CA Service Operations Insight

User Guide

r3.2

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Application Performance Management
- CA Business Intelligence
- CA Clarity™ Project and Portfolio Manager
- CA CMDB
- CA Configuration Automation (formerly CA Application Configuration Manager)
- CA eHealth® Performance Manager (CA eHealth)
- CA Embedded Entitlements Manager (CA EEM)
- CA Event Integration
- CA Insight™ Database Performance Manager
- CA NSM
- CA Process Automation
- CA Service Desk
- CA Server Automation (formerly CA Spectrum® Automation Manager)
- CA SiteMinder®
- CA Spectrum®
- CA Systems Performance for Infrastructure Managers
- CA SystemEDGE
- CA Virtual Assurance

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 4: Managing, Viewing, and Responding to Alerts 55

Chapter 5: Monitoring Services from the Dashboard 81

Chapter 6: Using Reporting 121

Chapter 7: Searching and Browsing USM Data with USM Web View on a PC 145

Chapter 8: Searching and Browsing USM Data with USM Web View on Mobile Device 161

Chapter 1: About This Guide

This guide contains information about the CA Service Operations Insight CA SOI features and components. The guide also provides the following procedures:

- View service models and the associated escalation and notification policy.
- Use CA SOI to support the incident resolution process in the data center.
- Communicate the real-time health and availability of services to the required end users in an easily understood format.

Note: This guide assumes that you have already installed all CA SOI manager components and connectors.

This section contains the following topics:

Intended Audience

This guide is intended for CA SOI operators. Operators are non-administrators that include the following roles and product-related responsibilities:

business managers and executives

Includes the CIO and Business Unit managers responsible for a large group of services, subscribers or both.

Primary goals are typically to reduce cost, increase quality, and help ensure governance and compliance requirements are met for all services delivered by the business to its customers (internal or external).

These users use CA SOI view the various CA SOI reports available to see the overall status of monitored services.

service owners and line of business owners

Responsible for specific services and also accountable for overall service availability and performance.

Primary goals are typically to help ensure services are delivered according to the cost and quality levels agreed with both the business, and the CRM/customers that consume their services.

These users use CA SOI to monitor services, respond and escalate alerts and view the various CA SOI reports available.

IT manager and IT vice president

Overall responsibility for the delivery of services within the datacenter.

Primary goals are typically to help ensure services are operating to required quality levels at an acceptable level of risk. May be required to support the business in cost reduction measures.

These users use CA SOI to monitor services, respond and escalate alerts and view the various CA SOI reports available.

IT operators

Responsible for maintaining the continuity of operations within the datacenter including the network, systems, applications and databases and focused on the availability of infrastructure elements within a single domain.

These users use CA SOI to monitor services and to view the various CA SOI reports available.

helpdesk operators

Communicates with customers or consumers of a service, takes reports of outages or performance degradation, creates trouble tickets, tries to establish the cause of the outage and estimated time to repair.

These users use CA SOI to escalate alerts.

Related Publications

The following publications, provided on the installation media and the CA SOI online bookshelf, provide complete information about CA SOI:

Administration Guide

Provides information about administering and maintaining the product after installation.

Connector Guide

Provides general information about connectors, the CA Catalyst infrastructure, and writing custom connectors.

Event and Alert Management Best Practices Guide

Provides information about viewing and managing the stream of events and alerts that CA SOI receives from connectors.

Implementation Guide

Provides information about installing and implementing the product.

Service Modeling Best Practices Guide

Provides information about planning, building, and managing service models in CA SOI.

Troubleshooting Guide

Provides information and procedures to diagnose and resolve problems with CA SOI.

Web Services Reference Guide

Provides information about the CA SOI web services for interacting with resources such as CIs, services, alerts, relationships, and escalation policy.

Online Help

Provides information about performing tasks in CA SOI user interfaces.

Readme

Provides information about known issues and information that is discovered after the guides were finalized. A CA SOI release may not have a Readme.

Release Notes

Provides information about operating system support, system requirements, database requirements, web browser support, and international support.

The following publications provide information about CA Catalyst connectors and are on each downloadable connector package:

<Product Name> Connector Guide

Provides information about a specific CA Catalyst connector, including prerequisites, installation, configuration, and data mapping.

<Product Name> Connector Readme

Provides known issues for a specific CA Catalyst connector and information that is discovered after the product-specific *Connector Guide* was finalized.

Local Documentation and Online Bookshelf

CA SOI provides access to the documentation locally and online.

Local Documentation

The local documentation is installed in the SOI_HOME\Documentation folder and includes the PDFs for all guides. The online help is also installed with CA SOI and accessed through the Dashboard (PC and Mobile) and USM Web View. The local documentation is updated with specific releases only.

Online Bookshelf

The online bookshelf is on support.ca.com and provides the most current documentation set, which can be updated between releases. The online bookshelf also provides the documentation for the latest supported versions of CA Business Intelligence, CA EEM, and CA Process Automation. For a list of Bookshelf updates, click the Update History link on the Bookshelf.

CA SOI provides access to the online bookshelf in the following locations:

- The Dashboard provides a Bookshelf link.
- The Operations Console provides a menu link under Help, Bookshelf.

Note: If you are unable to access the online bookshelf, contact your system administrator to provide the documentation set PDFs.

Chapter 2: Introducing CA Service Operations Insight

This section contains the following topics:

CA Service Operations Insight

When degradation or downtime affects a key service, customers quickly become frustrated. Whether they are external customers or your own employees, poor service has a negative impact.

Domain management solutions monitor various aspects of a service, including support for IT infrastructure components or the end-user experience. None of these individual solutions give you a complete, end-to-end view of service health and availability across all management domains. Operations personnel often guess how the fault or performance issues reported across the network, systems, database, or application monitoring tools actually affect key IT services, degrade service quality, or increase the risk of an outage. Similarly, service stakeholders may not understand whether IT enables them to fulfill their business objectives.

CA Service Operations Insight (CA SOI) helps overcome these challenges by unifying the health and availability information from your domain management tools and aligning with your IT services. CA SOI introduces a new service management layer to your management infrastructure and through an open and extensible integration platform (CA Catalyst), leverages and adds value to your investment in existing management technology. CA SOI provides integrations with several CA Technologies products and third-party applications, and the CA Catalyst integration platform lets you reconcile and synchronize data in CA SOI and across all domain managers. CA SOI uses several graphical interfaces (see page 25) to display the service operations data that supports the required business functions for all parties in the appropriate format. Operations staff uses these graphical interfaces to focus efforts correctly and business and IT objectives are properly aligned.

CA SOI also serves as a comprehensive level one operations console for managing the full stream of events and alerts from all integrated products. Operations staff can use CA SOI for a consolidated view of all alerts, enabling automatic escalation of important alerts that require quick action and problem resolution across domains from one interface. CA SOI provides alert queues for grouping logical categories of alerts. CA SOI also provides an event management layer that supports detailed event searches. CA SOI has several graphical interfaces for defining simple and complex event policies for event filtering, correlation, and enrichment.

CA SOI supports layered service and alert security through the use of user groups, customers, and alert queues. This security allows for a flexible user-specific view of the services and alerts company-wide.

Features Summary

CA SOI includes the following features:

- CA Catalyst enablement to adopt a common infrastructure that enables the following:
  - Integrations with CA Technologies products for systems, network, application, workload, security, help desk, and other domains, and with some third-party management products.
  - CI correlation to ensure that resources managed in multiple products appear in CA SOI as one entity.
  - CI reconciliation to ensure that resources managed in multiple products have a unified set of property values.
  - Bidirectional connectors that can retrieve data from domain managers and synchronize the data in the source domain manager according to reconciliation and other operations in CA SOI.
  - The ability to enact specific use cases, and the ability to manipulate the infrastructure to configure custom use cases and synchronization rules.
  - An open, extensible connector framework that enables easy field-based connections to other management solutions.
- Role-based, web-deployable, service-centric visualization and reporting to support business decision making at all levels of the organization
- Service modeling through the following processes:
  - Manual definition using imported IT components from the domain managers that directly monitor and manage them
  - The ability to define properties such as relationships and propagation between items, impact, and priority to refine all aspects of a service.
  - Service model import from service-aware products (for example, CA NSM and CA Spectrum) and CI repositories such as CA CMDB.

  - Service Discovery to define policies that dynamically discover resources and add to services or automatically create relationships between CIs.

- Service impact and root cause analysis that includes the following features:
  - Impact analysis to assess and prioritize the importance of each service element and fault condition relative to the service model. Impact analysis reveals the impact of a failure or degradation to related service components.
  - Tools to assist with root cause determination and to correlate failures, degradations, and ancillary activities that are based on the relationships of their configuration items and the state of the items.
- An event and alert management solution that includes the following features:
  - Event collection, storage, and federated searches across event sources.
  - Event Management policies to detect patterns and enact processing operations such as filtering and correlation on events before they become alerts.
  - Management of all collected alerts, including alerts that do not impact managed services.
  - Alert queues to group related alerts for specialized management.
  - A full cross-domain alert audit trail
  - Alert escalation tracking
  - A prioritized console view of service-related alerts and all alerts in alert queues
  - Integration with help desk products that provide access to the ITIL incident and problem management processes.
- Service-level agreements (SLAs) that you can define against monitored services to track service metrics over a defined time period against violation thresholds.
- Layered security through user groups, alert queues, and customer management. Security lets you view the actual impact of service degradation and alert conditions on customers that rely on managed services.
- Mobile device accessible dashboard and USM browser.
- Customer creation and management. Customers are any consumers of managed services, such as a department with an organization or an external client of an MSP. You create customers and assign services to the customers to determine the alert impact on that customer.

CA SOI Terminology and Concepts

CA SOI introduces the following terminology.

Quality and Risk

CA SOI uses health and availability data from your domain management tools to monitor your IT services from the following perspectives:

Quality

Quality indicates the level of excellence that consumers of an IT service experience, whether the consumers are customers, end users, or other IT services. The levels of quality are Operational, Slightly Degraded, Moderately Degraded, Severely Degraded, Down, and Unknown. The highest propagated impact of an associated quality alert determines the service quality value.

Risk

Risk indicates the likelihood of delivering the quality of service that is required to support the overall business objectives. The highest propagated impact of an associated risk alert determines the service risk value.

Business objectives include the following goals:

- Qualitatively, the concern that, at any given time, a service is not capable of delivering its intended functionality.
- Quantitatively, any metric or group of metrics that can analytically measure the ability, over time, of a service to deliver its intended functionality (for example, Service Impact).

Examples of an increased risk are a loss of redundancy in a web server farm or a failover condition in a database cluster. The risk of service degradation is either None, Slight, Moderate, Severe, or Down. CA NSM, CA eHealth, and CA Spectrum are some of the domain managers that produce risk events.

Consider a server in a web server farm that experiences a failure and is no longer accessible. This failure could increase the risk to delivering an online service, but there might be enough capacity to meet the current consumer demand. Therefore, quality is still at acceptable levels.

CA SOI uses the worst service quality or risk level to determine service health. For example, a slightly degraded service with a severe risk of degradation would have a service health of Critical. The following table shows the available Health, Quality, and Risk values:

Health	**Quality**	**Risk**
Normal	Operational	None
Minor	Slightly Degraded	Slight
Major	Moderately Degraded	Moderate

Health	Quality	Risk
Critical	Severely Degraded	Severe
Down	Down	Down

Health and Availability

Health is a reflection of the worst state that of either Quality or Risk. Health provides a high-level summary of the service health according to those metrics.

For example, if the Quality is Operational and the Risk is Severe, the service health shows a Critical status. Severe is the worst state of Quality and Risk.

Availability is an abstracted measure of service uptime and downtime that is based on the health of the service. The SA Manager measures service availability based on the service health:

Service Health	Service Availability
Normal|Minor|Major	Up
Critical|Down|Unknown	Down

For example, a severely degraded service has Down status even though the service is partially active. If the service maintained the Down status for 12 of the last 24 hours, availability would show as 50 percent for that period.

Severity

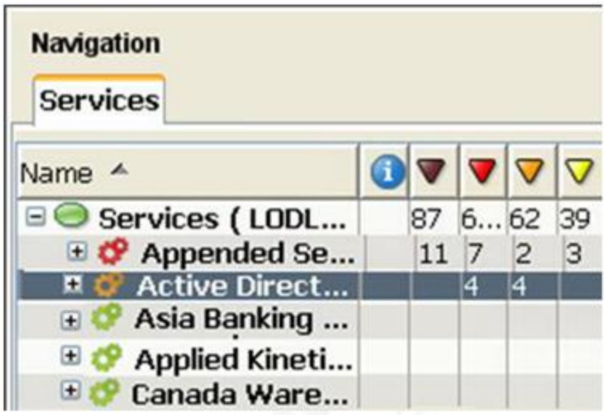
Severity indicates the condition of a CI as reported from the domain manager to CA SOI through alerts. If multiple domain managers send alerts for the same CI, the highest severity is used. CI severity helps determine the service impact by propagating the impact of the condition to related CIs in the service model according to propagation settings.

The following table describes each severity:

Severity	Color	Description
Normal	Green	Operational
Minor	Yellow	A nominal displacement of CI function that can require an inspection

Severity	Color	Description
Major	Orange	A serious causal change typically leading to degradation of function
Critical	Red	High probability of imminent failure and severe degradation of service
Down	Burgundy	The CI is incapable of providing function or service

Color-coded icons on the Operations Console indicate CI severity (the color-coded icons for services indicate the service impact). Alerts in the Contents pane have the color corresponding to their severity. The Navigation pane also represents severity in columns next to services and CIs. The following graphic shows that each column lists the number of items with the corresponding severity (represented by the colors in the previous table).



Navigation

Services

Name	ⓘ	▼	▼	▼	▼
⊟ Services (LODL...		87	6...	62	39
⊞ Appended Se...		11	7	2	3
⊞ Active Direct...			4	4	
⊞ Asia Banking ...					
⊞ Applied Kineti...					
⊞ Canada Ware...					

Note: If no alerts are raised for a CI, its severity is green even if the device contains child CIs with different severities. Also, groups are simply containers and would not usually have alerts. You can expand the tree and can follow the numbers to the row that lists the item whose severity you are looking for.

Configuration Item

A configuration item (CI) is a collection of information about a managed resource such as a printer, software application, or database. CA Catalyst uses an instance of a USM type for each CI. Connectors transform CIs between a domain manager format and USM.

CA SOI provides a view of CIs across all management domains in a single place, and provides a unified view from all the perspectives in which a CI is managed. CA Catalyst correlates and reconciles CIs managed by multiple domain managers so that CA SOI maintains one CI with a unified set of properties.

Events

An *event* is a message that indicates an occurrence or change in your enterprise. Events can indicate a negative occurrence or object state change. CA SOI Event Management lets you view and manage events that are received from all connectors. CA SOI collects events from various types of event sources:

- Domain managers that manage alerts indicating problems with their domain. Domain managers can include CA Spectrum for network faults, CA eHealth for network performance, CA NSM WorldView for system faults, and CA Application Performance Management for application performance
- High-volume raw event sources, such as CA NSM Event Management, SNMP traps, and IBM Tivoli Netcool

All collected events and alerts initially become events in CA SOI and are maintained in Event Stores that are distributed across the environment. The CA SOI Event Management component lets you manage a large event stream by exception using event policy to correlate, filter, and enrich events from any or all event sources. Event Management lets you control the types of information from the event stream that are displayed as actionable CA SOI alerts.

Infrastructure Alert

A domain manager reports an *infrastructure alert*, which is a fault condition on a CI in CA SOI. Events that are processed through Event Management become infrastructure alerts. CA SOI automatically associates infrastructure alerts with their corresponding CI and assigns a severity to each alert condition. The severity determines the CI color on the Operations Console. One CI can have several alert conditions simultaneously, and the alert with the highest severity determines the impact on the configuration item and its color. When the alerted CI belongs to a service, CA SOI calculates the impact value from the seriousness of the fault condition and the importance of the CI to the services it supports.

Infrastructure alerts typically include a URL so that an operator can navigate in context from the Operations Console to the originating domain manager and can view the alert in its original context.

Infrastructure alerts are service impacting when they affect a CI that is part of a managed service. Infrastructure alerts are non-service impacting when the infrastructure alerts affect CIs that are not part of a managed service. CA SOI displays and manages both infrastructure alerts types.

Alert Queues

Alert queues are user-defined alert groups. CA SOI auto-assigns alerts to a particular alert queue based on user-defined policy, which can include alert content and associated CIs. Alert queues let you group alerts as they come in based on specific criteria to monitor the status of your infrastructure more efficiently. You can add global and non-global escalation policies to alert queues to take a specified action automatically on alerts that come into a queue.

For example, consider a company with engineers responsible for different aspects of the infrastructure, such as networks, systems, and databases. Without defined queues, alerts from all integrated domain managers appear in one consolidated view on the Alert Queues tab. The administrator can define queues that are based on a domain (Network Alerts, Database Alerts, and so on). Engineers can then find and resolve their alerts quickly. The administrator can define additional queues that are based on other alert categories, such as severity, assignment status, or description for an optimized unified alert management system.

Services provide a similar organizational function as alert queues at a higher level with the additional benefit of resource topology and impact analysis. Defining alert queues is less intensive than modeling services, and they can simplify alert management as you make the transition to a service-oriented management paradigm. Alert queues are also useful in an environment with services defined to provide a supplemental management perspective outside of services. For example, you can define a queue for alerts that are not acknowledged or a queue for alerts from the same source domain manager.

Note: For more information and procedures about alert queues, see the *Event and Alert Management Best Practices Guide*.

Service

The concept of a service model, or referred to simply as a service, is central to CA SOI. A *service* typically consists of several CIs, which are grouped to represent entities like web server farms or clusters. Services can also contain *subservices*, which are subordinate service models. Service models typically represent high-level abstract entities like a web-based retail transaction service, an application server service, or a source control service. You can define any service type with CA SOI as long as one of the integrated domain managers monitors the service components.

CA SOI provides a comprehensive understanding of how a fault condition, which CA SOI represents through an infrastructure alert, impacts the business. Consider a managed resource such as a router, which you can accurately but narrowly define as a device that forwards data from one network to another. From a service perspective, however, a router is an indispensable component among other cooperating components that support interconnected business activities.

When router performance is compromised, the activities that depend on the router are often compromised as well. You can associate a router to other network devices, such as switches or servers. In turn, you can associate these devices with the applications or databases that they host. These relationships and dependencies comprise the logical and physical topology of the service. CA SOI lets you incorporate these relationships in the service model to capture how one configuration item relates to another and how they collectively deliver the service logic.

Service models contain policy that determines how alert conditions on one CI can impact related items and the service itself. You can modify and extend this policy to refine the model and capture the collective behavior of all associated entities.

You can reuse a service model any number of times, and you can combine it with other configuration items and services to build higher-level service models. For example, the DNS service can be critical to several higher-level services such as Microsoft Exchange and SAP. Similarly, Exchange itself can form part of higher-level services such as email, Blackberry, and so on.

You can define new service models, import them from domain managers, or define policies that automatically discover and create services according to specified criteria. For example, an operator can select configuration items that are discovered through integration with the domain managers and can create relationships among those configuration items. Similarly, if a service model (such as a business process view in CA NSM, a service model in CA Spectrum, or a service CI from the CA CMDB) is defined in a domain manager, you can import that service model and all its topographic information directly into CA SOI. You can extend or combine imported service models in the same manner as the service models defined in CA SOI, providing a powerful mechanism to leverage your existing investment.

Note: For more information and procedures about working with service models, see the *Service Modeling Best Practices Guide*.

Service Alerts

A *service alert* is an alert condition that CA SOI generates based on analysis of a modeled service that it is monitoring. Service alerts result when the condition of one or more CIs combines to impact the overall service quality or risk level. The policy that you define for that service model determines how CI alert conditions impact other CIs and the overall service.

You can use the Alert and Topology Views of the Operations Console to view the root cause infrastructure alerts that caused the service alert. You can also view the root cause type: root cause, symptom, or unclassified.

Customers

A *customer* in CA SOI is any consumer of a managed service. The CA SOI administrator creates customers and associates them with service models to see the impact of service degradation on the customer. Customer management provides an extra layer of security and insight into how end users dependent on provided services are affected when the services experience downtime or degraded performance.

For example, you can define a customer as a particular region of your company such as Europe, so that operators in that Europe see only the services and alerts particular to Europe. Similarly, you can define a customer that represents a division of your company. You can further define sub-customers, that represent entities within that division such as human resources and accounting.

For more information about customers, see the *Service Modeling Best Practices Guide*.

Components

CA SOI includes components that let you monitor services and resources, configure the product, add user groups, and perform other actions. The following section describes the chief components.

