$date) .'-07-16',
"Buddhist Lent Day"	=> date('Y', \$date) .'-07-17',
"King Vajiralongkorn's Birthday"	=> date('Y', \$date) .'-07-28',
"King Vajiralongkorn's Birthday observed"	=> date('Y', \$date) .'-07-29',
"The Queen's Birthday"	=> date('Y', \$date) .'-08-12',
"September Equinox"	=> date('Y', \$date) .'-09-23',
"Anniversary of the Death of King Bhumibol"	=> date('Y', \$date) .'-10-13',
"Anniversary of the Death of King Bhumibol observed"	=> date('Y', \$date) .'-10-14',
"Chulalongkorn Day"	=> date('Y', \$date) .'-10-23',
"King Bhumibol's Birthday"	=> date('Y', \$date) .'-12-05',
"Constitution Day"	=> date('Y', \$date) .'-12-10',
"Christmas Eve"	=> date('Y', \$date) .'-12-24',
"Christmas Day"	=> date('Y', \$date) .'-12-25',
"New Year's Eve"	=> date('Y', \$date) .'-12-31',

Configuring workflow

Configuration workflow.

Managing security, users, roles, groups, and permissions

This chapter includes the following topics:

- [About iServiceDesks security and permissions](#)
- [About group-level permissions](#)
- [About iServiceDesks authentication](#)
- [About adding users from LDAP](#)
- [Creating a group](#)
- [Editing a group](#)

- [Deleting a group](#)
- [Adding users to a group](#)
- [Viewing the permissions for a group](#)
- [Creating a new user](#)
- [Adding new iServiceDesks users from LDAP](#)
- [Editing a user account](#)
- [Disabling and enabling a user](#)

About iServiceDesks security and permissions

iServiceDesks manages access to the Process Manager portal through LDAP Authentication or Native Authentication.

iServiceDesks provides a high level of security within the Process Manager portal through the use of users, groups, organizational units, and permissions. The iServiceDesks permissions control all the views and possible actions in the Process Manager portal.

For example, permissions can grant or deny access to certain functions within iServiceDesks. Permissions can grant the ability to create users, and they can deny access to view and edit articles in the knowledge base.

The iServiceDesks permissions are pre-defined and stored in the database table. The permission that is applied at the most specific level takes precedence. For example, a group is denied access to view a knowledge base article.

Table 11-6 iServiceDesks permissions

Permissions level	Description
Group	<p>A collection of users.</p> <p>For example, the Support group might contain all your support technicians.</p> <p>The KB Editors group might contain all the people who can review and edit knowledge base articles.</p> <p>iServiceDesks permissions are almost always granted at the group level rather than at the user level.</p>
Permission	<p>Permissions control the access to and use of the Process Manager portal.</p> <p>What users can view and what actions they can perform are based on permissions.</p> <p>For example, permissions may grant access to certain functions within iServiceDesks, such as the ability to create users. Or permissions may grant or deny access to view and edit articles in the knowledge base. Access to everything in iServiceDesks is controlled through permissions.</p>

About group-level permissions

Groups are collections of iServiceDesks users. The use of groups lets you assign permissions more efficiently and helps simplify the ongoing administration of iServiceDesks permissions. Instead of assigning permissions to each user individually, you can specify the permissions for a group. The permissions for a group are valid for each user who is a member of that group. iServiceDesks permissions are almost always granted at the group level rather than at the user level.

When you apply permissions to groups, you do not have to edit the permission settings for the individual users. The permissions changes that you make at the group level are updated for every user who is a member of that group.

You can use the default groups that are provided with iServiceDesks or create new groups.

About iServiceDesks authentication

The authentication method can be defined in the **LDAP Settings** section in the **Setting** menu. By default, if no setup LDAP, iServiceDesks will use Native Authentication instead.

Table 11-7 Authentication methods for iServiceDesks users

Method	Description
Native Authentication	With native authentication, users are authenticated against the Process Manager database. This authentication method requires that you create user accounts in iServiceDesks.
LDAP Authentication	You can setup LDAP server connections or edit the settings for an existing server connection. You manage the LDAP server.