SA Manager

The *SA Manager* (also called SAM Application Server) is the primary management component in CA SOI. The SA Manager monitors the health and availability of managed resources and services. The SA Manager also processes events from connected applications and performs service impact and risk analysis. The SA Manager also does the following to integrate data:

- Updates the Persistent Store with USM data
- Updates the SA Store with analysis results and state changes

The SA Manager provides the following functionality for alert conditions:

- Automatic notification by email to indicate that an infrastructure or service alert has been created
- Automatic time-based escalation of alerts according to policy that, for example, notifies technicians or runs a command
- Creation of trouble tickets in CA Service Desk, BMC Remedy, or a custom help desk application with a relationship between the alert and its associated ticket

Note: For more information about alert escalation, see Viewing and Responding to Alerts (see page 55).

UI Server

The User Interface Server (*UI Server*) is the server that hosts the user interface applications.

CA SOI has the following user interfaces:

Dashboard

Displays service data that is tailored to the role of the user. Managers and others use this interface to analyze the overall health and availability of monitored services. They can also determine who is resolving problems and when those problems are fixed.

Administration UI

Provides tools for maintaining SA Manager and UI Server settings.

Operations Console

Supports all administrative functions, including service modeling, defining alert queues and defining associated policy, and provides an operational view of the data for analysis purposes. Operators and other technicians use this interface to view and respond to alerts that report fault conditions.

Mobile Dashboard

Provides content similar to the Dashboard in a format suitable for mobile devices. The Mobile Dashboard also lets you view service, alert queue, and customer details and take actions on alerts.

USM Web View

Lets you browse and search all USM data in the Persistence Store. You can use the USM Web View to locate specific information, browse data based on many different criteria, and subscribe to RSS feeds to be notified of updates to specific CIs. This interface also lets you create new CIs and update existing CI information.

CA SOI Workflow

CA SOI adds a service and operations management layer above the existing domain managers in your enterprise. CA SOI uses connectors and the overall CA Catalyst infrastructure to connect to the domain managers. Each domain manager is unique in the type of resources it manages, how it represents those resources, the alerts it raises, and so on. CA SOI translates this disparate data to standardized information to simplify the data visualization and issue resolution process.

The typical CA SOI service creation and administration workflow, from initial configuration to modeling to detailed reporting, is as follows:

1. **Configure security:** After installation, an administrator sets up security that defines the users and roles that will interact with the system.

2. **Define event policies:** Create the event policies optimize the quality of resultant alerts. For example, enriching alerts with contact information or creating an alert that is based on correlated conditions.

3. **Define the Alert Queues:** Establish the queues and policies that determine how operators visualize and manage alerts.

4. **Define the service:** Build service models in the Service Modeler that you open from the Operations Console. The Service Modeler lets an administrator build new service models by any combination of the following actions:

   - Importing CIs from the integrated domain managers
   - Importing existing service models from the domain managers or CA CMDB
   - Modifying any existing service models regardless of origin.

   Service modeling also includes the following features:

   - Creating associations and policy between CIs and services
   - Defining the user that is notified when an infrastructure or service alert is raised for the service
   - How any alert condition propagates
   - Whether and when the alert is raised as an incident in a supported helpdesk product.
   - Defining service level agreements that are associated with the service

5. **Define service access:** After a service definition, the administrator defines user groups that can view the service and its associated data. The access privileges determine the features user group can access: CA SOI features, services, customers, and alert queues. For example, a person responsible for monitoring the Payroll Service may need to view or access only HR-related services. Likewise, if CA SOI is monitoring services for several internal or external customers, each customer should have access to their own information only.

6. **Publish the service:** The administrator publishes a fully configured service so that CA SOI can begin to manage or instrument the service:

   a. The instrumentation process begins by determining the current active infrastructure alerts for each CI associated with the service model across all integrated domain managers. This process determines the overall state of the CI based on the highest impacting infrastructure alert condition.

b. Next, the propagation type and policy determine how the infrastructure alerts propagate across the model, and ultimately how they impact the service itself. If the service is impacted, one or more service alert conditions appear and the root cause information helps to diagnose and fix the problems. CA SOI also determines how an alert condition could impact a service by considering service quality, service risk, and overall service availability.

c. Alerts can enable a launch-in-context to the application reporting a fault condition, letting operators to gather more information to help diagnose and resolve an issue.

Note: For complete information about service modeling, see the *Service Modeling Best Practices Guide*.

7. **Define customers**: The administrator defines the customers to determine the system degradation impact to a specific customer.

   Note: For complete information about working with customers, see the *Service Modeling Best Practices Guide*.

8. **Manage alerts (see page 55):** As CA SOI detects infrastructure or service alert conditions, alerts appear on the Operations Console. The alerts are associated with services and alert queues and behave according to the associated escalation policies. A single infrastructure alert condition can affect multiple services (if the associated CI supports more than one service) or alert queues. Therefore, more than one alert escalation policy can be associated with the alert. Alert escalation policies automate the following escalation actions:

   - Alerting key personnel when alerts impact a service for which they are responsible.
   - Sending notifications when alerts have not been assigned or acknowledged during a specified time interval.
   - Raising a help desk incident for an infrastructure or service alert condition.
   - Running a command to help diagnose or fix the issue.
   - Running a CA Process Automation process.

   Note: For complete information about managing alerts, see the *Event and Alert Management Best Practices Guide*.

9. **View service information:** Conditions that impact a service are reflected across all views that may be supported for that service. The conditions are in the Operations Console (see page 29) and the Dashboard (see page 81).

10. **Report service details (see page 121):** You can run, configure, and schedule predefined reports on the service models to help managers make business decisions. The reports also show operators historical service and resource status. Reports can help you understand the impact of fault conditions and predict future issues that are based on past performance by spotting trends and chronic fault conditions.

Log into the Dashboard

You use a web browser to access the CA SOI interfaces using a URL (also known as a *web address*) provided by your system administrator. You log into the Dashboard.

Follow these steps:

1. Open your web browser and enter the URL provided by your system administrator.
2. Enter a valid user name and password.

   The CA SOI user interface opens to the Dashboard tab by default.

3. Click one of the following items:

   Dashboard tab

   Provides graphical information about service status. If you have not defined any services, the dashboard shows no data.

   Note: For more information, see Monitoring Services from the Dashboard.

   Reports link

   Displays the Business Objects CA SOI reporting interface. You must configure reporting before the Reports link is available.

   Note: For more information about working with reports, see Using Reporting (see page 121).

   Console link

   Displays the Operations Console, where you can view model services, monitor service status, and view and manage alerts. A Java application runs briefly when you start the Operations Console. For more information, see Managing, Viewing, and Responding to Alerts (see page 55).

   Google Earth link

   Launches a locally installed Google Earth instance with CA SOI services displayed according to their location property.

   USM Web View link

   Displays the USM Web View interface, which lets you search, browse, and interact with the store of USM data.

   Note: For more information, see Searching and Browsing USM Data with USM Web View (see page 145).

Chapter 3: Operations Console Basics

This section introduces how to navigate and customize the Operations Console.

This section contains the following topics:

Start the Operations Console

As an administrator or an operator you access the Operations Console from the Dashboard (see page 28).

On the Dashboard, click Console.

The Java Web Start dialog appears and indicates that the application is downloading then launching.

Note: You can receive an error that indicates you must install a higher JRE version. If the automatic installation does not work, manually download and install the latest JRE from the Java website and try to launch the Operations Console again.

Navigation Pane

The Navigation pane contains the following tabs:

Services

Lists services that have been imported from the domain managers or defined in CA SOI that you have the access privileges to view. You can navigate to the resources in the services, like servers and routers. The columns in the Services tab indicate whether each object is in maintenance mode, the granularity level, and the number of alerts of each severity currently open for each item.

Use the Filter fields in the List and Services tabs of the Contents pane to find specific CIs and services in the Services tab. Double-click a result to open the CI or service in the Services tab.

Alert Queues

Lists the set of alert queues and alerts on services that you have the access privileges to view. Each column displays the total number of alerts with that severity and the summation symbol column indicates the total number of alerts. Clicking an alert queue displays the alerts in that queue in the Contents pane. The alert queue icon color indicates the highest severity of any alert in the queue. Clicking the Information tab displays general information about the alert queue, associated escalation policies, cleared alert history, and user groups assigned to the alert queue.

Customers

Lists the defined customers. You create customers and associate them with service models to see the impact of service degradation on the service consumer.

Users

Lists the users and user groups that create service definitions, monitor alerts, and resolve the situations that cause the alerts.

Contents Pane

The Contents pane in the upper right of the Operations Console displays information about the services selected in the Navigation pane.

Note: Some tabs are not available based on selections in the Navigation pane.

When you select Services, the Contents pane displays the following tabs that contain information about services:

Alerts

Shows alerts for the service or CI selected in the Navigation pane. Select an alert to display details about it in the Component Detail section.

Note: Your administrator may have configured your view to be a subset of available alerts based on your role in the organization.

List

Displays resource name, health, quality impact, risk, granularity level, class, family, and IP address for resources that are direct children of the object selected on the Navigation pane. Use the Filter field in this tab to filter the displayed child CIs and services based on specified text. Double-click any object in this tab to open it in the Services tab.

Note: Quality impact and risk only apply to services.

Services

Displays service name, SLA status, health, quality impact, risk, priority, granularity level, operational mode, and management tier for subservices of the selected service, or for all services if you select the top-level Services item on the Services tab. Use the Filter field in this tab to filter the displayed services or subservices based on specified text. Double-click any object in this tab to open it in the Services tab.

Consider the following:

- The Tier column is hidden by default. Add this column if you have multiple CA SOI tiers. The column displays a value of Remote for services that come from remote CA SOI tiers. Any service with a value of Remote cannot be modified in the local Operations Console.
- The total number of services column (designated by a summation sign) is not shown by default. You can show this column by changing your Preferences (see page 46) for the Services Tab, Service Table Columns.

Topology

Displays a diagram that shows the relationships among the resources and subservices of the service selected in the Navigation pane.

Note: For information about topology, see Navigate the Topology View (see page 48).

Customers

Displays a list of all the customers that are associated with the service selected in the Navigation pane. This tab includes information about the customer name, customer identity, customer metrics, priority, and description.

Information

Shows details such as SLAs, maintenance schedules, role-based security for user groups, and the connector status for the selected service or CI. You can set service or CI properties such as Operational Mode, Priority, Location, maintenance schedules, and access privileges from the Information tab.

CMDB View

Displays the CA Service Desk interface in the context of CA CMDB CIs or services in CA SOI. The CMDB View tab only appears when a CA Service Desk/CA CMDB connector is present in any status on the SA Manager, and it is only selectable when you select an object from CA CMDB in the Operations Console. When you select a CA CMDB object and click the CMDB View tab, the CA Service Desk Log In page appears. Enter CA Service Desk user credentials to open the CA Service Desk interface that displays CI details, and click Visualizer to open the CMDB Visualizer, which displays the selected object and objects that relate to it.

Note: For more information about using and interpreting the CMDB Visualizer, see the CA CMDB documentation.

When you select Alert Queues, the Contents pane displays the Alerts tab, which shows the alerts that belong to the alert queue selected in the Navigation pane.

Component Detail Pane

The Component Detail pane in the lower right of the Operations Console displays detailed information about alerts, resources, or services. The information varies, depending on which tab you select in the Contents pane.

The Component Detail pane contains the following tabs, some of which may be unavailable based on the selections in the Contents pane:

Alert Details

Shows general details, annotations, update history, user groups with access to the alert queue, escalation action history, user-defined attributes, USM attributes, and so on, for the alert selected on the Alerts tab in the Contents pane. You can set alert properties and make annotations from this tab.

Information

Shows more information (such as general, SLAs, maintenance schedules, associated escalation policies, connector status, and so on) about the item selected on the Contents pane. If an alert is selected, the Information tab shows information about the service or CI associated with the alert.

Root Cause

Displays the alerts that have the highest impact on a service. If multiple alerts have equally high impact, you may see more than one root cause alert. Root cause alerts are categorized as Root Cause, Symptom, or Unclassified:

Root Cause

Identifies the root cause alert is the actual cause.

Symptom

Identifies the root cause alert is part of a root cause rule, but is not the root cause of the alert.

Unclassified

Identifies the root cause alert as neither Root Cause nor Symptom classifications.

Service Impact

Shows the business impact associated with the resource where the alert originated. This tab shows the name of the resource, the name of the associated service, the impact of the resource, and the health of the resource. Root cause alerts display all services impacted, including parent and associated services other than the service in which the CI is directly located. Non-root cause alerts only display the service in which the CI is located.

Customer Impact

Shows the customer impact level for all the customers that the selected service alert is impacting.

Alerts

Shows the alerts associated with the service selected from the List, Services, or Topology tab.

Cleared Alert History

Shows the alerts that have been created and cleared from a service or CI selected from the List, Services, or Topology tab. By default, this tab displays alerts cleared within the last 24 hours. You can change the time range using alert filters.

USM Properties

Shows the USM properties of the selected CI.

USM Notebook

Shows the USM properties of the CI from the perspective of all data sources and the reconciled set of USM properties.

Status Bar

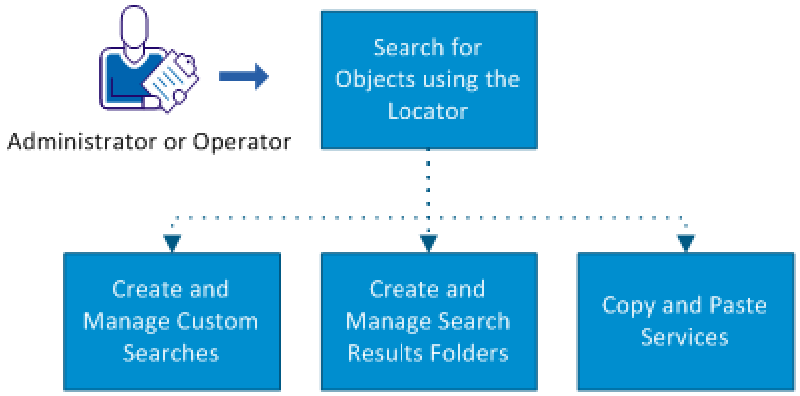
The Status bar at the bottom of the Operations Console provides a message icon 💬. Click the icon to display administrator messages.

How to Create and Manage Object Searches

As an administrator or an operator, you can search for objects in the CA SOI database with the Locator tool. Searches either run automatically when activated or prompt you for an input before performing the search. The Locator is useful when you know only partial information such as a part of an IP address. You can search monitored objects that belong to a service and staged objects that do not belong to a service.

Use this scenario to guide you through the process:

How to Create and Manage Searches


Administrator or Operator
Search for Objects using the Locator
Create and Manage Custom Searches
Create and Manage Search Results Folders
Copy and Paste Services

1. Search for objects using the Locator (see page 35).
2. (Optional) Create custom searches (see page 37).
3. (Optional) Create search result folders (see page 38).
4. (Optional) Copy and paste services (see page 38).

Search for Objects Using the Locator

You can search for objects in the SA Store database with the Locator tool. Searches either run automatically when activated or prompt you for input before performing the search. The Locator is useful when you know only partial information such as a part of an IP address. You can search both monitored and staged objects.

Follow these steps:

1. Open the Operations Console and click the Locator icon.
2. Double-click the item you want to search by in the Search Objects By tree.

   You can search by the following items:

   Custom Search Name

   Custom searches (see page 37) are user-created and named searches that either run automatically when activated or prompt you for input when activated.

   Category

   Specifies the object category, which is an optional string passed by an individual silo for each CI. Enter a partial or full search term.

   Examples: Windows, Linux, or database

   CIID

   Specifies the CI identification number, which CA SOI generates as a unique number for each CI in the database. Enter a partial or full search term.

   Class

   Specifies the class to search by. Select the class type from the drop-down list.

   Description

   Specifies a manually entered object text description. Enter a partial or full search term.

   Device ID

   Specifies the device identification number. Enter a partial or full search term.

   Granularity

   Specifies the granularity level (Low or Normal). Select the granularity level from the drop-down list.

   Instance ID

   Specifies the instance identification number. Enter a partial or full search term.

   IP Address

   Specifies the IP address. Enter a partial or full search term.

Launch in Context URL

Specifies the URL for launching the source application. Enter a partial or full search term.

Location

Specifies the physical address where the object resides.

Name

Specifies the object name, which you see in the Console. Enter a partial or full search term.

Namespace Map ID

Specifies the CI namespace map identification number. Enter a partial or full search term.

Notebook ID

Specifies the USM notebook ID number. Enter a partial or full search term.

Operational Mode

Specifies the operational mode. Select the operational mode from the drop-down list. You most often search for an operational mode of Maintenance.

Sheet ID

Specifies the identification number for a USM projection sheet. Enter a partial or full search term.

Source

Specifies the source domain manager from which the CI originated. For example, you could search for all CIs from a specific CA Spectrum installation. Each source is defined uniquely using a five-digit ID number defined by the USM schema. Select the object source from the drop-down list.

Note: For a list of connectors and their five-digit MdrProduct ID numbers, see the *Connector Guide*.

3. If a Search dialog displays, complete the dialog to perform the search:

   a. Enter a search value.

      Note: Leave the field empty to search all objects.

   b. (Optional) Select the Search Monitored Objects only check box to restrict the search to return only objects associated with a managed service. Clearing the check box includes all items in the search results, whether or not they are part of a managed service.

4. Click OK.

   Either the Results tab displays in the right pane with the results or a dialog indicates that no search objects were found.

   Note: Search results are limited to 5,000 by default. For more information about changing the default limit, see Set Preferences (see page 46).

5. (Optional) Right-click on a results row and select an item from the pop-up dialog:

   - Copy the monitored service into memory. You can then paste the object into the Navigation tree. For more information, see Copy and Paste Services (see page 38).
   - Add the selected objects to the modeled service in the Modeler. This option is available only if the Modeler is open; if multiple Modeler windows are open, the object is added to the last window opened.
   - Locate the object in the Navigation tree.

Create Custom Searches

You can create a custom search using comparisons and Boolean operators then save the search for reuse. You can also edit and delete the searches using the respective icons.

Follow these steps:

1. Open the Operations Console and click the Locator icon.
2. Click the Create a new search icon.
3. Select an attribute and comparison type.
4. Perform one of the following actions:

   - Select the Prompt check box then complete the Prompt for Value field. You are then prompted to enter an attribute value when you launch the search.
   - Enter an attribute value or select from the drop-down list (if available).

5. (Optional) Click Show Advanced and add more attribute criteria and create advanced logic using the logic buttons on the right-hand side of the dialog, then click Add.

   Note: For more information about creating advanced attribute criteria, click the Hints link above the expression pane.

   The attribute expression appears in the lower pane.

6. You can perform the following actions:
   - Click Launch to run the custom search.
   - Click Save As to set/change the search name or user access privileges for the custom search.
   - Click OK to add the custom search to the Search Objects by list once you have set a custom search name using Save As.

Create Custom Search Folders

You can create folders and subfolders to organize your searches. You can also edit and delete the folders.

Follow these steps:

1. Open the Operations Console and click the Locator icon.
2. Click the Organize icon.
3. (Optional) Select a folder if you want to create a subfolder.
4. Click Create Folder.
5. Enter a folder name and click OK.

Copy and Paste Services

You can copy and paste monitored services from the Locator search results and paste them as subservices in the Navigation pane.

Follow these steps:

1. Right-click a monitored service from the Locator results pane.
2. Click the Copy Service icon.

   Note: If the service is unmonitored, the icon is dimmed.
3. Switch to the Navigation pane.
4. Right-click the service or subservice under which you want to paste the copied service and select Paste.

   Note: If you copy and paste a top-level service, the original service is removed from its original top level and pasted as a subservice. However, if you paste a copied subservice, the original subservice appears in its original location and the new location.

   The copied service appears under the selected location.

How to View Object Audit Trails

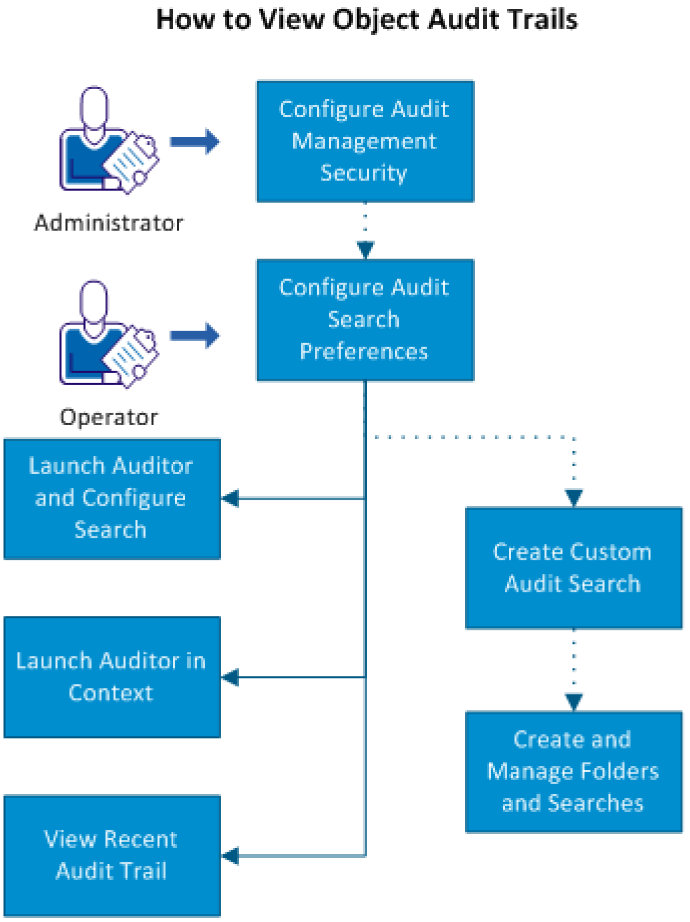
As an administrator or an operator (with access privileges), you can view the audit trail for objects (such as services, CIs, alerts, connectors, and so on). An audit trail shows updates to a selected object as tracked in the CA SOI database.