Creating a group

Groups are collections of iServiceDesks users. The use of groups lets you assign permissions more efficiently and helps simplify the ongoing administration of iServiceDesks permissions. Instead of assigning permissions to each user individually, you can specify the permissions for a group. The permissions for a group are valid for each user who is a member of that group. iServiceDesks permissions are almost always granted at the group level rather than at the user level.

Table 11-8 Creating a group

Method	Description
Automatically when a user logs on	When such a user enters their logon credentials, iServiceDesks checks if enable LDAP, the credentials will pass to LDAP server. Otherwise, the credentials will check against the iServiceDesks database automatically.

An administrator who has the appropriate permissions can create iServiceDesks groups manually.

To create a group

- 1 Login as Administrator.
- 2 In the menu left panel, click **Setting**.
- 3 Under Main Configuration, click **Group**.
- 4 Under Group, click **Add New**.

Table 11-9 Options in the Add Group dialog box

Option	Description
Group ID	It will be created automatically.
Group Name	Lets you type the name of the new group. You can use special characters but you cannot enter a name that is already assigned to another group.
Status	Enable or disable this group.

- 5 When finish, click **add** button.

Editing a group

An administrator or other user who has the appropriate permissions can edit iServiceDesks groups.

To edit a group

- 1 Login as Administrator.
- 2 In the menu left panel, click **Setting**.
- 3 Under Main Configuration, click **Group**.
- 4 Under Group, click your desire **Group ID**.

Table 11-10 Options in the Edit Group dialog box

Option	Description
Group ID	Editable value of group id.
Group Name	Lets you type the name of the new group. You can use special characters but you cannot enter a name that is already assigned to another group.
Status	Enable or disable this group.

- 5 When finish, click **update** button.

Deleting a group

An administrator or other user who has the appropriate permissions can delete iServiceDesks groups.

If there is a user account belong to that group, you will not be allowed to remove this group. Unless, you revoke that user account first.

To delete a group.

- 1 Login as Administrator.
- 2 In the menu left panel, click **Setting**.
- 3 Under Main Configuration, click **Group**.
- 4 Under Group, click **Delete** your desire Group ID.
- 5 In the confirmation dialog box, click **OK** to confirm the deletion.

Adding users to a group

You can add users to a group when you add a new or edit user account by select appropriate group.

Viewing the permissions for a group

The group permission (User Authorization Metrix) is stored in the database table, which is able to list all permissions for each group.

1. Administration
2. Service Request
3. Incident Management
4. Problem Management
5. Change Management
6. Knowledge Management
7. People
8. Link
9. API
10. General

Creating a new user

An administrator who has the appropriate permissions can create new iServiceDesks users.

Every iServiceDesks user requires permissions to perform any actions in the Process Manager portal. By default, every new user is assigned to the All Users group, which provides general permissions. However, you must assign the user to one of the groups that provide the permissions that are appropriate for that user's role.

To create a new user.

- 1 Login as Administrator.
- 2 In the menu left panel, click **Add User**.
- 3 Type user information.

Table 11-11 Options on creating a new user

Option	Description
User Login	Lets you specify the user to login. You can type the user's name or email address.
User's Groups	The group settings of this user for the new user. The permissions for a group are valid for each user who is a member of that group
Name	Clones the permissions settings of this user for the new user.
Title	Clones the organization unit settings of this user for the new user.
Department	This is department or company of this user.
Line Token	This is Line group to receive notification when open a new ticket or any updates to the ticket.
Email	Lets you add an email address to receive notification or password reset. This is mandatory field. Without this email address, you will not be able to reset password by yourself.

Option	Description
Phone	Lets you add phone numbers, along with additional details about the phone numbers, for the user.
User pending	If checkbox is ticked, this user is suspense temporary and not allow to perform any actions.
Receive ticket email	If checkbox is ticked, this user will be able to receive the email notification when open a new ticket or any updates to the ticket.
Lock from user edit	If checkbox is ticked, this user is locked temporary and not allow to perform any actions.

- 4 When finish, click **Add User** button.
- 5 The user will receive an email with new user login and password.

Adding new iServiceDesks users from LDAP

You can manually add new users to iServiceDesks from LDAP. At least you must assign the user to one or more of the groups that provide the permissions that are appropriate for that user's role.

To add new iServiceDesks users from LDAP manually

- 1 Login as Administrator.
- 2 In the menu left panel, click **Add User**.
- 3 Type user information, you must enter the **User Login** same as **User id** on LDAP.
- 4 When finish, click **Add User** button.

Editing a user account

An administrator or user who has the appropriate permissions can edit the data for

iServiceDesks users. Any of the user information that can be set during the user creation is available for editing.

To edit a user account

- 1 Login as Administrator.
- 2 In the menu left panel, click **Edit User**.
- 3 Find your user account, click to **User Id**.
- 4 Update the user information.
- 5 When finish, click **update** button.
- 6 If reset password has made, the user will receive an email with new user login and password.

Disabling and enabling a user

The Administrator who has the appropriate permissions can disable a user so that the user cannot use iServiceDesks. Disabled users can be enabled so that they can access iServiceDesks again.

To disable or enable a user

- 1 Login as Administrator.
- 2 In the menu left panel, click **Edit User**.
- 3 Find your user account, click to **User Id**.
- 4 Tick the checkbox of **User Pending**.
- 5 When finish, click **update** button.

Managing the LDAP connections

This chapter includes the following topics:

- [About LDAP authentication](#)
- [Adding LDAP server connections](#)
- [Editing the settings of an LDAP server connection](#)
- [Define LDAP as the authentication method](#)

About LDAP authentication

After iServiceDesks installation, you must decide what authentication you want to use between LDAP Authentication or Native Authentication. For LDAP authentication, the iServiceDesks database does not store sensitive information such as passwords.

When you use LDAP authentication, you still need to create user accounts and organizational units in iServiceDesks. For example, you might create an account for a short-term contractor who you do not want to add to LDAP

The communication between iServiceDesks and LDAP occurs by means of LDAP queries against the LDAP database.

Bear in mind that when you change the user id on LDAP, it will not affect to the user id on iServiceDesks also as example below.

- When you delete a user from LDAP, the user is not deleted from iServiceDesks. So, this User id in iServiceDesks will not be usable for authentication.
- When you change the User Login on iServiceDesks, it will affect while you send User id and Password to LDAP for authentication.

If you edit user information or delete a user in LDAP, the information will not be updated in iServiceDesks.

Adding LDAP server connections

If your organization uses LDAP authentication as its authentication method for iServiceDesks, you must setup LDAP server connections.

To add LDAP server connections

- 1 Login as Administrator.
- 2 On the menu left panel, click **Setting**.
- 3 Under Main Configuration, click **LDAP** button.
- 4 Type information with option following.

Table 11-12 LDAP connection

Option	Description														
IP Address/DNS Name	Lets you type the IP address or host name of your LDAP server.														
TCP port	Lets you type the TCP port connecting to LDAP server.														
Relative Distinguished Names (RDN)	Lets you type the Relative Distinguished Names (RDN) of your LDAP connection. It is unique name that identifies the entry at the respective hierarchy connected by commas.														
	<table border="1"> <thead> <tr> <th>String</th> <th>Attribute type</th> </tr> </thead> <tbody> <tr> <td>DC</td> <td>domainComponent</td> </tr> <tr> <td>CN</td> <td>commonName</td> </tr> <tr> <td>OU</td> <td>organizationalUnitName</td> </tr> <tr> <td>O</td> <td>organizationName</td> </tr> <tr> <td>STREET</td> <td>streetAddress</td> </tr> <tr> <td>L</td> <td>localityName</td> </tr> </tbody> </table>	String	Attribute type	DC	domainComponent	CN	commonName	OU	organizationalUnitName	O	organizationName	STREET	streetAddress	L	localityName
String	Attribute type														
DC	domainComponent														
CN	commonName														
OU	organizationalUnitName														
O	organizationName														
STREET	streetAddress														
L	localityName														

Option	Description	
	ST	stateOrProvinceName
	C	countryName
	UID	userid
	For example, using “ou=users,ou=guests,dc=zflexsoftware,dc=com”	
User id	Lets you specify the credentials of the account that can connect to the LDAP and retrieve user and group information.	
Password	For security purposes, you must retype the password every time you add or edit an LDAP server connection.	