You can also create and manage custom searches and folders.

The following examples are a small subset of the many audit trail updates available:

- a state change
- acknowledged
- cleared
- created
- deleted
- maintenance mode

Use this scenario to guide you through the process:


How to View Object Audit Trails
Administrator
Configure Audit Management Security
Operator
Configure Audit Search Preferences
Launch Auditor and Configure Search
Launch Auditor in Context
View Recent Audit Trail
Create Custom Audit Search
Create and Manage Folders and Searches

1. (Optional) Configure the audit management security (see page 41).
2. (Optional) Configure your audit search preferences (see page 41).
3. Perform any of the audit trail searches:
   - Launch the Auditor and manually enter the audit trail search parameters. (see page 41)
   - Launch the Auditor in the context of an object (see page 42).
   - View the recent audit trail for an object (see page 42).
4. (Optional) Create custom audit trail searches (see page 42).
5. (Optional) Create and manage your custom audit trail search folders and searches (see page 43).

Configure Audit Management Security

The default user groups that CA SOI provides have Auditor access. However, if an administrator creates a user group, the administrator must configure the user group access in the Privileges tab Audit Management section.

Configure Audit Search Preferences

You can configure the maximum number of audit trail entries that CA SOI retrieves in the Auditor and the Information tab sub-views.

On the Operations Console, select View, Preferences, then select Auditor.

Launch Auditor and Manually Enter Audit Trail Search Parameters

You can launch the Auditor and manually select or enter search criteria.

Follow these steps:

1. On the Operations Console toolbar, click the Auditor ✎ icon.
2. Double-click a search type and perform the indicated action:

   Action Type

   Specifies the type of action that either CA SOI or a user performed. Select an action from the drop-down list.

   Internal ID

   Specifies the internal object or model identification number. This number varies depending on the object type. For alerts, the ID is the alert ID, for CIs and services, the ID is the CIID, and so on. Enter the number.

   Record Type

   Specifies the object record type. Select a record from the drop-down list.

   Time Stamp Range

   Specifies the audit trail time stamp begin and end time search range. Select or enter the date and time for the range.

   User Name

   Specifies the user login that performed the action. Enter the user name.

3. Click OK.

Launch Auditor in Context

You can launch the Auditor in context so that CA SOI automatically generates a search that is based on the context selection. For example, if you launch the Auditor with an alert selected, the Auditor shows the audit trail for the alert.

Right-click an object and select Launch CI Audit on objects in the following Operations Console locations:

- Navigation pane
- Topology chart
- Locator (see page 34) results

View Recent Audit Trail

You can view the recent audit trail entries for a selected object.

Follow these steps:

1. Select an object in any of the following locations:
   - Navigation pane
   - Topology chart
2. In the Component Details pane Alerts tab or Information tab, expand the Most Recent Audit Trail section.

   Note: If you select an alert in the Contents pane, the Information tab Recent Audit Trail section shows the entries for the CI related to the alert.

Create Custom Audit Trail Searches

You can create a custom audit trail search using comparisons and Boolean operators then save the search for reuse. You can also edit or organize (see page 43) the searches using the respective icons.

Follow these steps:

1. On the Operations Console toolbar, click the Auditor icon.
2. Click the Create a new search icon.
3. Select an attribute and comparison type.

4. Perform one of the following actions:
   - Select the Prompt check box then complete the Prompt for Value field. You are then prompted to enter an attribute value when you launch the search.
   - Enter an attribute value or select from the drop-down list (if available).
5. (Optional) Click Show Advanced and add more attribute criteria and create advanced logic using the logic buttons on the right-hand side of the dialog. Then click Add.

   Note: For more information about creating advanced attribute criteria, click the Hints link above the expression pane.

   The attribute expression appears in the lower pane.
6. You can perform the following actions:
   - Click Launch to run the custom audit trail search.
   - Click Save As to set/change the audit trail search name for the custom audit trail search. You can also select a folder for the custom search.

Create and Manage Custom Audit Trail Search Folders and Searches

You can create folders and subfolders to organize your audit trail searches. You can also rename, move, and delete the folders and custom audit trail searches.

Follow these steps:

1. On the Operations Console toolbar, click the Auditor icon.
2. Click the Organize icon.
3. (Optional) If you want to create a subfolder, select a folder.
4. Click Create Folder.
5. Enter a folder name and click OK.

Operations Console Customization

As an administrator or an operator , you can customize the Operations Console in the following ways:

- Specify which columns appear, resize columns, and sort column data (see page 44)
- Dock and undock panes (see page 44)
- Clone (copy) panes (see page 45)

- Set display preferences (see page 46), such as such things as which columns to display on the Alerts tab and the default filter to use for viewing all alerts.
- Export or import display preferences (see page 48)
- Navigate (see page 48), collapse, or expand (see page 52) the Topology view.

Customize Columns

You can change the way the Operations Console panes display table columns.

To specify the columns to display

1. Right-click a column heading.
2. Select the columns to display and click OK.

To specify column order

1. Select View, Preferences.
2. Expand Alerts Tab and Alerts Table, and click Column Order.

   Buttons for the available columns appear in a horizontal line.
3. Drag the buttons to the position you want, and click OK.

To resize columns

- Mouseover between columns so that the double-arrow icon opens. Click and drag left or right.
- Double-click the right side of a column header boundary to fit the column to the longest text it contains.

To sort columns

You can click a column heading to sort by that one heading or follow these steps to sort by multiple headings:

1. Right-click a column heading.
2. Click the Sort tab.
3. Select up to three columns by which to sort the table contents and whether to sort Ascending or Descending for each property, and click OK.

Dock and Undock Panes

By default, all panes open in the Operations Console; however, you can modify the view when necessary. Docked panes are visible on the main Operations Console page, and you can undock panes to separate them from the main page.

Each pane contains one of the following buttons:

◥

Undocks the pane from the Operations Console. The pane opens in its own window and is removed from the main Console view. The button changes to the Dock button, which is a mirror image of the Undock button. Undocking panes can help you to make better use of your screen space.

◣

Docks an undocked pane with the Operations Console. To display closed panes, click the View menu and select the pane to display. You can also use the View menu to dock undocked panes.

Clone Panes

Cloning opens the Contents or Component Detail pane in a separate window that contains another instance of the pane. Cloning is useful for viewing more than one area of the Operations Console simultaneously. If you navigate away from the original source, the cloned window information display is not affected.

To clone panes, click the Clone icon in the upper right corner of the Contents or Component Detail pane.

Note: If you click the Clone button in the Contents pane while the Component Detail pane is visible, a new window opens that contains instances of both panes.

Set Preferences

As an administrator or an operator, you set preferences that affect how the Operations Console displays information. You can specify such things as which columns to display on the Alerts tab, the default filter to use for viewing all alerts, and whether to add subcomponents to a service you are creating. Administrators can set preferences for either the logged in user only or for all users in a specified user group. An administrator can also lock a user group from changing any preference.

You can set the following preferences. The set preferences dialog provides more details about the preferences available for each tab.

Alerts Tab

Lets you set a global filter for all displayed alerts; specify whether a popup opens and a beep sound occurs for new alerts; control column order, the columns displayed, sort order of data in columns, and font; indicate whether a confirmation dialog opens when alerts are cleared (closed); and indicate whether the available ticket actions dialog displays when submitting a ticket.

Auditor

Lets you set the maximum number of audit entries the Auditor retrieves.

General

Lets you specify the default font for Information panes and tables; indicate the region used to format dates, times, and numbers; select an overall look other than the system default; specify the amount of scrollbar adjustment after a click of a scrollbar arrow; indicate whether the time format is 12-hour or 24-hour; select Coordinated Universal Time (UCT) instead of the default local system time zone; and specify the number of seconds that the cursor hovers over a button, field, or other component before a tooltip appears.

List Tab

Lets you specify the columns displayed, sort order of data in columns, and font.

Locator

Lets you set the maximum number of results returned and if only monitored objects are searched in the Locator dialog.

For more information, see Search for Objects Using the Locator (see page 35).

Modeler

Lets you set values for the Service Modeler window, which is where you create and edit services. You can specify the confirmation and other dialogs to display, the default display and layout style, the default values for new items added, whether to retain the previous settings when performing various actions, whether automatic policy maintenance is active, and whether to add sub-components when adding a parent object to a service.

Service Discovery

Lets you set display options for Service Discovery confirmation dialogs including warning dialogs.

Services Tab

Lets you specify a maximum number of elements to display and whether a warning opens if the limit is exceeded; control the columns displayed, sort order of data in columns, and font; control whether drag-and-drop of items in the Services tab is allowed and if a confirmation dialog displays; and specify how items are displayed when the Operations Console opens.

Topology

Lets you set values for the Topology tab in the Contents pane of the Operations Console. Some preferences are the same as for the Service Modeler because they both have a Topology view. You can specify the confirmation dialogs to display, the layout for imported services, and whether to retain the previous interface settings.

For more information, see Navigate the Topology View (see page 48).

Web UI

Lets you change the logo at the upper left corner of the browser interface, which has the Dashboard and Administration tabs. Changing the logo is useful for customers who want to display their own logo.

Follow these steps:

1. Access the Operations Console.
2. Do one of the following:
   - Select View, Preferences to set preferences for the logged in user.
   - Select the User tab, right-click a user group, and select Set Preferences to set preferences for all users in the selected user group.
3. (Optional) Click the type of preference you want to configure from the list in the left pane.

   Note: An alternative method is to click a plus (+) button to display a list of available preferences in the left pane.

4. Set the preferences you want to change, and click OK.

   Most preferences take effect immediately. The following preferences, however, require a restart of the Operations Console:

   - Alerts Tab, Alerts Table
   - General, Locale
   - General, Look and Feel

- General, Time Format
- General, Time Zone
- Services Tab, Initial View

5. (Optional) Select the Make Changes Permanent check box to keep your changed preferences the next time you log in.
6. Restart the Operations Console if the change did not take effect.

   The preference change takes effect for the logged in user or the selected user group.

Export or Import Preferences

Preferences affect how the Operations Console displays information. You can export preferences to a file so that another user or user group can copy them.

Follow these steps:

1. Open the Operations Console and select View, Preferences.
2. Click the top level to select all preferences, or click a subfolder containing the type of preferences you want to import or export.
3. Click the Export or Import button.
4. (Optional) Click one or more check boxes to remove the checkmark.
5. Click OK.

   The Select Users/Groups dialog opens.
6. Click a user or group, and click OK.

Navigate the Topology View

As an administrator or an operator, you can view, collapse, or expand the Topology. The Topology view is a graphical representation of the relationship among services and the devices that support them. Icons represent the object type, and arrows and the position of icons represent the relationships. CA SOI highlights the selected Object on the Services tab with small boxes.

Note: The Topology view is available in the main Contents pane and in the Service Modeler window. Some toolbar buttons described in this section do not appear on both windows.

Follow these steps:

1. Open the Operations Console, and perform one of the following actions:

   ■ Select a service from the Services tab in the Navigation pane and click the Topology tab in the Contents pane.

   ■ Select Tools, Create New Service.

   ■ Right-click a service from the Services tab in the Navigation pane and select Edit Service.

   One or more icons on the Topology pane represent the service.

2. Use the toolbar buttons as necessary to complete the following actions:

   (Pan Tool)

   Moves the topology up, down, right, and left when you click the tool and drag on the screen.

   Note: You can use the mouse wheel to zoom in and out.

   (Select Tool)

   Displays details about a service or resources when you click the tool then click a service or resource in the right pane. The details appear in the Component Detail area under the Topology.

   (Interactive Zoom Tool)

   Enlarges or reduces the topology when you drag the tool on the screen. Other zoom buttons include the Marquee Zoom Tool and Zoom Level Control.

   Note: You can also zoom by using the mouse wheel.

   (Link Navigation Tool)

   Displays relationships to and from objects when you click the tool and mouseover the object. The tooltip describes the relationship. For large topologies, click the relationship link to pan to the linked object at the other end.

   (Marquee Zoom Tool)

   Increases the magnification in a specific region when you click the tool and select a region in the right pane. Other zoom buttons include the Interactive Zoom Tool and Zoom Level Control.

   (Relationship Tool)

   (Service Modeler only) Specifies the type of relationship to create between objects when you click the tool and select one of the available relationships. Once you select a new relationship, all new objects obtain that relationship type.

● **(Adjust and View buttons)**

(Contents pane only) Rearranges the topology when you click the Adjust button and drag items. Click Save when you are finished to save the changes. Select the default option button View to disable further changes.

Note: You can also adjust the layout while in View mode when you click Apply Automatic Layout and select a layout from the drop-down list.

(Save Topology Layout)

(Contents pane only) Saves topology changes.

✓ **(Perform Service Validation)**

(Service Modeler only) Verifies that a service is complete and correct.

Note: Automatic validation occurs after every change to the service.

(Apply Automatic Layout)

Changes the type of chart when you click the button and select one of the following options:

Circular

Emphasizes clusters that are present in a network topology.

Grid

Arranges objects in horizontal rows and vertical columns.

Hierarchical

Emphasizes relationships among objects by placing them at different levels. The layout is like an organizational chart at a company, which is the default when you build services from scratch.

Orthogonal

Minimizes bend points by arranging objects horizontally and vertically, at 90 degree angles.

Symmetric

Emphasizes symmetries that are present in a network topology, which is the default for newly discovered services. Symmetric is also the fastest and yields the smallest topologies.

(Refresh Layout Contents)

(Contents pane only) Updates the service topology according to recent changes. The topology may require a refresh to reflect the current service topology if the SA Manager has a high processing load, a shutdown of the SA Manager interrupted processing, or a heavy volume of import events are being processed. When you click the button, you get a confirmation message that states one of the following:

- No topology updates were necessary
- All necessary topology updates are complete

(Delete Selected Topology Objects)

(Service Modeler only) Removes objects from the service when you select them and click the button.

(Straighten Selected Edges)

Removes bends in the links between items when you select a wavy line and click the button. This button is available in the Service Modeler, and in the Contents pane when you click the Adjust option button.

(Undo Last Action)

Discards topology changes.

(Redo Last Action)

Repeats your last action.

(Chart Complexity Level)

Displays the type of relationship among objects when you click the button and select Advanced. Simple is the default in the Contents pane, and Advanced is the default in the Service Modeler. When you select Advanced, the arrows between objects are color-coded and contain the first letter of the relationship type. When you select Advanced with Names, the arrows between objects are color-coded and contain the full name of the relationship type.

(Filter Configuration Item Condition Visibility)

(Contents pane only) Emphasizes severities when you click the button and select a severity. Items with severities lower than the one selected are dimmed. For example, if you select Major, items with Normal and Minor severities are dimmed.

For more information, see Severity (see page 19).

(Change Relationship Visibility)

Hides the links between objects when you click the button and select Hide ALL from the drop-down list. Show ALL is the default. On the Service Modeler, you can also select specific relationships (aggregates, bound, and so on).

(Toggle Item Highlighting)

(Contents pane only) Enables or disables synchronization with the Component Detail pane. By default, details for the selected item in the topology are displayed, but you may want to turn it off to increase performance when you adjust or navigate the service topology.

(Show/Hide Item List Pane)

Displays or removes a table of details beneath the Topology pane.

(Zoom Level Control)

Specifies the amount of magnification. Other zoom buttons include Interactive Zoom Tool and Marquee Zoom Tool.

(Toggle Overview Window)

Displays a small view of the topology. This window is useful when you want to change the region or zoom level of the topology view.

You can use the following shortcut keys to quickly switch between tools when the Topology pane is active and one of the tools is already selected:

- P: Pan Tool
- S: Select Tool
- I: Interactive Zoom Tool
- L: Link Navigation Tool
- Z: Marquee Zoom Tool

Collapse or Expand the Topology View

If a service is complex, you can show fewer items by collapsing child objects in the Topology view of the Contents pane or the Service Modeler.

Follow these steps:

1. Open the Operations Console, and complete one of the following actions:
   - Select a service from the Services tab in the Navigation pane, and click the Topology tab in the right pane.
   - Select Tools, New Service.
   - Right-click a service from the Services tab in the Navigation pane and select Edit Service.

   Note: The Topology view can take several seconds to load.

   One or more icons represent the service on the Topology pane.

2. Right-click an item with child objects, and select Collapse/Expand, Collapse.

   Note: An alternative way to collapse is to press Shift+click over the parent item.

   The child items are no longer visible. The parent item has a small plus icon (+) in the lower right.

To expand the Topology view

Right-click a parent item that is displayed with the + icon, select Collapse/Expand, and select one of the following options:

Expand

Opens all child items. (Expand performs the same function as Shift+click.)

Expand one level

Opens the next level of child items. (Expand one level performs the same function as double-clicking the plus (+) icon.)

Notes:

- You can undo (Ctrl + Z) or redo (Ctrl + Y) a collapse or expansion.
- You can save a collapsed or expanded view in the Service Modeler. You can save it in the Contents pane when you select the option button Adjust and click the Save icon. When the View option button is selected, you cannot save the layout.

Chapter 4: Managing, Viewing, and Responding to Alerts

This section contains the following topics:

Introduction to Alert Management

An *alert* is a message on the Operations Console that reports a fault condition that is associated with a resource or service.

Once service models are defined, alert conditions that impact configuration items in the integrated domain managers appear in CA SOI as infrastructure alerts. CA SOI provides a powerful and unified alert console that gives operators a view of the following items:

infrastructure alerts

A domain manager reports an *infrastructure alert*, which is a fault condition on a CI in CA SOI.

service alerts

A *service alert* is an alert condition that CA SOI generates based on analysis of a modeled service that it is monitoring.

Service alerts can originate from CA SOI based on analysis of the service model, impact policy, and active infrastructure alerts. They can also originate from a service-oriented domain manager, such as CA Spectrum Service Manager.

CA SOI alerts include details like the alert severity that the domain manager assigns and the number of services the alert impacts. In CA SOI, you can acknowledge (see page 65), assign (see page 65), annotate (see page 66), exempt (see page 68), and clear alerts (see page 66). You can send notification messages (see page 70) to notify technicians about an alert. Alerts can trigger escalation policy that performs actions such as automatically opening help desk tickets. Escalation policies are defined by your administrator. You can also perform some escalation actions manually (see page 69).

You can sort and filter alerts by any property and CA SOI can present alerts in several ways:

- The list of all service-impacting alert conditions. You can sort to show the most business critical (or highest service impacting) alerts across the entire service infrastructure.
- The list of alerts impacting a specific service and its subservices and configuration items.
- The list of alerts impacting a specific configuration item.

Operations personnel are responsible for the day-to-day tasks involved in monitoring the health of services and resources. The topics in this section explain the properties of an alert. The procedures help you get the most value from the alert management features of CA SOI.

Alert Properties and Extended Alert Information

CA SOI alerts contain the following properties. Some properties originate from the domain manager. Other properties (for example, service impact and number of impacted services) originate from CA SOI.

# Impacted Customers

Indicates the number of customers that the alert impacts. This number is based on the number of customers that are assigned to the service that the alert impacts.

# Impacted Services

Indicates the number of services the alert impacts based on the number of services its associated CI is included in.

Acknowledged

Indicates whether an operator has acknowledged the alert.

Assigned

Indicates the name of the operator that is assigned to the alert.

Category

Indicates whether this alert condition affects the quality or risk of the services it impacts.

Class

Indicates the class (USM type) of the CI the alert is associated with.

Date / Time

Indicates the date and time when this alert was generated.

Family

Indicates the CI class family that the alert is associated with.

Highest Customer Impact

Indicates the highest impact value that the alert causes for an associated customer.

Highest Customer Priority

Indicates the highest customer priority of a customer that is associated with a customer associated with a related service.

Is Exempt

Indicates whether the alert is excluded from impact analysis calculations.

Maintenance

Indicates whether the CI associated with the alert is currently in maintenance mode.

Name

Indicates the associated CI that the alert condition impacted.

Service Impact

Indicates the impact, which is calculated by multiplying alert severity and the significance of the CI to the service. When multiple services are impacted, the most affected service is displayed.

Service Impact Value

Indicates the impact value of the service alert. This value is always a factor of 10. The Service Impact Value displayed in the Alerts table can be different from the service impact value for the corresponding service in the Topology tab. The Topology tab displays how the child objects impacted the service.

Severity

Indicates the alert severity (see page 19) that the originating domain manager assigned.

Source

Indicates the domain manager where the alert originated. The format is *MdrProduct_domainserver@connectorserver*. For example, CA:00005_spectrohost.ca.com@spectrohost.ca.com refers to a CA Spectrum connector installed on spectrohost.ca.com monitoring a CA Spectrum instance that is installed on the same system.

Source Alert ID

Indicates the ID number of the alert in the source domain manager. Only infrastructure alerts have a Source Alert ID, because service alerts are generated in CA SOI, not from a source domain manager.

Summary

Describes the alert condition.

Ticket ID

Indicates the ID of the associated help desk ticket.

Unmanaged

Indicates whether the alert is associated with any services. An unmanaged alert does not have a service association.

User Attribute (1-5)

Indicates any configured customized values. These attributes are blank by default, but you can send values to the attributes through Event Management. You can also customize the attribute names.

You can also view the correlatable USM properties for the alert's associated CI:

- ModificationTime
- PrimaryIPV4Address
- PrimaryIPV4AddressWithDomain
- PrimaryIPV6Address
- PrimaryIPV6AddressWithDomain
- PrimaryMacAddress
- PhysSerialNumber
- BioSystemID
- Vendor
- AssetNumber
- PrimaryDnsName
- SysName

Note: For more information about USM properties, see the USM schema documentation. For information about how to access the USM schema documentation, see the *Connector Guide*.

In addition to these properties, alerts have associated extended information such as annotations, update history, and escalation history in the Alert Details tab. This information provides a full audit trail of the manual and automated actions that are taken to help diagnose and remedy an alert condition.

Annotations

Indicates the interim steps that were taken to resolve the situation that caused an alert. These comments highlight the incident management process in real time, and they can provide information for the problem management process.

Update History

Indicates how the alert has evolved since alert creation. Updates can include changes in severity and properties (such as the acknowledged flag).

Escalation Action History

Indicates the automated actions that notify, diagnose, or remedy the problem and the results of those actions. For example, if an email notification is sent, confirmation that it was sent successfully is included. If a remote device was pinged, the results are included. Escalation history therefore provides a detailed audit trail of the automated actions taken in response to an alert condition.

Alert Queues

Show the alert queues to which the alert belongs.

User Defined Attributes

Displays the names and values of the user-defined attributes.

Most Recent Audit Trail

Provides a list of recent object actions.

Severity

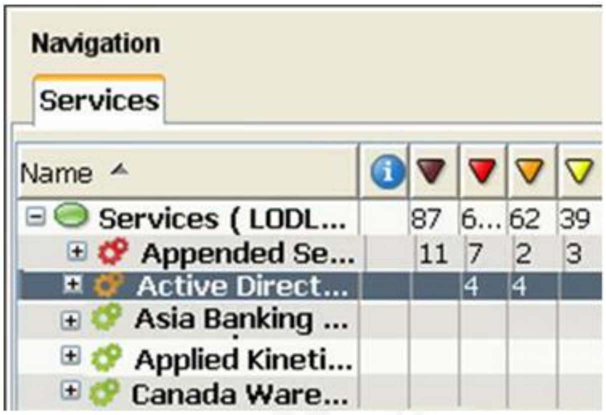
Severity indicates the condition of a CI as reported from the domain manager to CA SOI through alerts. If multiple domain managers send alerts for the same CI, the highest severity is used. CI severity helps determine the service impact by propagating the impact of the condition to related CIs in the service model according to propagation settings.

The following table describes each severity:

Severity	**Color**	**Description**
Normal	Green	Operational
Minor	Yellow	A nominal displacement of CI function that can require an inspection

Severity	Color	Description
Major	Orange	A serious causal change typically leading to degradation of function
Critical	Red	High probability of imminent failure and severe degradation of service
Down	Burgundy	The CI is incapable of providing function or service

Color-coded icons on the Operations Console indicate CI severity (the color-coded icons for services indicate the service impact). Alerts in the Contents pane have the color corresponding to their severity. The Navigation pane also represents severity in columns next to services and CIs. The following graphic shows that each column lists the number of items with the corresponding severity (represented by the colors in the previous table).



Name ▲	ⓘ	▼	▼	▼	▼
⊟ Services (LODL...		87	6...	62	39
⊞ Appended Se...		11	7	2	3
⊞ Active Direct...			4	4	
⊞ Asia Banking ...					
⊞ Applied Kineti...					
⊞ Canada Ware...					

Note: If no alerts are raised for a CI, its severity is green even if the device contains child CIs with different severities. Also, groups are simply containers and would not usually have alerts. You can expand the tree and can follow the numbers to the row that lists the item whose severity you are looking for.

View Alerts, Alert Details, and Extended Information

You can view alerts in several different ways in the Operations Console.

- To view all alerts impacting services, select the Services object at the top of the tree on the Services tab in the Navigation pane.

  Alerts that impact all services are displayed on the Alerts tab in the Contents pane.

- To view all alerts impacting a specific service, expand the tree on the Services tab in the Navigation pane (if necessary) and select the service whose alerts you want to see.

  Alerts that impact the service are displayed on the Alerts tab in the Contents pane.

- To view all collected alerts (which may or may not impact services), select the Alert Queues tab.

  The Alert Queues tab appears with the Alert Queues folder selected. Select a user-defined queue to view the alerts in that queue, or select the Default queue to view all alerts that do not belong in any other queue.

- To view details about an alert, click the alert in the Contents pane.

  Additional details about the alert appear in the Alert Details tab of the Component Detail pane. Other details are also shown such as annotations, update history, and escalation history. Click the plus sign (+) icon in these sections to view a history of actions performed on the alert.

  Note: You can also open the alert details as a separate window by right clicking the alert and selecting Alert Detail from the shortcut menu.

  You can sort alerts by clicking the column headings on the Alerts tab.

  The USM Properties and USM Notebook tabs display the USM properties for the alert. These properties differ from the properties displayed in the Operations Console, and you interact with these properties when you use Event Management functionality.

View All Services Impacted by an Alert

One configuration item may support more than one service, and therefore alert conditions affecting that CI may impact multiple services. CA SOI lets you see all services impacted by an alert and shows an impact value based on how critical that CI is to each service.

Follow these steps:

1. Expand the tree on the Services tab in the Navigation pane (if necessary) and select the service with alerts that you want to view. You can also select the Services object to display all alerts.

   The alerts display in the Contents pane on the Alerts tab.

   Note: You can sort alerts by clicking the column headings on the Alerts tab.

2. Click the alert whose services you want to see.

   The Alert Details tab opens by default in the Component Detail pane.

Note: You can also open the alert details as a separate window by right-clicking the alert and selecting Alert Detail from the shortcut menu. You can modify many of the properties (see page 64) displayed on the Alert Details tab.

3. Click the Service Impact tab in the Component Detail pane.

   The Service Impact tab displays a list of services this alert impacts, the extent of the impact on each service, and the current health of the service. Other details are also shown such as annotations, update history, and escalation history. Click the plus sign (+) icon in these sections to view a history of actions performed on the alert.

View the Root Cause of a Service Alert

CA SOI analyzes the alerts associated with a service to determine which alert has the highest impact and identifies this as the root cause alert. CA SOI classifies root cause alerts as Root Cause, Symptom, or Unclassified. CA SOI provides rules that determine the root cause alert classification. CA SOI determines the classification in the following order:

Root Cause

Identifies the root cause alert is the actual root cause.

Symptom

Identifies the root cause alert is part of a root cause rule, but is not the root cause of the alert.

Unclassified

Identifies the root cause alert as neither Root Cause nor Symptom classifications.

For example, ComputerSystem A is low on memory, which causes Application X to run out of memory. The Root Cause is the low memory alert associated with ComputerSystem A. The Symptom is the out of memory alert associated with Application X. The root cause rules establish that the low system memory can cause the out of memory errors on the application, and the service model ensures that Application X is running on ComputerSystem A.

You can use the root cause classification as an attribute criteria for creating escalation policy and alert queue rules.

Follow these steps:

1. Expand the tree on the Services tab in the Navigation pane (if necessary) and select the service whose alerts you want to view, or select the Services object to display all alerts.

   The alerts are displayed in the Contents pane on the Alerts tab.

2. (Optional) Select the filter Service Alerts from the Available filters drop-down list on the Alerts tab of the Contents pane.

   The Alerts tab displays only service alerts.

3. Click the alert whose root cause you want to see.

   The Alert Details tab opens by default in the Component Detail pane.

4. Click the Root Cause tab in the Component Detail pane.

   The Root Cause tab displays the alert that corresponds to the root cause of the fault condition that affects the service.

   Note: If multiple alerts have equally high impact, you may see more than one alert.

Launch Alert Source

From the Operations Console, you can launch the domain manager application that is the source of an infrastructure alert to view more information about the issue.

To launch alert source, right-click an infrastructure alert and select Launch <*Domain Manager*>, where *Domain Manager* is the name of the domain manager interface to launch.

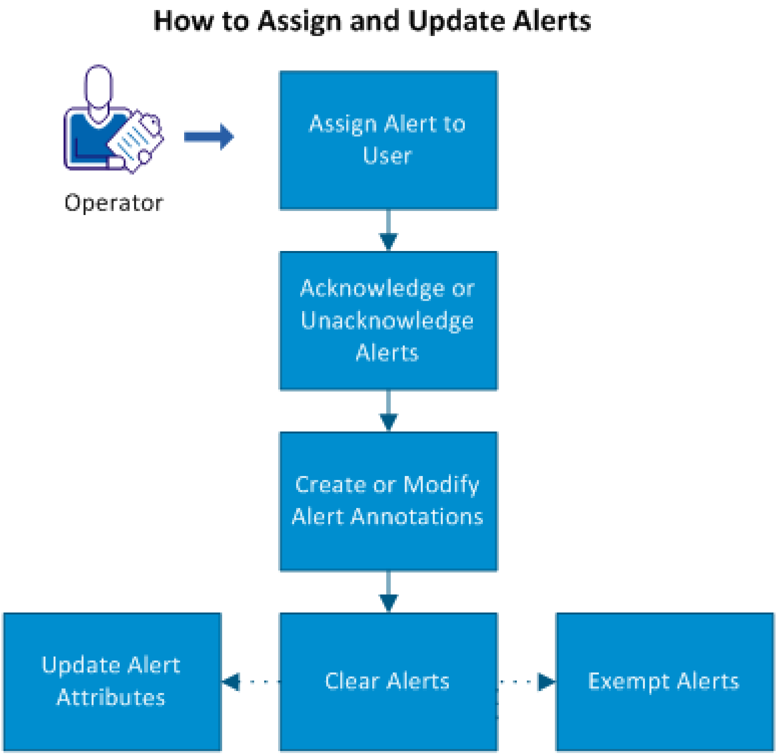
The domain manager interface opens in the context of the alert. You may have to enter valid product credentials to log in to the interface.

If the Launch option is not available, configure launch in context in the connector. For information about how to configure launch in context in CA Catalyst connectors, see the *Connector Guide*.

How to Assign and Update Alerts

As an operator you can update alerts and notify other users. Your administrator sets the features available to you. If a feature is not available, contact your administrator.

Use the following scenario to guide you through the process:


How to Assign and Update Alerts
Operator
Assign Alert to User
Acknowledge or Unacknowledge Alerts
Create or Modify Alert Annotations
Update Alert Attributes
Clear Alerts
Exempt Alerts

1. Assign an alert to a user to resolve the issue (see page 65).
2. Acknowledge or unacknowledge the alert (see page 65).
3. Add an alert annotation (see page 66).
4. Clear an alert (see page 66).
5. (Optional) Update the alert attributes (see page 67).
6. (Optional) Exempt alerts (see page 68).

Assign Alerts

When an alert arrives on the Operations Console, you assign someone to resolve the situation that caused it. The steps taken to solve the situation are recorded in the Update History section on the Alert Details tab of the Component Detail pane.

Note: This feature is available only if you have appropriate access privileges. For more information, contact your CA SOI administrator.

Follow these steps:

1. Select an alert to assign in the Alerts tab.
2. Click the *set* link next to the Assigned property in the General Information section.
3. Enter an assignee, and press Enter.

Acknowledge or Unacknowledge Alerts

The first step in resolving an alert is acknowledging its existence. Because acknowledgment creates an audit history entry that identifies who acknowledged the alert, you can also use acknowledgment to indicate alert ownership.

Note: This feature is available only if you have appropriate access privileges. For more information, contact your CA SOI administrator.

To acknowledge an alert, right-click an alert and select Acknowledge.

Note: An alternative is to select one or more alerts and click the icon *Acknowledge selected alerts* on the toolbar. This icon lets you acknowledge multiple alerts at a time.

A checkmark appears in the Acknowledged column.

Note: If you acknowledged the wrong alert, you can remove the checkmark by clicking the *Unacknowledge selected alerts* icon.

Create or Modify Alert Annotations

Annotations are comments that can track the steps to resolve the situation that caused an alert.

Note: This feature is available only if you have appropriate access privileges. For more information, contact your CA SOI administrator.

For information about annotating multiple alerts at the same time, see Update Alert Attributes (see page 67).

Follow these steps:

1. Click the alert to annotate.

   Note: If you want a larger detail window, right-click the alert and select Alert Detail.

2. Scroll down to the Annotations section on the Alert Details tab, and click the plus sign icon (+) to open the section.

   A small toolbar and a container for multiple annotations appear.

3. Complete one or both of these actions:

   - Click *Adds a new annotation* ⊕, enter text in the dialog that opens, and click OK.

   - Select the annotation to modify, click *Modifies the selected annotation* 📝, update the text in the dialog that opens, and click OK.

   Note: You can also print the annotations and export them to a CSV (comma separate values) file. Click the Print or the Export icons in the Annotations section.

Clear an Alert

You clear an alert when you resolve the situation that caused creation of the alert.

Note: This feature is available only if you have appropriate access privileges. For more information, contact your CA SOI administrator.

After you clear an alert, you can view cleared alert history in the following places for historical analysis:

- In the Cleared Alert History tab of the Component Detail pane when you select a service. This tab displays all cleared alerts that were once associated with the selected service.

- In the Cleared Alert History table of the Contents pane Information tab when you select an alert queue. This tab displays all cleared alerts that were once associated with the selected alert queue.

Follow these steps:

1. Right-click the alert and select Clear.
2. Click OK.

   The alert is cleared and removed from the Alerts tab. Any associated help desk ticket is also closed.

Update Alert Attributes

You can manually add values for the following attributes from the Write Alerts dialog:

- Annotations
- Assigned
- Ticket ID

This feature lets you quickly make a note in the alert, specify an assigned technician, or manually link the alert with a corresponding help desk ticket.

If you have integrated CA SOI with a help desk application such as CA Service Desk or BMC Remedy, the Ticket ID attribute should populate automatically for incidents created based on the Create Ticket escalation policy.

Note: This feature is available only if you have appropriate access privileges. For more information, contact your CA SOI administrator.

Follow these steps:

1. Perform one of the following actions:
   - Right-click an alert and select Write Alerts.
   - Select multiple alerts using the Ctrl key, right-click any of the selected alerts, and select Write Alerts.
2. Select the attribute to update in the Attribute drop-down list, enter an attribute value in the Attribute Value field, and click OK.

   Note: If you selected multiple alerts, all alerts inherit the specified annotation, assignment, or ticket ID.

Exempt or Unexempt Alerts

You can exempt an alert if you do not want the condition of the alert to affect the overall status of a service. You can only exempt infrastructure alerts, not service alerts. When a user exempts an alert, the name of the alert is dimmed to let other users know it is exempt. To exempt or unexempt an alert, use the following feature.

You can manually exempt alerts on the Operations Console. The exempted alerts appear dimmed in the Alerts tab.

Follow these steps:

1. Select a service in the Services Tab or an alert queue in the Alert Queues tab.
2. In the Contents pane Alerts tab, select an alert or press Ctrl/Shift + click to select multiple alerts.
3. Click the Exempt selected alerts +▽ icon.

   The exempted alerts are dimmed.

   Consider the following items:

   - You can also right-click an alert and exempt the alert with the context menu.
   - To unexempt the alerts, repeat the same steps and click the Unexempt selected alerts −▽ icon.
   - You can add the Exempt column to the Alerts tab. The column displays Yes or No for Exempt/Unexempt alerts. For more information about adding columns, see the *User Guide*.

The Alert Details tab lets you view and change the Exempt status of the selected alert.

How to Escalate Alerts

As an operator, you can manually escalate alerts by taking a defined action or sending an email notification.

Alert escalation is the ability to enact some escalating action as a result of an alert. Actions include opening a help desk ticket, running a command, sending an email, and so on.

Depending on your access privileges, you can manually escalate an alert in the following ways:

- Take a defined escalation action (see page 69)
- Send an email notification (see page 70)

Any user can view a help desk ticket associated with an alert, regardless of user access privileges.

Take Action on an Alert

You can take any defined action on alerts that are displayed either on the Services tab or on the Alert Queues tab in the Contents pane.

Follow these steps:

1. Right-click an alert in the Operations Console Alerts tab and select Take Action.

   Note: If there is already a default action set, the default action performs. To change the default action, change the preference (see page 46) from the Alerts Tab folder in the View, Preferences menu item.

2. Perform one of the following actions:

   - Select an existing escalation policy action.
   - Click Create and create an action in the Escalation Action Editor dialog.

3. (Optional) Select the Use this selection as the default and do not show this dialog again check box. This option hides the dialog in the future and uses the default action.

4. Click OK.

   CA SOI attempts to perform the action. A dialog opens indicating whether the action succeeded or failed.

5. (Optional) Click Show Details to view successful or failure information.

6. Click OK.

Send an Alert Email Notification

You can notify a technician about an alert situation. For example, the technician may need to fix a resource or restart a service. You can send an email that contains the information in the alert.

Note: This feature is available only if you have appropriate access privileges. For more information, contact your CA SOI administrator. If this feature is unavailable, contact your administrator.

Follow these steps:

1. Right-click an alert and select Mail.

   Note: An alternative is to select one or more alerts and click ✉ on the toolbar. This icon lets you send information about multiple alerts.

2. Perform one of the following actions:

   - Enter an address in the To: field and other addresses in the CC: field. Only the To: field is required.
   - Enter a subject in the Subject field.
   - Select email or pager in the Template field.
   - (Optional) Edit any text in the body of the message.

3. (Optional) Click Edit to remove one or more alert fields from the message. Select the check box for the fields you want to send and click OK.

4. In the Mail Selected Alerts dialog, click Send.

Work with Alert Tables

Alerts associated with a resource or a service are organized in alert tables. You can print or export alert tables.

Export a Table of Alerts

You can export the alerts associated with a service to a CSV file. The table is in the same format as the container on the Alerts tab. You can use the file in a spreadsheet or other application that reads comma-separated value files.

Note: You can also export alert annotations, history, and associated queues in the Component Detail pane.

Follow these steps:

1. Expand the tree on the Services or Alert Queues tab in the Navigation pane (if necessary) and select the service or alert queue whose alerts you want to export.

   The alerts for that service or alert queue are displayed in the Contents pane on the Alerts tab.

2. Click on the toolbar.
3. Select a location and click Save.

Print a Table of Alerts

You can print the alerts associated with a resource or service in tabular format on a local or network printer. The table is in the same format as the container on the Alerts tab. If one of your printers is Adobe PDF, you can create a PDF file.

Notes:

- You can print the entire table or only selected alerts. If one alert is selected, you can print alert details for it.
- You can print alert annotations, history, and associated queues in the Component Detail pane.

Follow these steps:

1. Right-click any alert and select Print.

   Note: An alternative is selecting File, Print, and then selecting *Alerts* from the drop-down list on the dialog that opens.

2. Select printer options, if necessary, and click OK.

View Service Information

To view details about a service select a service in the Services tab and click the Information tab in the Component Detail pane.

The Information tab displays the following service information:

Note: Depending on your user group privileges, you may not be able to edit all properties in this tab.

Service Name

Displays the name of the service at the top of the tab.

General Information

Displays a list of the following basic service information:

Health

Displays the service health state.

Quality Impact

Displays the impact of infrastructure alerts on service quality.

Risk

Displays the risk of infrastructure alerts on service quality.

Family

Indicates the CI class family that the alert is associated with.

Operational Mode

Displays the current operational mode, either Production or Maintenance.

Priority

Displays the service priority value.