- 5 In the right pane, click **Test and Save** button.
- 6 If the test result is ok, the LDAP configuration will be saved in the database.
- 7 If the test result is failed, recheck your LDAP setting.

Editing the settings of an LDAP server connection

After you add your LDAP server connections, you may need to edit the settings of an LDAP server connection. For example, if you need to change the user name and password for an LDAP server connection, you can change it.

Define LDAP as the authentication method

If you want to use LDAP as your authentication method for iServiceDesks, Administrator must define the variable of LDAP Server to “yes” in the iServiceDesks configuration file.

Table 11-13 LDAP connection

Option	Description
LDAP_AUTH	Type value on the right side. “yes” – require LDAP authentication “no” – require Native authentication

Managing Application Programming Interface (API)

This chapter includes the following topics:

- [About configuring API iServiceDesks](#)
- [Before you use API iServiceDesks](#)
- [Understanding API RESTful](#)

About API iServiceDesks

iServiceDesks is ready for REST (Representational State Transfer) API with simple stateless architecture that runs over the HTTP to retrieve (GET) or create (PUT) the incident ticket using JavaScript Object Notation (JSON) format for transmitting data between a server and iServiceDesks application.

Before you use API iServiceDesks

To use API iServiceDesks, make sure that there is an API token assigned to trusted source hardware or application and probably check a default group named “API” reside in the iServiceDesks system.

Understanding API RESTful

Any hardware or application can send GET or POST operations with RESTful format to get information or create an incident request automatically with message format below.

The API allows you to perform read (GET) operations with REST format.

GET - Retrieves one incident record.

URL format

Table 11-13 GET operation

Name	Value
Default URL	/inc_api_add.php?api_token="token"&api_call="call_id"

Parameter(s)

Name	Description
api_token	Request a token from your administrator related to the System Name using for authentication
api_call	Incident number

The API allows you to perform create (POST) operations with REST format.

POST - Inserts one incident record.

URL format

Table 11-14 POST operation

Name	Value
Default URL	/inc_api_add.php

Parameter(s)

Name	Description
api_workflow	Workflow identification number for incident
api_token	Request a token from your administrator related to the System Name

Name	Description
	using for authentication
api_details	Details of the problem
api_impact	Impact level (“1 – High”, “2 – Medium”, “3 – Low”)
api_urgent	Urgent level (“1 – High”, “2 – Medium”, “3 – Low”)
api_user	(Optional) User id
api_openby	(Optional) Full name who open this ticket
api_riaseby	(Optional) Full name who raise (owner) this ticket
api_email	(Optional) Email address of raiser (owner) who want to get update
api_due	(Optional) Target date to resolve the problem
api_device	(Optional) System Name which send the RESTful message to iServiceDesks system
api_subject	(Optional) Short description of the problem

Managing Workflow Designer

This chapter includes the following topics:

- [About workflow designer](#)
- [Add new workflow](#)
- [Workflow designer configuration](#)

About workflow designer

Workflow Designer lets an administrator customize workflows to meet the needs of the organization. With Workflow Designer, you can design workflows to apply rules, make decisions, assigned users and route the ticket.

The Workflow Designer that is included with iServiceDesks lets you modify the iServiceDesks workflows in any way that you want based on Business Process Model and Notation (BPMN) which

is standard for business process modeling that provides a graphical notation for specifying business processes in a Business Process Diagram (BPD), based on a flowcharting technique very similar to activity diagrams from Unified Modeling Language (UML).

Add new workflow

Only administrator can create a workflow for each service (Service Request, Incident, Problem, Change and Knowledge Management). The new workflow can be created by using form contains the minimum amount of information that is required to create a workflow.