Location

Displays the service location.

Description

Displays the service description. Click Set to enter a new description.

Service Level Agreements

Displays the SLA associated with the service with information such as name, status, and description.

Maintenance Schedules

Displays maintenance schedules associated with the service. From this table, you can edit an existing maintenance schedule.

Connectors

Displays the connectors managing the service CIs.

How to View Alert Queues

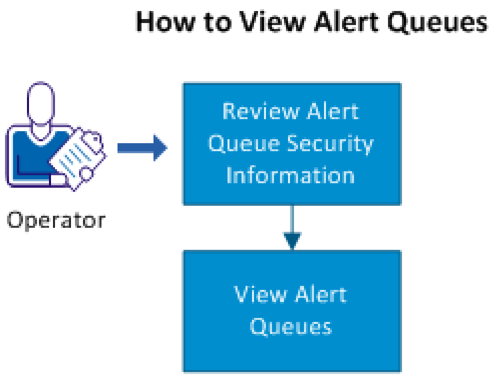
As an operator, you can view alert queues to which an administrator has assigned you access.

Alert queues are user-defined alert groups. CA SOI auto-assigns alerts to a particular alert queue based on user-defined policy, which can include alert content and associated CIs. Alert queues let you group alerts as they come in based on specific criteria to monitor the status of your infrastructure more efficiently. You can add global and non-global escalation policies to alert queues to take a specified action automatically on alerts that come into a queue.

For example, consider a company with engineers responsible for different aspects of the infrastructure, such as networks, systems, and databases. Without defined queues, alerts from all integrated domain managers appear in one consolidated view on the Alert Queues tab. The administrator can define queues by domain (such as Network Alerts or Database Alerts). With organized queues, engineers can quickly find and resolve their alerts. Additional queues could be defined based on other alert categories, such as severity, assignment status, and description to enable an optimized unified alert management system.

Services provide a similar organizational function as alert queues at a higher level with the additional benefit of resource topology and impact analysis. Defining alert queues is less intensive than modeling services, and they can simplify alert management as you make the transition to a service-oriented management paradigm. Alert queues can also remain useful in an environment with services defined to provide a supplemental management perspective outside of services. For example, you can define a queue for alerts that have not been acknowledged or a queue for alerts from the same source domain manager.

Use this scenario to guide you through the process:



1. Review alert queue and security information (see page 74).
2. View your alert queues (see page 76).

Review Alert Queue Security Information

The following topics explain how the administrator provides you access to alert queues.

Alert Queues and Security

Your CA SOI administrator assigns you to user groups. The administrator sets user group access to specific CA SOI features, services, alert queues, customers, and so on. Consider the following items when viewing alert queues:

- You can see all non service-impacting alerts and they can show in your alert queues. Because non service-impacting alerts are not associated with a service, they cannot be restricted with access privileges.
- You can see alert queues only to which you have access privileges.
- You can see alerts in alert queues only on the services to which you have access privileges.
- You can edit alert queues for which you have access privileges. Only administrators can edit the Default queue.
- You can only delete alert queues that you created.

Example: User Group Access to Alert Queues

In this example, we have the following data in CA SOI:

Services: Sales, Finance, Operations

Note: Because service privileges also dictate the services that appear in a particular alert queue, this example also includes the service access settings.

Alert Queues: Database Alerts, Critical Alerts

Note: For this example, the alert queue names indicate the type of alerts that each alert queue is configured to show. For example, if the Sales service has a critical alert, the Sales service appears in the Critical Alert queue (assuming the User Group has access privileges for the Sales service.)

User Groups: Group1, Group2, Group3, Admin

The following table shows the User Groups and their access to available services and alert queues:

User Group	Service Access	Alert Queue Access
Group1	Sales, Operations	Database Alerts
Group2	Finance, Operations	Critical Alerts
Group3	Operations	Database Alerts, Critical Alerts
Admin	All Services	All Alert Queues

The following table shows the User Groups and what they see in CA SOI based on their service and alert queue access:

User Group	Sees on the Services Tab	Sees on the Alert Queues Tab
Group1	Sales, Operations	Database Alerts queue with database alerts impacting to Sales and Operations services and all unmanaged database alerts.
Group2	Finance, Operations	Critical Alerts queue with critical alerts related to the Finance and Operations services and all unmanaged critical alerts only.

User Group	Sees on the Services Tab	Sees on the Alert Queues Tab
Group3	Operations	Database Alerts and Critical Alerts queues with critical alerts related to the Operations service and unmanaged critical database alerts only.
Admin	All Services	All alert queues with all managed and unmanaged alerts.

View Alert Queues

You can display the alerts in a selected alert queue and view detailed information about a selected alert.

Follow these steps:

1. Start the Operations Console and click the Alerts Queues tab in the Navigation pane.

   The alerts queues for which you have access privileges display. The columns to the right of the queue name display the number of alerts of each severity in the queue and the total number of alerts in the queue. The alert queue icon color indicates the highest severity of any alert in the queue.

2. Select an alert queue.

   The alerts in the selected alert queue displays in the Contents pane. The Contents label displays the currently selected queue.

3. Select the Information tab in the Contents pane.

   The Information tab displays queue details, such as description, criteria, priority, associated escalation policies, and cleared alerts that once belonged to the queue.

4. Return to the Alerts tab, and click an alert to display detailed information about that alert.

   For more information about viewing alert details, see View Alerts, Alert Details, and Extended Information (see page 60).

How to View Customers and Customer Details

As an operator, you can view customers and see how alerts impact the customers.

A *customer* in CA SOI is any consumer of a managed service. The CA SOI administrator creates customers and associates them with service models to see the impact of service degradation on the customer.

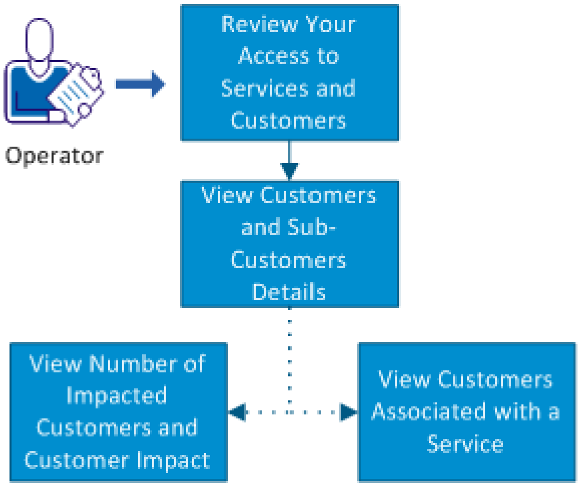
Your CA SOI administrator assigns you a customer and sets the specific services that you can view for that customer. Therefore, the following access privileges limit your service access for each customer:

- Your user group access to services.
- Your customer access to services.

If you need access to additional services or customers, contact your administrator.

Use this scenario to guide you through the process:

How to View Customers and Customer Details


Operator
Review Your Access to Services and Customers
View Customers and Sub-Customers Details
View Number of Impacted Customers and Customer Impact
View Customers Associated with a Service

1. Review the information about your access to services and customers (see page 78).
2. View customers and sub-customer details (see page 78).
3. (Optional) View the number of impacted customers and the customer impact (see page 79).
4. (Optional) View the customers that are associated with a service (see page 80).

Your Access to Services and Customers

Your CA SOI administrator assigns you to user groups. The administrator sets user group access to specific CA SOI features, services, alert queues, customers, and so on.

If you require access to a specific service or customer, contact your administrator.

View Customer and Sub-Customer Details

You can view information about customers and sub-customers, including list of sub-customers, associated services, and associated service alerts.

Follow these steps:

1. Open the Operations Console and click the Customers tab in the Navigation pane.

   A list of all customers displays. The columns to the right of the customer name display the number of alerts of each severity for the customer and the total number of alerts for the customer. These alerts are the alerts that are impacting the services that are assigned to the customer.

   If a customer is associated with a service and an alert is generated that impacts that service, the alert also impacts the associated customer. An alert can impact multiple customers for the following reasons:

   - Because multiple customers are associated with a single service.
   - Because an alert impacts multiple services and each service has an associated customer.

2. View the customer tree icon color for any customer to see the overall customer health. Of all the services that are assigned to the customer, the service with the worst health represents the customer health. The customer tree icon color, therefore, shows the color that is based on that service's health.

3. Select a customer (or sub-customer) in the Customers tree and do any of the following tasks:

   - Click the Alerts tab to view all the alerts (from the services that are assigned to the selected customer) for the customer. This tab includes information about alert severity, category, summary, count of impacted customers, and so on.

     Note: You can also display the number of impacted customers by adding the # Impacted Customers column (see page 44).

     When you remove or add a service to a customer, the associated alert list is changed accordingly.

     Note: The alert list for the parent customer shows the aggregate of all alerts from all of its child customers.

   - Click the Services tab in the Contents pane to view a list of all services that are associated with the customer. This tab includes information about the service name, health, risk, granularity, and so on.

- Click the List tab in the Contents pane to view a list of sub-customers. This tab includes information about the all the sub-customers available under the selected parent customer. The tab displays the customer name, ID, priority, impact (or customer health), quality, risk, and description.

  Note: Of all the services that are assigned to the customer, the service with the worst health represents the customer health. Similarly, the service with the worst quality represents the customer quality, and the service with the maximum risk represents the customer risk.

- Click the Information tab in the Contents pane to view general information about customers. This tab includes general information about the customer: name, ID, and priority. This tab also includes current metric information: health, quality impact, risk, and priority. The Security pane shows the user groups that have access to the customer.

- Click the Customer Impact tab to view the customer impact level. This tab is available to user groups with access privileges only.

4. Review the information. For the Services and Alerts tabs, you can use the additional tabs in the Component Detail pane to get detailed information.

View Number of Impacted Customers and Customer Impact

You can view the number of impacted customers due to an alert and the customer impact.

Follow these steps:

1. Open the Operations Console and click either the Services tab or the Alert Queues tab.
2. Select a service or an alert queue.
3. The Contents pane displays the column "# Impacted Customers" which indicates the number of customers that the alert impacts.
4. Select an alert and select the Customer Impact tab in the Component Details pane.

View Customers Associated with a Service

You can view all the customers that are associated with a specific service. This information helps you analyze the impact that a particular service has on different customers. When an administrator associates or removes a service from a customer, CA SOI updates the information in the Customers tab accordingly.

Follow these steps:

1. Open the Operations Console and click the Services tab.
2. Select a service for which you want to see the associated customers.
3. Click the Customers tab in the Contents pane.

   All customers that are associated with the selected service display in the pane. The pane also provides detailed information about the related customers; for example, name, ID, description, priority, and so on.

Chapter 5: Monitoring Services from the Dashboard

This section describes how to customize and interpret the service data that displays on the Dashboard. The Dashboard is accessible as a PC browser-based interface (see page 83) and as a mobile device interface (see page 107).

This section contains the following topics:

Dashboard Terminology

This section describes some common terms as they relate to the CA SOI dashboard.

Risk

Risk indicates the likelihood of delivering the quality of service that is required to support the overall business objectives. The highest propagated impact of an associated risk alert determines the service risk value. If an alert has no defined type, it is a risk alert by default.

In an IT infrastructure, risk is the measure of how much the problems that are currently associated with an IT element impacts the likelihood that the required service quality levels are delivered. In other words, as IT elements encounter problems, the risk of service quality degradation increases.

Due to typical IT risk-mitigation measures such as redundancy, fault tolerance, and high availability, faults in the IT infrastructure may not directly result in service quality degradation. However, these faults do increase the *risk* of delivering the required service quality.

For example, consider a server farm that has 12 servers that support an online application:

- If three of the servers are unavailable, the risk of a service outage can be considered Slight.
- If six of the servers are unavailable, the risk of a service outage can be considered Moderate.
- If ten of the servers are unavailable, the risk of a service outage can be considered Severe.

The risk settings are Down, Severe, Moderate, Slight, None, and Unknown.

Quality

Quality indicates the level of excellence that consumers of an IT service experience, whether the consumers are customers, end users, or other IT services. The levels of quality are Operational, Slightly Degraded, Moderately Degraded, Severely Degraded, Down, and Unknown. The highest propagated impact of an associated quality alert determines the service quality value.

For example, the transaction time that is associated with completing a user task, such as logging in to the system, is a quality metric. Quality metrics are typically associated with a threshold. For example, if transaction time exceeds 5 seconds, the service quality could be considered to be Moderately Degraded.

Health

Health is a reflection of the worst state that of either Quality or Risk. Health provides a high-level summary of the service health according to those metrics.

For example, if the Quality is Operational and the Risk is Severe, the service health shows a Critical status. Severe is the worst state of Quality and Risk.

Availability

Availability is an abstracted measure of service uptime and downtime that is based on the health of the service. The SA Manager measures service availability based on the service health:

Service Health	Service Availability
Normal|Minor|Major	Up
Critical|Down|Unknown	Down

For example, a severely degraded service has Down status even though the service is partially active. If the service maintained the Down status for 12 of the last 24 hours, availability would show as 50 percent for that period.

Priority

Priority indicates the importance of a service to the business. Priority determines the following orders:

- The order in which the Dashboards display all services.
- The order in which escalation policies run when they affect more than one service.

SLA

A *service-level agreement* (SLA) is a contract that specifies the service expectations of internal or external customers. An example is the downtime that is acceptable for various resources.

Access the Dashboard on a PC

As an administrator or an operator, you access the Dashboard on a PC, log in to CA SOI (see page 28) and click the Dashboard tab.

View Service Status and Details

As an administrator or an operator, you view the status of services and the service details.

The Dashboard tab contains the Services table. The table displays information about the services that CA SOI is monitoring and managing. Below the table, charts display additional detail about a selected service.

Follow these steps:

1. Click the Dashboard tab.

   By default, the Services table includes the following columns:

   Note: You can resize the table height to display more or less services per page; however, you cannot adjust the width.

   Services

   Displays the name of the service. If the service name includes a number in parentheses next to its name, that number represents the count of subservices in the next level only (not subservices of those subservices).

   Use the Services column filter (see page 86) (▼) to filter data in the table.

   Priority

   Displays the priority setting of the service. The priority settings are Critical, High, Medium, Low, None, and Unspecified.

   Use the Priority column filter (see page 86) (▼) to filter data in the table.

   Current SLA

   Specifies if a service level agreement (SLA) is defined for the corresponding service. The column is blank if no SLA is defined. If an SLA is defined, the column displays one of the following icons:

   - Green check—The service is compliant for the current SLA period.
   - Red X—The service is not compliant; it has been violated for the current SLA period.
   - Red circle with a slash—The SLA is inactive.

   Use the Current SLA column filter (see page 86) (▼) to filter data in the table.

   Health

   Displays the health rating of the service. Each icon represents the health metric as follows:

   - If the service is in the Production Operational Mode, the color-coded health settings are Down (burgundy), Critical (red), Major (orange), Minor (yellow), and Normal (green).

- If the service is in Maintenance Operational Mode, the health rating can be one of the production modes (Down, Critical, Major, Minor, or Normal) or Unknown.
- If the service is in Testing Operational Mode, the health rating is set to Unknown.

Use the Services column filter (see page 86) (▽) to filter data in the table.

Quality

Displays the quality rating of the service. The color-coded quality settings are Down (burgundy), Severely Degraded (red), Moderately Degraded (orange), Slightly Degraded (yellow), and Operational (green).

Use the Quality column filter (see page 86) (▽) to filter data in the table.

Risk

Displays the risk that is associated with the service. The color-coded risk settings are Down (burgundy), Severe (red), Moderate (orange), Slight (yellow), and None (green).

Use the Risk column filter (see page 86) (▽) to filter data in the table.

Availability [24 hours]

Displays the availability of the service, which is expressed as a percentage that is calculated over the past 24 hours.

Note: An asterisk (*) next to an Availability value indicates that the value does not represent a complete set of data, which is a full 24 hour period.

Use the Availability [24 hours] column filter (see page 86) (▽) to filter data in the table.

Operational Mode

Displays the mode of the service. The modes are Testing, Maintenance, and Production.

Use the Operational Mode column filter (see page 86) (▽) to filter data in the table.

Launch To

Contains an Action button and drop-down menu that allow you to open the Operations Console or the corresponding domain manager application for the associated service.

Use the Launch To column filter (see page 86) (▽) to filter the data in the table.

2. (Optional) Click the column heading to switch the sort order between ascending and descending for that column. Ctrl + click to select multiple columns.

3. (Optional) Rearrange the display order of the columns by dragging and dropping appropriate columns. For example, if you want the Priority column to appear before the Services column, you can drag-and-drop the Priority column before the Services column.

   Note: If you rearrange the column order, CA SOI does not save the order. To change the column order permanently, see Customize the Services Table (see page 96).

4. (Optional) Enter a search string in the Find field. If a service name contains the entered string, the string is underlined in the Services column. However, CA SOI does not remove any entries. Click the arrows (< and >) to move among underlined services.

   The sections that follow provide information about the Details panel and the Quality, Risk, Availability, Alerts, and SLA tabs. These tabs show various charts for the selected service. You can resize these charts as necessary.

5. (Optional) Double-click a service row to display the associated service detail charts in carousel mode.

Column Filters

Each column in the Services table includes a filter icon (▽) that lets you find and display specific information. Applied filters have a red icon (🔻) to distinguish between columns with applied and unapplied filters. You can perform the following actions with filters:

- Click an unapplied filter icon (▽). Depending on the column, you enter a Search term, adjust a slider, or select check boxes to filter the data.
- Further refine the information by applying filters to multiple columns.
- Prioritize the filter order by Ctrl + left-clicking columns. A number appears in each column to show the filter priority. For example, you can first apply a filter to the Service column and can then enter the Search term "Alpha." You apply a second filter to the Health column and clear all check boxes except the burgundy icon (which indicates a Health state of Down) red icon (Critical). These multiple filters result in the Dashboard displaying only those services that contain the string "Alpha" *and* that have a Down or Critical Health status.
- Switch between ascending (▲) and descending (▼) order by left-clicking a column.
- Clear a filter by clicking an applied filter icon (🔻) and clearing any search fields or selecting all checkboxes.

Note: Sorting changes are not permanent; however, you can save filters. For more information, see Customize the Services Table (see page 96).

View Risk Details

The Risk tab in the Service History portlet displays the risk summary as a pie chart and an area chart for the selected service.

Follow these steps:

1. Select a service entry in the Services portlet.

   The service details appear in the Service History portlet.

2. Click the Risk tab.

   Note the following items in the Risk pie and area charts:

   - The area chart shows Risk as a percentage, with the higher number representing a higher risk of the associated service being unavailable.
   - The pie chart shows color-coded sections that correspond with the number of hours or days the risk is unchanged.
   - The pie chart shows the following periods:
     - The number of hours equaling 24 when the Last 24 Hours option is selected.
     - The number of days equaling 30 when Last 30 Days option is selected.
     - The number of hours equaling 168 when the Last 7 Days option is selected. The conversion of days to hours allows information to be displayed with greater detail and avoids the need to display fractions of days.
   - The pie chart shows the time that the service was in Maintenance mode.
   - The pie chart displays Unknown if the data is not available for the entire selected time period. For example, if you select Last 30 Days and you have only 20 days of data, the Unknown section is displayed with a label showing 10.00.

View Quality Details

The Quality tab in the Service History portlet displays the quality summary as a pie chart and an area chart for the selected service.

Follow these steps:

1. Select a service entry in the Services table.

   The service details appear in the Service History portlet.

2. (Optional) Click the Quality tab.

Note the following items in the pie and area charts on this tab and the other tabs:

- The charts can take a short time to display.
- You can mouseover the sections of the pie chart or points on the area chart to display summary details for the selected day or hour.
- You can select the time period that displays from the drop-down list for each chart.
- If the Report server is configured, you can click the chart to open the reporting interface in the context of the selected service and time period.
- The charts are color-coded. The pie chart shows the following states: Down (burgundy), Severely Degraded (red), Moderately Degraded (orange), Slightly Degraded (yellow), and Operational (green). The area chart contains a legend that describes the color-coding.
- The summary shows the status for the last full hour or day depending on which time period is selected. For example, if you are using the Last 24 Hours mode, and mouseover 2 PM in the area chart, the summary shows the period from 1:30 PM until 2 PM.
- The area chart only displays the times when Quality, Risk, or Availability states are something other than Normal or None. That is, the area chart displays data in the following situations:
  - Quality is Minor, Major, Critical, Down, Maintenance, or Unknown.
  - Risk is Slight, Moderate, Severe, Down, Maintenance, or Unknown.
  - Availability is Down, Maintenance, or Unknown.
- The pie chart and the area chart treat Unknown time differently.

  For example, if you select Last 24 Hours, the pie chart shows a full 24 hours. If there are only 23 hours of data in the database, the pie chart classifies the 24th hour as Unknown as the data is not available. CA SOI does *not* obtain the Unknown state from the database.

The area chart does not infer data; the chart reflects only the state values, other than Normal, that are present in the database. If the service was in a normal state for all 23 hours, the area chart is empty. Additionally, if there is no data in the database with an actual state of Unknown, there is no Unknown time displayed in the chart. The same behavior occurs when Last 7 Days or Last 30 Days is selected.

- The area chart displays the data for a specific time period. For example, if the Quality data between 2 PM and 2:30 PM is Major 80% of the time, and from 2:30 PM-3 PM it is also Major 80% of the time, the area chart starts at 2:30 PM with 50% and ends at 3 PM with 80%.

  As another example, if the service is placed in Maintenance mode between 2AM and 4AM, the area chart for Maintenance data starts drawing the curve from 2 AM and goes up to 100% Maintenance at 2:30 AM. This is because the maintenance data between 3:30 AM and 4 AM is 100% and from 4 PM to 4:30 PM it is 0%. The area chart starts to curve down at 4 PM, and reads 0% at 4:30 PM. You can mouseover each data point to display the details.

View Availability Details

The Availability tab displays the availability summary as a pie chart and an area chart for the selected service.

Follow these steps:

1. Select a service entry in the Services table.
2. Click the Availability tab.

   Note the following items in the Availability pie and area charts:

   - The area chart shows Availability as either 100% (available) or 0% (not available).
   - The pie chart shows the actual state: Critical status and Down status indicate that the service is not available. The other states indicate that the service is available.
   - The pie chart shows the time that the service was in Maintenance mode.
   - The pie chart displays Unknown if the data is not available for the entire selected time period. For example, if you select Last 24 Hours and you have only 20 hours of data, the Unknown section is displayed with a label showing 4.00.

View Alert Details

The Alerts tab displays the service alerts and direct cause alerts that are associated with the selected service.

Follow these steps:

1. Select a service entry in the Services table.
2. Click the Alerts tab.

   The following types of alerts display:

   Service Alerts

   Displays the alert condition that CA SOI generates based on analysis of a service model that it is monitoring. Service alerts result when the condition of one or more configuration items combines to impact the overall quality or risk that is associated with the service. The policy that is defined for that service model determines how configuration item alert conditions impact other configuration items and the overall service.

   If a help desk ticket exists, the Last Alert timestamp and summary are hyperlinked to the ticket. If the help desk integration is not configured as described in Configure Help Desk Integration, the number of tickets is 0 (zero). Click the link to open the ticket in the corresponding help desk product.

   Direct Cause Alerts

   Displays the following information for the corresponding configuration item:

   - Alert category and icon. The valid categories are defined in USM, such as Activity, Application, Cloud, Database, Issue, Network, Relationship, Service, System, and Other.

     Note: The Other icon represents New categories.
   - Number of alerts for the category
   - Number of open alerts for the category and the number of associated help desk tickets
   - Last alert in the category (the timestamp and summary are hyperlinked to the corresponding help desk ticket, clicking it opens the ticket in the corresponding help desk product)

   Direct cause alerts are assigned an impact value that is calculated based on the fault condition seriousness and the CI importance to the services or subservices it supports. The categories in the list are sorted based on the severity of the open alerts (Critical comes before Major, Major before Minor).

View SLA Details

The SLA tab displays the current SLA status as a pie chart and the SLA History as a bar chart.

Follow these steps:

1. Select a service entry in the Services table.
2. Click the SLA tab.

   Note the following items in the SLA charts:

   - The charts display the following color-coded states: Up (green), Unplanned (red), Maintenance (brown), Unknown (gray).
   - Unplanned is the total of outage and violation time (it does not include maintenance time). Violation is the time after the threshold has been reached.
   - The pie chart pane also includes the following information:
     - **SLA Current Status**—Displays date and time that the SLA was last calculated.
     - **Type**—Displays the type and state of SLA. SLAs can be based on Availability, Health, Quality, or Risk.
     - **Threshold**—Displays the actual time (in minutes and seconds) or percentage of time that an SLA has been violated.
     - **Description**—Displays the description that was entered when the SLA was created in the Operations Console.
     - **Violation Time**—Displays the time that exceeds the threshold. For example, if the threshold is 300 seconds and outage time is 800 seconds, then the violation time is 500 seconds.
     - **Updated**—Displays the time that the chart was last updated. Midnight is represented as 00:00:00.
   - You can select Line Chart from the drop-down list to display the SLA History in a line chart instead of the default bar chart.
   - The bar chart can show a single SLA, but the line chart requires at least two SLA data points to draw the line.
   - You can mouseover the sections of the bar chart or data points on the line chart to display summary details for the corresponding day.
   - You can click any of the charts to generate an SLA History report for the selected service. Click the pie chart to generate a report for the last 24 hours. Click the bar or line chart to generate a report for the SLA time period.
   - The SLA charts display the date using the yyyy/mm/dd format, for example, 2009/05/08 is May 8th, 2009. The reports that are generated from the SLA charts use the mm/dd/yyyy format.

Display Service Detail Charts in Carousel Mode

As an administrator or an operator, you display service detail charts in carousel mode. Carousel mode is an interactive graphical display that allows you to rotate among available charts and generate reports.

Follow these steps:

1. Double-click a service row under any of the following headings: Current SLA, Quality, Risk, or Availability.

   The service detail charts for the selected service display in carousel mode.

2. Perform any of the following actions to rotate among charts:

   - Select a chart from the drop-down list above the chart carousel.
   - Double-click a chart.
   - Use the scroll bar below the chart carousel.

3. (Optional) Select the chart time period from the drop-down list above the chart carousel.
4. (Optional) If available, select a chart type (Bar or Line) from the chart drop-down list.
5. (Optional) Double-click a chart to generate the associated detail report.

   Note: The system administrator must configure the report server before users can launch the reports.

   The reports that are generated are the same as the reports you generate from InfoView. For report descriptions, see the report list (see page 131).

Run Reports from the Dashboard

As an administrator or an operator, you can generate BusinessObjects reports from the Dashboard.

Note: Before you can generate reports, the reporting functionality must be configured. For more information, contact your system administrator.

You can generate the following reports from the CA SOI Dashboard:

- SLA Current Status
- SLA History
- Quality Summary Status
- Quality Status
- Risk Summary Status

- Risk Status
- Availability Summary Status
- Availability Status

Note: You can also run various additional reports in BusinessObjects InfoView. For more information, see Using Reporting (see page 121) in the *User Guide* and online help.

Follow these steps:

1. Log in to the CA SOI interface, and click the Dashboard tab.
2. Select a service entry, on which you want to report, in the Services table.

   The Details of Selected Service pane for the selected service opens and displays the Quality tab.
3. (Optional) Click the Risk or Availability tab to generate a report of that type.
4. Perform one of the following actions:
   - To generate a Summary Status report for the current tab, select the time period on which to report (Last 24 Hours, Last 7 Days, Last 30 Days), then click the pie chart.
   - To generate a Status report for the tab you are on, click the data point in the area chart for the time period on which to report.

View Services with Google Earth

As an administrator or an operator, use Google Earth to view services that CA SOI monitors. Install Google Earth on the same computer as the browser you are using to view the CA SOI dashboard. If CA SOI does not detect a Google Earth installation, the dashboard provides a link to install Google Earth.

Note: The Google Earth link is not active by default. The system administrator sets user group access.

Follow these steps:

1. Click the Dashboard tab.

   The dashboard opens with a Google Earth link on the top right of the page. If Google Earth is installed on your system, the link is underlined; otherwise, the link is unavailable.

2. (Optional) Mouseover the dimmed Google Earth link.

   A pop-up displays the URL to install Google Earth.

3. (Optional) Install Google Earth if it is not already installed on your system.

   After Google Earth is installed, the Google Earth link appears as white and underlined after you refresh the user interface.

4. Click the Google Earth link.

   You are prompted to download a .kml file. The file enables communication between CA SOI and Google Earth.

5. Click Open.

6. Enter your user name and password, and click OK.

   Google Earth displays the following items:

   - CA Technologies logo
   - Temporary Places and CA SOI folders in the My Places pane
   - Color-coded push-pin icons (known as *placemarks* in Google Earth) on the globe for each CA SOI service
     - Green placemarks represent services with Normal health.
     - Yellow placemarks represent services with Minor health.
     - Orange placemarks represent services with Major health.
     - Red placemarks represent services with Critical health.

- Burgundy placemarks represent services with Down health.
- Gray placemarks represent services with Unknown health.

The placemarks appear on the globe at the coordinates at the location you entered.

7. Click the plus sign next to the CA SOI folder and then the Services folder.

   The Normal and Degraded folders appear and display the services in that state.

   Note: The contents of these folders are updated as appropriate when the state of a service changes.

8. Perform one of the following actions:

   - Click the service name link to display the service details.

     The configuration items that are associated with the service are listed under Resources, and the service location is listed below them.

   - Double-click the service name link to zoom to the most detailed view of the location available.

9. Select File, Exit.

   You are prompted to save the services listed in the Temporary Places folder to the My Places folder.

10. Click Save.

    The services are saved in the My Places folder and Google Earth closes. You can view the services and their details by opening Google Earth and navigating to the desired service.

Dashboard Customization

As an administrator, you can configure the dashboard to tailor its appearance and contents to fit your users' needs. You can customize how the dashboard data appears, limit the displayed data, and add custom information.

This section describes all dashboard customization that you can perform.

Change the Icon Shown on the Dashboard

You can replace the icon that is shown on the CA SOI Dashboard with a custom graphic. You replace the icons for selected user groups by setting a preference in the Operations Console. If necessary, you can assign different logos for each user group to support multi-tenancy or different groups within one organization.

Follow these steps:

1. Open the Operations Console, and click the Users tab in the left pane.
2. Click a user group and select View, Preferences.
3. Expand the following preferences from the list in the left pane: Web, Logo Icon File Name.
4. Copy your icon file to the following directory:

   SOI_HOME\SamUI\webapps\sam\ui\images
5. Enter the file name in the Logo Icon File Name field and click OK.

   The change takes effect the next time a user in the group logs in to the Dashboard.

Customize the Services Table

The Dashboard tab contains the Services table. The table displays information about the services CA SOI is managing. You can customize this table to display only the columns that contain the information important to you.

Note: CA SOI applies updated preferences when the Dashboard refreshes, which is every 30 seconds by default.

Follow these steps:

1. Click the Dashboard tab.

   The Services table displays up to five rows of services and up to eight columns (depending whether it is the default view or has already been customized). The Services column is always included in the table.
2. Click Preference.

   The Columns tab of the User Preference dialog opens with the currently included columns listed in the Show Columns field, and the unused columns listed in the Hide Columns field.
3. Click one or more columns you want to move to the opposite pane (use Shift+click or Ctrl+click for multiple selections).

4. Click the arrows to move the selected columns to the opposite pane.

   Notes:

   - The columns listed in the Hide Columns field are removed from the Services table. The corresponding tab is *not* removed from the Details of Selected Service panel when you save your changes.
   - When you move a column to the Show Columns field, it appears at the bottom of the list. The table displays the columns in the order that is determined by this list. The first column (top of the list) is the first (leftmost) column in the table. The last column in the list is the rightmost column in the table. You can select a column in the Show Columns list, then click the up or down arrows to change the column order.

5. For the Current SLA, Health, Quality, and Risk tabs, move any of the SLA states to the Hide (if value equals) column to prevent services in that state from appearing in the Services table.

6. Click the Other tab, and perform one of the following actions:

   a. Clear the check box next to any priority state to prevent services in that state from appearing in the Services table.

   b. Clear the check box next to any operation mode to prevent services in that mode from appearing in the Services table.

   c. Set the availability minimum and maximum (expressed as a percentage) to prevent services that do not fall within the specified range from appearing in the Services table.

7. Click the Tabs tab and click the arrows to show or hide specific details tabs.

8. Click Save.

   Note: Your changes are saved immediately, but are not reflected until the Dashboard refreshes, which is approximately every minute by default.

Add Custom Tabs to the Dashboard

You can configure CA SOI to display up to ten custom tabs on the Dashboard. Each custom tab displays a website that can be important for you to monitor. The following websites are examples:

- A website that an associated service produces and hosts.
- A website that provides you with information related to service management. For example, an Intranet site that informs you when the associated service is updated with new components.

The custom tabs appear at the top of the Dashboard to the right of the Administration tab.

Follow these steps:

1. Click the Dashboard tab and click Preference.
2. Click the Custom Links tab, enter the appropriate information in the following fields, and click Save:

   Show

   Specifies whether the corresponding custom tab is shown or hidden. You can clear the check box to hide the custom tab after it is created.

   Tab Title

   Specifies the text that appears on the custom tab.

   Web Address

   Specifies the URL of the website that is displayed on the custom tab. The transfer protocol (for example, http or https) is required. You can optionally enter {servicename} to include the service as part of the query to a third-party tool. For example, to pass the service name to www.anyurl.com, enter the following URL query:

   ```
   www.anyurl.com/?query={servicename}
   ```

   The custom tab appears next to the Administration tab and displays the corresponding website when clicked.

3. (Optional) Repeat Step 3 to add additional custom tabs.

Note: Only a regular CA EEM user can save new custom tabs. The 'samuser' can create new tabs but they are not saved in the preference setting.

Add Custom Links to the Dashboard

A custom link can launch any URL that provides more information about a service, such as an internet search on the service name or a URL for the source management application. You can add the custom launch-in-context links for all services to the Action drop-down menu on the Dashboard.

Follow these steps:

1. Open the SOI_HOME\SamUI\webapps\sam\WEB-INF\console\config\custom-menu-config.xml file in a text editor on the UI Server.
2. Create and uncomment a full menu item using the conventions described in the custom-menu-config.xml file, and follow the instructions in the file, paying close attention to the following attributes:

   item name

   Specifies the name to display in the Actions drop-down menu.

   URL

   Specifies the launch URL. You can use the value {0} as a substitution value for the service name in the URL.

   The Dashboard requires only these two attributes to enable the link, but they must exist in the context of a full menu item. The other attributes can be empty, but the link appears in the Launch menu of the Operations Console.

   For information about creating custom Operations Console menus and links, see Operations Console Menu Customization.
3. Save and close the file.
4. Restart the CA SAM User Interface service.

   The custom link appears in the Dashboard for all services when you click the Actions menu.

Customize the Details Pane

The Dashboard tab contains the Details pane, which provides detailed information about the service selected in the Services table. You can customize the pane to display only the tabs that contain the information important to you.

Follow these steps:

1. Click the Dashboard tab and click Preference.
2. Click the Tabs tab.
3. Click one or more tab names (use Shift+click or Ctrl+click for multiple selections) to move to the opposite column.

   The selected tab names are highlighted.
4. Click the arrows to move the selected tabs to the opposite field.
5. Click Save.

   Note: When you move a tab to the Show Tab field, it appears at the bottom of the list. However, unlike customizing the Services table, you cannot modify the order of the tabs.

Add Custom Metrics to the Dashboard

You can add custom metrics to the dashboard that appear as table columns on the Services pane or as line charts on the Details pane. CA SOI can retrieve custom metrics from Microsoft SQL Server and Sybase databases to add important service-related data that CA SOI does not monitor by default to the Dashboard.

Note: To retrieve metrics from another database type, use your own driver that works with those databases. CA Technologies supports only Microsoft SQL Server and Sybase database metrics.

Follow these steps: for custom table columns

1. Open the SOI_HOME\SamUI\webapps\sam\thinuiconf\custom_metric_definition.xml file in a text editor on the UI Server.

   This file contains detailed instructions and examples for adding custom dashboard metrics.

2. Create a custom metric table using the provided example, or find the METRIC_TABLE tag and uncomment the example entry in the section labeled '<!-- Put custom metric here'. For either method, populate the following attributes in the entry:

   MAPTODASHBOARDTABLENAME

   Retain the default MyServicesStatusTable value. This attribute must have this value for the metric to display.

   NAME

   Specifies the custom metric name. This name follows the Java class name convention, such as no spaces or special characters.

   COLUMNLABEL

   Specifies the column labels to display in the Services pane. The number of values in this attribute equal the number of values in the DATANAME attribute minus one.

   COLUMNALIGN

   Specifies the column alignment of each label. The alignments are not used. The number of values in this attribute equal the number of values in the COLUMNLABEL attribute.

   COLUMNDATATYPE

   Specifies the data type for each column. The number of values in this attribute equal the number of values in the COLUMNLABEL attribute. Use 'string' as the data type for normal text display, or select from one of the following icon styles: image_sla, image_health, image_quality, image_risk. See the dashboard for examples of these icon styles.

   COLUMNSORTABLE

   Specifies whether each column is sortable. Enter 'true' or 'false'.

   CONNECTION_URL

   Specifies the connection URL for the database that contains the metric information. The only supported driver is JTDS, which supports most major database vendors.

   USERNAME

   Specifies the user name for connecting to the database.

PASSWORD

Specifies the password for connecting to the database. Use the SOI_HOME\tomcat\bin\WSSamEncryptCmd.bat utility to generate an encrypted password for this file.

QUERY

Specifies the query for obtaining the metric information from the database. Note the following items:

- For best results, use a simple query. If a complex query is required, create a database view to mask the complex query and expose only the relevant metric data.
- Ensure that the service name is the first field in the query, because it is used as the key to map to data in the dashboard table.
- CA SOI does not verify the external connection, so ensure that the database is always available to avoid errors.

DATANAME

Specifies the column names in the SELECT query. These values map directly to the SELECT statement. If the column names in the query are mixed-case, use exact characters.

DATATYPE

Specifies the data type of the columns defined in the query.

REFRESH_RATE

Specifies the refresh rate to retrieve custom metric data in minutes. The refresh rate must be greater than 60 seconds. A high frequency rate affects UI Server performance.

3. Save and close the file.

4. Restart the CA SAM User Interface service.

   The metric appears as a table column in the Services pane. If you defined multiple metrics, you cannot control the relative order of the metrics.

Follow these steps: for custom line charts

1. Open the SOI_HOME\SamUI\webapps\sam\thinuiconf\custom_metric_definition.xml file in a text editor on the UI Server.

   This file contains detailed instructions and examples for adding custom dashboard metrics.

2. Create a custom metric chart using the provided example, or find the METRIC_CHART tag and uncomment the example entry in the section labeled '<!-- Put custom metric here'. For either method, populate the following attributes in the entry:

   NAME

   Specifies the name of the custom metric chart. The name must be unique, so prefix the chart name with 'CUSTOMMETRIC_'.

   TITLE

   Specifies the chart title that displays on the tab in the dashboard Details pane.

   XLABEL

   Specifies the label of the X-axis data on the chart.

   XDATATYPE

   Specifies the data type of the X-axis data on the chart. The current supported types are 'string' and specific time unit data types (hour, date, month, and year). For more information about these types, see the text in the configuration file.

   XDATATYPELOCALE

   Specifies the locale value of the datetime data that is retrieved from the database. This parameter only applies when the XDATATYPE value is a time-unit data type. The value should conform to the appropriate standard local type, such as EN_US. If this value is empty, the chart uses the locale of the UI Server system as the default.

   YLABEL

   Specifies the label of the Y-axis data on the chart. You can have up to six Y-axis labels.

   YDATATYPE

   Specifies the data type of the Y-axis data on the chart. Enter the same number of data types in the YLABEL attribute.

   YDISPLAYUNIT

   Specifies the display unit in the Y-axis chart.

CHART_REFRESH_RATE

Specifies how often the chart sends requests to update data in minutes.

CONNECTION_URL

Specifies the connection URL for the database that contains the metric information. The only supported driver is JTDS, which supports most major database vendors.

USERNAME

Specifies the user name for connecting to the database.

PASSWORD

Specifies the password for connecting to the database. Use the SOI_HOME\tomcat\bin\WSSamEncryptCmd.bat utility to generate an encrypted password for this file.

QUERY

Specifies the query for obtaining the metric information from the database. Note the following items:

- For best results, use a simple query. If a complex query is required, create a database view to mask the complex query and expose only the relevant metric data.
- Ensure that the number of values in XLABEL plus the number of values in YLABEL equals the number of columns in the query.
- CA SOI does not check the external connection, so ensure that the database is always available to avoid errors.

DATANAME

Specifies the column names in the SELECT query. These values should map directly to the SELECT statement. If the column names in the query are mixed-case, use exact characters.

DATATYPE

Specifies the data type of the columns defined in the query.

REFRESH_RATE

Specifies the refresh rate to retrieve custom metric data in minutes. The refresh rate must be greater than 60 seconds. A high frequency rate affects UI Server performance.

3. Save and close the file.
4. Restart the CA SAM User Interface service.

The metric appears as a separate tab in the Details pane that displays a line chart.

Configure the Dashboard Refresh Rate

Users with administrator rights can configure the dashboard refresh rate.