When you create a workflow, you can perform the following actions:

- 1 In the workflow Management portal, click **Add**.
- 2 You can enter detail. The options are as follows.

Table 11-15 Options on the Create a New service request

Option	Description
Service	Lets you specify the Service Request, Incident, Problem, Change or Knowledge Management.
Name	Lets you specify the unique name of this workflow.
Description	Lets you type a brief description of the workflow. Make this description as specific as possible. For example, you might type "User ID request" or "Firewall request." This description becomes the service request title, which identifies this service request in any service request lists in the Process Manager portal.

- 3 Click button Save workflow.
- 4 Then you will go to the workflow designer configuration.

Workflow Designer Configuration

You can use the default settings or you can edit them as necessary. We recommend that you review the settings to familiarize yourself with them and then customize them for your organization.

Examples of the types of settings that you might change are as follows:

Table 11-16 Options on the Create a New service request

Option	Description
	Lets you start the workflow. This must be only one in the workflow.
	Lets you end the workflow. This must be only one in the workflow.
	Lets you specific a new task. <ul style="list-style-type: none"> ● Double click on this task to define shot description. ● Add authorization groups to access this task on the right panel.
	Lets you make a connection link between tasks. <ul style="list-style-type: none"> ● Double click on this connection link to define shot description. ● Select an action between tasks on the right panel.
	Lets you restore the workflow to the original.
	Lets you open the workflow from the local file system on your PC/Laptop.
	Lets you save the workflow to database.
	Lets you download the workflow to the local file system on your PC/Laptop for backup purpose or using it with another service.

When complete design, you must save the workflow first and then deploy to iServiceDesks system later on. Be aware, there would be some tickets might be impacted with your changes. The workaround solution can be applied by providing temporary authorization to those user groups for passing through new task assignment.

Debug mode and logging

This chapter includes the following topics:

- [About debug mode and logging](#)
- [How to turn on the debug mode](#)
- [Downloading of log files](#)

About debug mode and logging

When users encounter program errors while using, you should notify the system administrator. So, the administrator will open the debug mode and ask the user to perform those actions again.

The system will store variables and error values in log files. Then developers can use those files to be examined, analyzed for bugs of the program.

How to turn on the debug mode

The administrator can enable the debug mode to store variables and error values in log files.

To turn on the debug mode, please perform the following actions:

1. Log in as an administrator.
2. The left menu, click on the Settings menu.
3. Click on the Debug Mode.

4. Fill in the details with the following options.

Table 11-17 Option to turn on the debug mode

Option	Description
Debug mode	<p>You can choose to enable (ON) or disable (OFF) debug mode.</p> <p>Turning on the debug mode, it may affect the overall performance of the system if there are a large number of users.</p> <p>If you disable (OFF), you will not be able to edit the next fields.</p>
Entry process (GET)	<p>You can store variables and error values of the entry process (GET) into the log files by selecting enable (ON) or disable (OFF).</p> <p>Recorded data when opening or entry the initial process, most of them will retrieve the data from the database and display on the screen.</p>
Post process (POST)	<p>You can store variables and error values of post process (POST) into the log files by selecting enable (ON) or disable (OFF).</p> <p>Recorded data when submitting the data, most of them will collect the information from the screen and write into the database.</p>
Internal loop (LOOP)	<p>You can store variables during internal looping (LOOP) into the log files by selecting enable (ON) or disable (OFF).</p> <p>Recorded data when looping within the program to display or calculate the results of various</p>
Log Retention (days)	<p>Separate log files for each day</p> <p>The log files will be deleted if over then log retention (days).</p> <p>For example, the retention period is 5 days. The files that exceed 5 days will be deleted from the system.</p>

5. Click the Save button.

Downloading the log files

The administrator can download the log files by considering the list of files in the debug setting screen sorted by recent date.

Downloading log files, please perform the following actions:

1. Log in as an administrator.
2. The left menu, click on the Settings menu.
3. Click on the Debug mode.
4. At the bottom of screen, you will see a list of files sorted by recent date.
5. Click on the file which contain the error on specific date to download.
6. Send the log file to the system developer to find the cause of the problem.