Follow these steps:

1. Navigate to the SOI_HOME\SamUI\webapps\sam\ui\ directory, and open the refresh.properties file in a text editor.
2. Locate the following line, and change the refresh rate:

   ```
   dashboard.refresh=30000
   ```

   The default refresh rate is 30000 milliseconds (30 seconds). Increasing the refresh rate may improve the user experience when using the dashboard.
3. Save and close the file.

   This new refresh rate is used the next time that a new browser is opened.

Configure the Level of Services the Dashboard Displays

Users with administrator rights can configure the number of service levels that the Dashboard displays. This is a system-wide configuration setting where all users see the same number of service levels.

Follow these steps:

1. Navigate to the SOI_HOME\SamUI\conf\thinuiconf directory and open the tables_definition.xml file in a text editor.
2. Locate the following line, and change the SERVICE_LEVEL="ALL" to SERVICE_LEVEL="*numeric_value*".

   ```
   <TABLE NAME="MyServicesStatusTable" TITLE="ServicesStatus"
   CONSOLELINKTEMPLATE="/sam/oneclick.jnlp?explorer="
   SSOREDIRECT="/sam/sso/redirect?reqURL=" SERVICE_LEVEL="ALL">
   ```

   For example, SERVICE_LEVEL="1" displays only top-level services, SERVICE_LEVEL="2" displays the first two levels of a service, and so on.
3. Save and close the file, and then restart the CA SOI User Interface service.

   The Dashboard displays the level of services that you configured.

Display CA SOI Dashboard in SharePoint

As an administrator or an operator, you can configure Microsoft SharePoint to display the CA SOI Dashboard. This procedure assumes SharePoint is installed and you have working knowledge of adding content to SharePoint. For more information about installation and working with SharePoint, see the SharePoint documentation.

Obtain the CA SOI URL to complete this procedure.

Follow these steps:

1. Open your browser to the SharePoint server.
2. Log in to SharePoint as an administrator.
3. Select the tab (site) where you want to add the Dashboard.
4. Click Site Actions near the top right of the page, then click Edit Page.
5. Click Add a Web Part.
6. Select the Page Viewer Web Part check box under All Web Parts, Miscellaneous.
7. Click Add.

   The Page Viewer Web Part appears at the top of the page.
8. Click Edit, then click Modify Shared Web Part.

   A dialog expands and provides fields for the new website; in this case, the CA SOI Dashboard.
9. Enter the URL link to CA SOI.
10. (Optional) If necessary, adjust the height and width to display the CA SOI Dashboard correctly.
11. Click OK, then click Exit Edit Mode.

    The CA SOI Dashboard displays in SharePoint.

Access the Dashboard on a Mobile Device

As an administrator or an operator, you can access a version of the Dashboard that is designed for mobile devices. On the Mobile Dashboard, you can view and perform a subset of actions available on the PC version of the Dashboard (see page 83) and the Operations Console.

Note: For a list of supported mobile devices, see the *Release Notes.*

Follow these steps:

1. Open a web browser and enter the following URL:

   `https://UI server:port/mobile`

   Note: You are automatically redirected to an https connection if you enter http. You can change this behavior in the mobile dashboard configuration file.

   UI server

   Defines the name of the system where the UI Server is installed.

   port

   Defines the port on which the specified server listens.

   Note: The default port is 7070 for a non-SSL connection, and 7403 for an SSL connection.

2. Enter your login credentials and tap Login.

   Note: Your login credentials are the same as your CA SOI credentials. The “samuser” administrator account cannot be used here.

Navigate the Mobile Dashboard

As an administrator or an operator, you can view Dashboard data on a mobile device.

The Mobile Dashboard provides three tabs at the top of the home page that provide access to services, alert queues, and customers.

Note: You can tap the navigation bar at the top of any page to see and navigate the path of the current page location. The icon to the left of the navigation bar indicates the path through which you came to your current location (through a Services page, an Alerts page, or a Customers page). A Home icon indicates that you are on a home page.

Tap a tab to access the following information:

Services (see page 108)

Displays the Services home page which contains a list of all services with status indicators that provide metrics overviews.

Note: By default, this page is automatically displayed when you first log in.

Alert Queues (see page 109)

Displays the Alert Queues home page which contains a list of the alert queues to which you have access.

Customers (see page 110)

Displays the Customers home page which contains a list of customers with status indicators that provide an overview of associated services for each customer.

View Services

The Services home page displays a list of your services and a status overview for each service.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. You can perform the following actions on this page:
   - Tap the plus sign (+) next to a service to show the parent and child services of that service. Tap All Services to return to the original list.
   - Tap a service or child service to display the Alerts (see page 112) for the selected item.
   - Tap the yellow panel containing the down arrow to change the metrics that are displayed, change the display order to ascending or descending, or set the page to Favorite services only.
   - Tap Alert Queues (see page 109) to display the available alert queues.
   - Tap Customers (see page 110) to display customers.

Manage Favorite Services

You can manage services using a Favorite Services list, so that you can quickly find the services that matter to you. After you define favorite services, you can configure the Services home page to display only your favorites.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Menu button in the upper-right corner.
3. Tap Favorite Services.

   Note: An active star ✪ indicates services on your Favorite Services list.
4. You can perform the following actions on this page to update the services on your favorites list:
   - Tap the gray box to the right of a service to add or remove it from your favorites.
   - Use the Service filter slide bar to switch the view from All to Favorite to display all services or favorites only, on this page.

     Note: The Favorite view is more effective for removing favorites from your Favorite Services list.

View Alert Queues

The Alert Queues home page displays the alert queues to which you have access. You can view the alerts in a selected alert queue by tapping it.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap Alert Queues.

   The number to the right of an alert queue name indicates the alert count in that queue. The count can include alerts that you do not have user access privileges to view. Therefore, the alert count can be higher than the actual alerts that display in the alert queue.
3. You can perform the following actions on this page:
   - Tap the Services (see page 108) tab to view services.
   - Tap the Customers (see page 110) tab to view customers.

- Tap the yellow panel containing the down arrow to change the sort order (by name or by alert number) or the sort direction (ascending or descending).
- Tap an alert queue to display the alerts in the alert queue, then tap an alert to display the available actions (see page 115) for the selected alert. These alerts include alerts affecting a service to which you have user access privileges and alerts that do not impact any services. If an alert affects a service that you do not have user access privileges to view, the alert does not appear in the list.

View Customers

The Customers home page displays the customers to which you have access. You can also view the overall health, risk, and quality of the services for the selected customers. By default, CA SOI orders customers by health in ascending order.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap Customers.

   The indicator to the right of a customer name displays, by default, the health for services that are associated with the customer.

3. You can perform the following actions on this page:
   - Tap a customer name to see the services it is associated with.
   - Tap the yellow panel containing the down arrow to open the configuration page. On the configuration page you can change the sort order (by health, risk, or quality) or the sort direction (ascending or descending).

     Note: When you change the sort order for health, risk, or quality, the indicator next to the customer changes to display the associated service status.

   - Tap the plus sign (+) next to any customer to see its subcustomers.
   - Tap the Services (see page 108) tab to view services.
   - Tap the Alert Queues (see page 109) tab to display the available alert queues.

View Service Metrics

The Metrics page displays the health, risk, availability, quality, and SLA (if defined) for the selected service.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.

3. Tap Metrics.
4. You can perform the following actions on this page:
   - Tap Details (see page 111) to display the USM properties for the service.
   - Tap Alerts (see page 112) to display active alerts for the service.
   - Tap Hierarchy (see page 112) to display the parent and child services of the service.

View Service USM Properties

The Details page displays the USM properties for the selected service.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap Details.
4. You can perform the following actions on this page:
   - Tap Metrics (see page 110) to display the health, quality, risk, and availability for the selected service.
   - Tap Alerts (see page 112) to display active alerts for the service.
   - Tap Hierarchy (see page 112) to display the parent and child services of the service.

     Note: If this service does not have any parent or child services, the Hierarchy tab does not appear.

View Service Hierarchy

You can view the parent and child services of a selected service.

Note: The hierarchy is for services only, so there are no CIs provided, only parent and child services. Also, if this service does not have any parent or child services, this page is not available and the Hierarchy tab does not appear.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap Hierarchy.
4. You can perform the following actions on this page:
   - Tap a parent or child service to select that service and display its parent and child services.
   - Tap Details (see page 111) to display the USM properties for the service.
   - Tap Alerts (see page 112) to display active alerts for the service.
   - Tap Metrics (see page 110) to display the health, quality, risk, and availability for the selected service.

View Service Alerts

The Alerts page displays active alerts for the selected service. You can also access alerts by viewing an alert queue (see page 109).

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.

   Each alert displays a colored icon that indicates the severity (see page 19) of the alert. If an alert displays a blue check mark, the alert is acknowledged.

   Direct Alerts

   Lists the alerts that are raised on the service itself.

   Affecting Alerts

   Lists the alerts that are raised on the CIs and child services in the service.

3. You can perform the following actions on this page:
   - Tap Metrics (see page 110) to display the health, quality, risk, and availability for the selected service.
   - Tap Details (see page 113) to display the USM properties for the service.
   - Tap Hierarchy (see page 112) to display the parent and child services of the service.

     Note: If this service does not have any parent or child services, the Hierarchy tab does not appear.
   - Tap an alert to see the alert details and to take action (see page 115).

View Alert USM Properties

The Alert USM Properties page displays the USM properties for the selected alert.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.
4. Tap Details.
5. You can perform the following actions on this page:
   - Tap Actions (see page 115) to perform available actions on the alert.
   - Tap Affected CIs (see page 113) to display the CIs that the alert impacts.

View CIs Affected by an Alert

You can display the CIs affected by a selected alert.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.

4. Tap Affected CIs.
5. You can perform the following actions on this page:
   - Tap Details (see page 113) to display the USM properties for the selected alert.
   - Tap Actions (see page 115) to perform available actions on the alert.
   - Tap a service to display the Alerts page (see page 112) for the selected service.
   - Tap a CI to display the USM properties for the CI (see page 114).

View CI USM Properties

You can view the USM properties for a selected CI.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.
4. Tap Affected CIs.
5. Tap a CI.
6. You can perform the following actions on this page:
   - Tap Alerts (see page 112) to display alerts impacting the CI.
   - Tap Hierarchy (see page 115) to display the CI hierarchy.

View CI Hierarchy

You can view the parent-child relationship between CIs and services for a selected CI.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.
4. Tap Affected CIs.
5. Tap a CI.

6. Tap Hierarchy.
7. You can perform the following actions on this page:
   - Tap Alerts (see page 112) to display alerts impacting the CI.
   - Tap Details (see page 114) to view the CI USM properties.
   - Tap a service to display the metrics (see page 110) for that service.

View CI Alerts

You can view the alerts impacting a CI.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.
4. Tap Affected CIs.
5. Tap a CI.
6. Tap Alerts.
7. You can perform the following actions on this page:
   - Tap Details (see page 114) to view the CI USM properties.
   - Tap Hierarchy (see page 115) to display the CI hierarchy.
   - Tap an alert to see the Actions page (see page 115) for the alert.

Perform Actions on Alerts on the Mobile Dashboard

As an administrator or an operator (with access privileges), you can perform actions on alerts. You can also access the Actions page from alert queues (see page 109).

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.

4. You can perform the following actions on this page:

   - Tap E-mail to email alert information (see page 116).
   - Tap Acknowledge Alert or Unacknowledge Alert to acknowledge/unacknowledge an alert (see page 118).
   - Tap Exempt Alert or Unexempt Alert to exempt/unexempt an alert (see page 118).
   - Tap Clear Alert to clear an alert (see page 119).

     Note: The Exempt, Unexempt, and Clear actions can be used only with infrastructure alerts.

   - Tap any other escalation action that is listed to perform it. For more information about creating escalation actions, see the *Event and Alert Management Best Practices Guide.*
   - Tap Details (see page 113) to display the USM properties for the selected alert.
   - Tap Affected CIs (see page 113) to display the CIs that the alert impacts.

Email Alerts

You can send an email from your mobile device that details the alert conditions and provides a link to the alert on the Mobile Dashboard.

Note: For this feature to work, an SMTP server needs to be configured in the Administration, E-mail Configuration section of the CA SOI Dashboard.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.
4. Tap Email.

   The Notification Methods dialog opens with an automatically populated message containing the alert details. The subject of this message is the alert label.

5. Modify the subject and message if necessary, then enter an email recipient, then tap Send.

   CA SOI sends the email.

Escalate Alerts

You can send an escalation action for a selected alert. Only escalation actions defined in the Operations Console appear on the list.

Note: This feature is available only if you have appropriate access privileges. For more information, contact your CA SOI administrator.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.
4. Tap an escalation action.

   The escalation action is performed and a message appears indicating the action was performed successfully. If the action opened a ticket, then a request number appears also.

View Alert Root Cause

A *root cause alert* is an alert that CA SOI determines after analyzing the alerts associated with a service which is based on one of the following criteria:

1. A triggered root cause rule determining the alert that is the true root cause of the service degradation which is based on relationships and topology.
2. The alert with the highest impact if no root cause rules have been triggered.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.

   Note: Root cause links are provided for service alerts only.

4. Tap Go to root cause.

   The Actions page (see page 115) opens for the selected root cause alert.

Acknowledge or Unacknowledge Alerts

You can acknowledge or unacknowledge alerts to let other users know that you are acting on the alert. When a user acknowledges an alert, a blue check icon displays next to the alert to let other users know it is acknowledged. To acknowledge or unacknowledge an alert, use the following feature.

Note: This feature is available only if you have appropriate access privileges. For more information, contact your CA SOI administrator.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.
4. Tap Acknowledge Alert or Unacknowledge Alert.

   A confirmation dialog opens.
5. Tap Yes.

   The alert is acknowledged or unacknowledged.

Exempt Alerts on a Mobile Device

You can exempt or unexempt alerts on the Mobile Dashboard.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.
4. Tap Exempt Alert or Unexempt Alert and confirm the operation.

Clear Alerts

You clear an alert when you resolve the situation that caused the creation of the alert. You can only clear infrastructure alerts, not service alerts.

Note: This feature is available only if you have appropriate access privileges. For more information, contact your CA SOI administrator.

Note: Service alerts imported from the CA SOI Domain connector are treated similarly to alerts imported from any domain manager, and therefore can be cleared.

Follow these steps:

1. Access the Mobile Dashboard (see page 107).
2. Tap the Status Indicator to the right of a given service.
3. Tap an alert.
4. Tap Clear Alert.

   A confirmation dialog opens.
5. Tap Yes.

   The alert is cleared.

Chapter 6: Using Reporting

This section provides the process and procedures for viewing and managing InfoView reports.

This section contains the following topics:

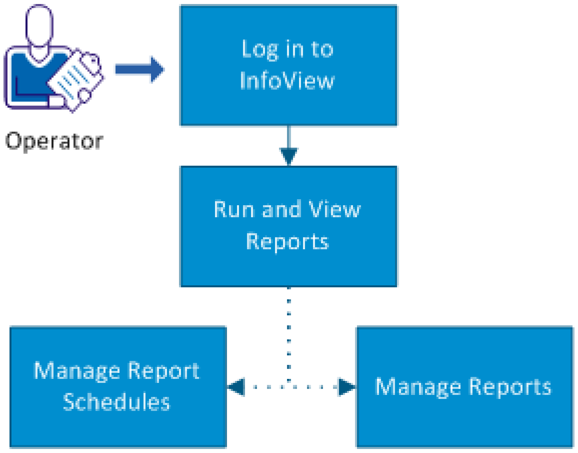
How to View and Manage Reports

As an operator, you can schedule and run predefined reports using InfoView. You use these reports to view metrics and service details over specified time ranges. The reporting features available to you depend on the access privileges your administrator sets.

In addition to the reporting features included in this documentation, you can access the online help from InfoView.

Use the following scenario to guide you through the process:

How to View and Manage Reports



Follow these steps to run and manage reports:

1. Log in to InfoView (see page 122).
2. Run and view the reports (see page 122).
3. (Optional) Manage the report schedules (see page 137).
4. (Optional) Manage the reports (see page 142).

Log In to InfoView

You must log in to InfoView to access reporting functionality.

Follow these steps:

1. Click the Reports link in the top right corner of the CA SOI interface.

   Notes:

   - If the Reports link does not appear next to the Console and Help links, the reporting functionality is not configured. Contact your CA SOI administrator or perform the procedure described in Configure Reports if you have the required user permission.
   - If the BusinessObjects InfoView home page appears without requiring you to log in, then you can skip the rest of this procedure.

2. Enter a valid user name and password and then click Log In.

   Note: If you do not know your user name and password, contact your CA SOI administrator.

Run and View Reports

The topics in this section provide procedures to run reports, view the latest instance of reports, view a report history, and manage report schedules.

Run a Predefined Report on Demand

You can use the tree in the left pane of the InfoView window to access the predefined reports installed by the CA SOI installation program. After you display a report, you can view the last instance, schedule, or run the report. Detailed explanations of the reports available (in alphabetical order) are provided in the topics that follow.

Follow these steps:

1. Click Document List.
2. Click the plus sign (+) next to the following tree nodes in the Folders pane: All, Public Folders, then CA Reports.

3. Click the CA Service Operations Insight folder.

   The following folders and reports display in the right pane:

   Note: Detailed descriptions of these reports are provided in the topics that follow.

   Alert Management

   Provides reports with details related to alert response and closure, ticketed alerts, and the top ten alert sources.

   Alert Response and Closure **(see page 126)**

   Shows the average of alert, acknowledgement, assignment, and closure time for a selected time period. The chart shows the average time for each operation in minutes. The table lets you open detailed reports for each operation.

   Ticketed Alerts **(see page 133)**

   Shows the alerts with associated tickets for a selected time period. The chart shows the total number of tickets opened daily. The table displays ticketed alert details and lets you view the associated ticket.

   Top Ten Alert Sources **(see page 134)**

   Shows the ten connector sources that generated the most alerts for a selected time period. The chart displays the alert count for each source. The table lets you open detailed reports for each source.

   Detail Reports

   Provides reports with details related to availability, health, quality, and risk. Detailed explanations of these reports are provided in the topics that follow.

   Service Availability **(see page 127)**

   Shows the availability for selected services for a selected time period. The chart shows the total time broken into the different states (defined by CA SOI). The table displays the duration and state of individual time segments included in the report time period.

   Service Health **(see page 128)**

   Shows the health for selected services for a specified time period. The chart shows the total time broken into the different states (defined by CA SOI). The table displays the duration and state of individual time segments included in the report time period.

   Service Quality **(see page 129)**

   Shows the quality for selected services for a selected time period. The chart shows the total time broken into the different states (defined by CA SOI). The table displays the duration and state of individual time segments included in the report time period.

Service Risk (see page 130)

Shows the risk for selected services for a selected time period. The chart shows the total time broken into the different states (defined by CA SOI). The table displays the duration and state of individual time segments included in the report time period.

Top Ten Reports

Provides reports with the highest down time, highest risk, lowest quality, and degrading CIs:

Top Ten High Risk Services (see page 134)

Displays the ten services with the most risk time.

Top Ten Low Quality Services (see page 135)

Displays the ten services with the most low quality time.

Top Ten Problematic Services (see page 135)

Displays the ten services with the most down time.

Top Ten Service Degrading CIs (see page 136)

Displays the ten configuration items (CIs) with the most service down time.

Service SLA Summary (see page 131)

Shows a summary of service SLA compliance for a selected time period. It also contains details about overall SLA outage and outage periods, specific outage periods, and root cause alerts.

Service Summary (see page 132)

Shows a summary of service health and lists outages for a selected time period. This report is also embedded as a sub-report per service in the Top Ten reports related to health.

Top Ten Service Degrading CIs (see page 136)

Displays the ten configuration items (CIs) with the most service down time. This report is also available in the Top Ten Reports folder described later in this procedure.

4. Double-click the name of the report you want to view.

   Note: The report prompt page can take several seconds to generate.

5. Enter information in the following fields as appropriate and click Run Report:

   Important! If you see other parameters or panes in the prompt page, then your administrator has not enabled the CA SOI custom prompt pages. Contact your administrator.

   Edit Report Title

   Enter the report title in the Report Title field. You can accept, replace, or append the default title.

   Select Services

   (Not available for all reports) Select the services to include in the report, and move them to the Selected Services list. Alternatively, select the All check box to include all services in the report. Select SLAs to include when generating the Service SLA Summary report. This pane only appears for reports that require you to specify services or SLAs to include. You can Shift + Click to select a range of services or Ctrl + Click to select individual services.

   Select Trend Line

   (Not available for all reports) Select Yes to display the average trend line when generating the selected report. The trend line is a two-period data trend that requires at least three data points to plot the trend line.

   Consider the following:

   - The All check box is selected by default. Clear the check box before selecting individual services.
   - For the Service Summary report (see page 132) only, do not select more than approximately 20 services as they are combined into one summary bar chart and the chart becomes unreadable.

   Select Date Range

   Configure the date range using the following drop-down lists:

   Select Range By

   Specifies the type of time period on which to report. Select Pre-Defined Time Period and select a time period to use, select Last and select a number of days or hours, or select Specific Date Range and enter a specific start and end date.

   Previous Day

   Displays selected services completed in the full 24 hours of the previous day from midnight to midnight.

   Previous Week

   Displays selected services completed in the previous full calendar week from midnight Sunday to midnight Saturday.

Today

Displays selected services completed from midnight this morning until now.

Week To Date (WTD)

Displays selected services completed from midnight Sunday until now.

Month To Date (MTD)

Displays selected services completed from midnight of the first day of the month until now.

Year To Date (YTD)

Displays selected services completed from midnight January 1 until now.

Time Zone

Specifies the time zone to use for the report.

The report generation begins. When it completes, the report opens.

6. (Optional) Click the following:

   - The Export this report icon to save the report to various formats.
   - The Export this report icon to save the report as a PDF.
   - The Parameters icon currently does not have a specified function.
   - Group Tree to display all services for which reports were generated so you can jump to a specific service rather than scroll through each report page.

Alert Response and Closure Report

The Alert Response and Closure report shows per customer the average of alert acknowledgment, assignment, and closure times (in minutes) for a selected time period.

Average Times to Acknowledge, Assign and Clear Alerts Chart

Indicates the average time (in minutes) for each operation by date.

Average Times to Acknowledge, Assign and Clear Alerts Table

Indicates the actual average time in minutes for each operation by date.

Average Time to Acknowledge

Indicates the average time to acknowledge alerts over a 24-hour period. Click the minutes to display the Alerts with the Longest Acknowledged Time report.

Average Time to Assign

Indicates the average time to assign alerts over a 24-hour period. Click the minutes to display the Alerts with the Longest Assigned Time report.

Average Time to Clear

Indicates the average time to clear alerts over a 24-hour period. Click the minutes to display the Alerts with the Longest Cleared Time report.

Service Availability Report

The Service Availability report provides the availability for selected services for a selected time period.

Availability Summary for Service

The pie chart represents 100% of the time period for the report and each wedge represents the percentage of time the service was in a particular availability state.

Up Time

Specifies the percentage of total time that the service was available.

Down Time

Specifies the percentage of total time that the service was experiencing an outage.

Unknown Time

Specifies the percentage of time that the service availability was unknown.

Maintenance

Specifies the percentage of time that the service was on down time for maintenance.

Availability Detail for Service

Provides the actual availability time and maintenance time for the specified services.

Availability

Specifies the availability state of either Up (available) or Down (unavailable due to maintenance or outage) and the health state (Normal, Minor, Major, Critical, or Down).

Operational Mode

Indicates either Production or scheduled Maintenance mode.

Start Time Adjusted

Specifies the start time adjusted to the beginning of the report, regardless of the actual start time of the operational mode.

Duration

Specifies the duration of the operational mode, which is one of the following:

- the length of time from Start Time Adjusted to the beginning of the next availability state
- the length of time from the Start Time Adjusted to the end of the report time period
- the length of the report if there is only one availability state

Details

Click the Details link to generate an outage detail report for the selected operational mode and time period.

Note: Not all availability states have a details link. Typically states of Normal do not have details; also, some states are the result of changes in child services and so the details are not directly linked.

Service Health Report

The Service Health report displays the health for selected services for a selected time period.

Health Summary for Service

The pie chart represents 100% of the time period for the report and each wedge represents the percentage of time the service was in a particular health state.

Health Detail for Service

The table displays the duration and state of individual state time segments included in the report time period.

Service Health

Specifies the health state: Normal, Minor, Major, Critical, or Down.

Operational Mode

Indicates either Production or scheduled Maintenance mode.

Start Time Adjusted

Specifies the start time adjusted to the beginning of the report, regardless of the actual start time of the operational mode.

Duration

Specifies the duration of the operational mode, which is one of the following:

- the length of time from Start Time Adjusted to the beginning of the next health state
- the length of time from the Start Time Adjusted to the end of the report time period
- the length of the report if there is only one health state

Details

Click the Details link to generate an outage detail report for the selected operational mode and time period.

Note: Not all health states have a details link. Typically states of Normal do not have details; also, some states are the result of changes in child services and so the details are not directly linked.

Service Quality Report

The Service Quality report displays the quality for selected services for a selected time period.

Quality Summary for Service

The pie chart represents 100% of the time period for the report and each wedge represents the percentage of time the service was in a particular quality state.

Quality Detail for Service

The table displays the duration and state of individual state time segments included in the report time period.

Service Quality

Specifies the quality state: Operational, Slightly Degraded, Moderately Degraded, Severely Degraded, or Down.

Operational Mode

Indicates either Production or scheduled Maintenance mode.

Start Time Adjusted

Specifies the start time adjusted to the beginning of the report, regardless of the actual start time of the operational mode.

Duration

Specifies the duration of the operational mode, which is one of the following:

- the length of time from Start Time Adjusted to the beginning of the next quality state
- the length of time from the Start Time Adjusted to the end of the report time period
- the length of the report if there is only one quality state

Details

Click the Details link to generate a detailed quality report for the selected operational mode and time period.

Note: Not all quality states have a details link. Typically states of Normal do not have details; also, some states are the result of changes in child services and so the details are not directly linked.

Service Risk Report

The Service Risk Report displays the risk for selected services for a selected time period.

Risk Summary for Service

The pie chart represents 100% of the time period for the report and each wedge represents the percentage of time the service was in a particular risk state.

Risk Detail for Service

The table displays the duration and state of individual state time segments included in the report time period.

Service Quality

Specifies the quality state: None, Slight, Moderate, Severe, or Down.

Operational Mode

Indicates either Production or scheduled Maintenance mode.

Start Time Adjusted

Specifies the start time adjusted to the beginning of the report, regardless of the actual start time of the operational mode.

Duration

Specifies the duration of the operational mode, which is one of the following:

- the length of time from Start Time Adjusted to the beginning of the next risk state
- the length of time from the Start Time Adjusted to the end of the report time period
- the length of the report if there is only one risk state

Details

Click the Details link to generate a detailed risk report for the selected operational mode and time period.

Note: Not all risk states have a details link. Typically states of None do not have details; also, some states are the result of changes in child services and so the details are not directly linked.

Service SLA Summary Report

The Service SLA Summary report displays a summary of selected services SLA compliance for a selected time period. It also contains details about overall SLA outage and outage periods, specific outage periods, and root cause alerts.

Each table in the report is a service and within each service table it is divided by SLA.

SLA Type

Specifies the SLA type: Availability, Health, Quality, or Risk.

Status

Indicates an SLA status of Compliant or Violated for the selected time period.

SLA Name

Indicates the defined SLA name.

Start Time

Specifies the start time based on the SLA schedule and adjusted by the time zone you selected on the report selection page (see page 122). CA SOI uses the start time of the SLA schedule that is closest to the starting time of the date and time range you selected for your report, so the report date, time range, and SLA schedule times may not exactly match with your selected report parameters.

End Time

Specifies the end time based on the SLA schedule and adjusted by the time zone you selected on the report selection page.

SLA Details

Click the Details link to generate a detail report for the selected SLA Type (Availability, Health, Quality or Risk) and time period.

Service Summary Report

The Service Summary report displays a summary for selected services' health and lists outages with customer information for a selected time period. This report is desirable for generating an overview for a group of services that you are interested in. This report is also embedded as a sub-report per service in the Top Ten reports related to health. Maintenance time is split from down time to avoid confusion between a scheduled maintenance outage and a problem outage.

Consider the following:

- If you select more than approximately 20 services the Service Summary bar chart may become unreadable as all service are combined into one chart.
- Service names are automatically truncated to 32 characters in length for display purposes.

Service Outage and Maintenance Summary

Displays a bar chart that shows the service outage by service as a percentage of total outage time in the time range selected. A red bar indicates down time and a brown bar indicates scheduled maintenance. The actual outage time is provided in the Service Outage and Maintenance Details table.

Service Outage and Maintenance Details

Provides the actual down and maintenance time for the specified services and time range.

Service Name

Displays the service for which down time and maintenance time are provided. Click the service name to generate a detailed Health report for the service, which is displayed in a new report tab.

Down Time

Provides the actual down time and the percent of the time.

Maintenance Time

Provides the actual scheduled maintenance time and the percent of the total time.

Ticketed Alerts Report

The Ticketed Alerts report displays, per customer, the alerts with associated tickets for a specified time period. The chart shows the total number of tickets opened daily. The table displays ticketed alert details and lets you view the associated ticket.

Total Number of Tickets Chart

Displays the total number of tickets by date that is based on the total number of alerts and the total number of alerts with opened tickets.

Ticketed Alert Detail Table

Provides information about each ticketed alert.

Logged Time

Indicates the date and time the alert was generated.

Alert Source

Indicates the domain manager containing the CI that triggered the alert.

Alert Message

Indicates the triggered alert message.

Alert Type

Indicates the type of alert: Risk or Quality.

CI Name

Indicates the CI that triggered the alert.

Category

Indicates the USM type of the CI.

Acknowledged

Indicates if the alert has been acknowledged.

Assigned To

Indicates the user or application the ticket is assigned to. If the field is empty, then the ticket has not been assigned.

Cleared Time

Indicates the date and time the alert was cleared. If the field is empty, then the alert has not been cleared.

Ticket ID

Indicates the ticket identification number. Click the ticket to open the ticket in CA Service Desk.

Top Ten Alert Sources Report

The Top Ten Alert Sources report displays the ten domain manager sources that generated the most alerts for a selected time period. The chart displays the alert count for each source. The table lets you open detailed reports for each source.

Alerts by Source Chart

Displays a pie chart which represents all alerts and each pie piece represents the number of alerts the source generated.

Top Ten Alert Sources Table

Displays the total alert counts by connector.

Sources

Indicates the connector name that has alerts.

Alerts Count

Displays the total alerts for the connector. Click the alert count to display a detailed alert count report for the connector. The report shows the alert count information by date and the alert details. Click Ticket ID to open the associated help desk application.

Top Ten High Risk Services Report

The Top Ten High Risk Services report displays a summary of the top ten highest risk services and lists outages per service for the selected time period. The risk time (down time) is all risk states greater than Moderate (see page 18).

Note: CIs that cause Availability Down Time for one or more services are included in this report. CIs that generate alerts which do not cause Availability Down Time are not included.

Top Ten High Risk Services Chart

Displays the top ten services with the greatest risk.

Top Ten High Risk Services Table

Provides the actual down time and maintenance time for the specified services.

Service Name

Displays the service name of a high risk service. Click the service name to generate a detailed Risk report for the service, which is displayed in a new report tab.

Down Time

Provides the actual down time and the percent of the total time.

Maintenance Time

Provides the actual scheduled maintenance time and the percent of the total time.

Top Ten Low Quality Services Report

The Top Ten Low Quality Services report displays a summary of the ten services with the most time in a low quality state.

Top Ten Low Quality Services Chart

Displays the ten services with the lowest quality.

Service Name

Displays the service for which quality is the lowest.

Percentage of Low Quality Time

Provides the percent of time that the quality was low.

Top Ten Low Quality Services Table

Displays the ten services with the lowest quality for a selected time period. Click the service name to generate a detailed Quality report for the service, which is displayed in a new report tab.

Low Quality Time

Provides the actual low quality time and the percent of the total time.

Maintenance Time

Provides the actual scheduled maintenance time and the percent of the total time.

Top Ten Problematic Services Report

The Top Ten Problematic Services Report displays a summary of the top ten services with the most overall down time.

Top Ten Impacted Services Chart

Displays the top ten services with the most downtime as a percentage of total time.

Top Ten Impacted Services Table

Provides the actual down time and maintenance time for the specified services as a percentage of the time period.

Service Name

Displays the service name for a problematic service. Click the service name to generate a detailed Health report for the service, which is displayed in a new report tab.

Down Time

Provides the actual down time and the percent of the total time.

Maintenance Time

Provides the actual scheduled maintenance time and the percent of the total time.

Top Ten Service Degrading CIs Report

The Top Ten Service Degrading CIs report displays a summary of the top ten CIs which cause service down time (outage and maintenance) for the selected time period.

Note: CIs that cause availability down time for one or more services are included in this report. CIs that generate alerts which do not cause availability down time are not included.

Top Ten Service Degrading CIs Chart

Displays the top ten CIs with greatest total service down time.

Note: The bar colors and gradations in this chart have no significance.

Top Ten Service Degrading CIs Table

Provides a list of the CIs with highest down time from longest down time to shortest.

CI Name

Provides the configuration item name.

Class Name

Provides the configuration item class, which is a service or a specific type of resource such as a CPU or application.

Total Service Downtime

Provides the combined total of all service downtime for that particular configuration item, which may exceed the actual time duration of the report.

View the Latest Instance of a Report

You can view the latest instance of a report to learn its status without rerunning it.

To view the latest instance of a report, right-click the report name and select View Latest Instance.

The latest instance of the report opens.

Consider the following situations:

- The report must have been scheduled (see page 138) and run successfully at least once for the View Latest Instance option to appear.
- Only the user that scheduled the report can use the View Latest Instance feature. If a different user clicks the View Latest Instance link, the default Report Prompt page opens.

View a Report History

You can view a scheduled report instance history to access the historical details of a report. Details include run time, format, status, and so on. You can use the details to determine whether you want to reschedule the report.

To view a history of report instances for a report, right-click the report name and select History.

The History page opens, displaying all previously run scheduled instances of the report.

Note: The History page does not show the history of reports that were run manually. The page shows only the history for reports that the scheduler ran.

Manage Report Schedules

The topics in this section provide procedures to create, view, and modify report schedules.

Schedule a Report

You can schedule a report to run one or more times at a specific time of the day, week, or month.

Note: The following procedure is for report servers running Tomcat. The procedure varies slightly for IIS report servers.

Follow these steps:

1. Right-click a report name and select Schedule.

   Note: You must have the appropriate authorization to schedule reports or the Schedule option is not displayed.

2. Enter a report title, and click Recurrence.

3. Select one of the following options from the Run Object drop-down list, and click Database Logon:

   Now

   Runs the report immediately when you click Schedule.

   Once

   Runs the report once on the specified date.

   Hourly

   Runs the report every specified number of hours and minutes within the specified start and end dates.

   Daily

   Runs the report every specified number of days within the specified start and end dates.

   Weekly

   Runs the report every week on the specified days within the specified start and end dates.

   Monthly

   Runs the report every specified number of months within the specified start and end dates.

   Nth Day of Month

   Runs the report on the specified day of every month within the specified start and end dates.

   1st Monday of Month

   Runs the report on the first Monday of every month within the specified start and end dates.

Last Day of Month

Runs the report on the last day of every month within the specified start and end dates.

X Day of Nth Week of the Month

Runs the report on a specified day of the specified week of every month within the specified start and end dates.

Calendar

Runs the report based on the selected calendar. Custom calendars can be created in the Central Management Console.

The Database Logon page appears.

4. Enter information in the following fields and click Parameters:

User

Specifies the user name to access the database.

Password

Specifies the password to access the database.

5. Enter information in the following panes, and click Save:

Important! If you see other parameters or panes in the prompt page, then your administrator has not enabled the CA SOI custom prompt pages. Contact your administrator.

Edit Report Title

Enter the report title in the Report Title field. You can accept, replace, or append the default title.

Select Services

Select the services to include in the report, and move them to the Selected Services list. Alternatively, select All to include all services in the report. Select SLAs to include when generating the Service SLA Summary report. This pane only appears for reports that require you to specify services or SLAs to include.

Note: If the selected object name contains an apostrophe, the report does not return any data unless it is selected by using the All option. Contact the owner or creator of the service, SLA, or other object to rename or recreate the object without an apostrophe if you want to report on it independent of the other objects.

Select Date Range

Configure the date range using the following drop-down lists:

Select Range By

Specifies the type of time period for the report. Select Pre-Defined Time Period and select a time period to use, select Last and select a number of days or hours, or select Specific Date Range and enter a specific start and end date.

Time Zone

Specifies the time zone to use for the report.

6. Skip the Filters page.

   Important! Do not change any settings on the Filters page.

7. Click Format.

8. Verify that Crystal Reports is selected in the Format Options drop-down list, and click Destination.

   Note: Using any other option can cause unexpected results.

9. Select one of the following from the Destination drop-down list and click Events:

   Default Enterprise Location

   Specifies that the report instance is saved in the default enterprise location.

   Note: For more information about defining the default enterprise location, see the Business Objects documentation.

   Business Objects Inbox

   Specifies that the report instance is saved in the Job Server's default location or the Inbox of the user or group you specify if you clear the Use Default Settings check box. Select Shortcut in the Send As section for this option to work.

   Email Recipients

   Sends the report instance to the user configured in the Job Server's default or the email address specified in the To field if you clear the Use Default Settings check box. You can also specify a subject line, a message body, and whether attachments are included.

   FTP Server

   Specifies that the report instance is saved in the Job Server's default location or the FTP server host specified in the Host field if you clear the Use Default Settings check box. Provide a port number and access credentials for the FTP server.

File System

Specifies that the report instance is saved in the Job Server's default location or the directory specified in the Directory field if you clear the Use Default Settings check box. Provide a user name and password to access the directory's host server.

10. Click Print Settings.
11. Select whether you want to print to PDF always or use the Crystal Reports settings (if you have Crystal Reports installed).
12. Leave the Print Crystal reports when scheduling check box clear unless you want the report to print automatically.
13. Select the page layout settings from the drop-down list and configure based on your selection.
14. Click Events.
15. Select one or more events from the Available Events box and click the arrow to move them to the Selected Events box. Custom events can be created in the Central Management Console.

    The selected events are displayed in the Events to wait for and Events to trigger on completion boxes.
16. Click Scheduling Server Group.
17. Specify a Server Group by selecting the appropriate option button. The default selection is the first available server.
18. Click Schedule.

View a Scheduled Report

You can view a scheduled report to learn report details such as the status, external destination, creation time, start and end time, and server used.

Follow these steps:

1. Right-click the report name and select History.
2. Click the link in the Status column for the appropriate report instance.

Modify a Report Schedule

You can modify a report schedule to change the following properties:

- Running time
- Destination
- Format

- Caching options
- Server group
- Events

You can either replace the existing schedule or create a schedule from the existing schedule.

Follow these steps:

1. Right-click a report and select History.
2. Select a report in the History Page then select Actions, Reschedule.
3. Change time, destination, format, caching options, server group, and events as necessary, and click Schedule.

Manage Reports

The topics in this section provide procedures for exporting, printing, and deleting reports and also procedures for managing report folders.

Export a Report

You can export a report to store its data in another program.

Follow these steps:

1. Run or click View Latest Instance for the report you want to export.

   The selected report opens.

2. Click the Export this report icon.
3. Select the export format from the File Format drop-down list, specify the page range to export, and click Export.
4. Click Save to rename the report file (all exported files are named CrystalReportViewer by default) and specify where you want to save it.

Print a Report

You can print a report to view or store it on paper.

Follow these steps:

1. Run or click View Latest Instance for the report you want to print.

   The selected report opens.

2. Click the Print this report 🖨 button.
3. Select a page range and click Export.

Delete a Report

You can delete a report when you no longer need it.

Note: You cannot delete the default reports provided with CA SOI.

Follow these steps:

1. Right-click the report and select Organize, Delete.
2. Click OK.

Add Reports to My Favorites

You can add your most useful reports to a folder in the favorites section to simplify locating and accessing them later.

Follow these steps:

1. Right-click a report and select Organize, Create Shortcut.
2. Right-click the My Favorites folder (or a child folder) and select Paste Shortcut.

   A shortcut is added to the selected report in the selected folder.

Chapter 7: Searching and Browsing USM Data with USM Web View on a PC

The topics in this section describe how to search and browse for USM data using USM Web View. You can access USM Web View through your PC or mobile device.

For browser support, see the *Release Notes*.

This section contains the following topics:

Access the USM Web View Starting Page on a PC

As an administrator or an operator, you can search or browse for USM data and create CIs by accessing the USM Web View Starting Page. You can access the Starting page from either the Dashboard or by entering the URL directly into your browser.

To access the Starting page from the Dashboard

On the Dashboard, click the USM Web View link.

Note: The user validation for USM Web View only verifies users defined in CA EEM. Therefore, the administrator defined during installation (samuser by default) is invalid.

To access the Starting page with a URL

1. Open a web browser and enter the following URL:

   ```
   http://UI server:port/ssaweb
   ```

   UI server

   Defines the name of the system where the UI Server is installed.

   port

   Defines the port on which the specified server listens.

   Note: The default port is 7070 for a non-SSL connection, and 7403 for an SSL connection.

2. Enter your login credentials and click OK.

   Note: The user validation for USM Web View only verifies users that are defined in CA EEM. Therefore, the administrator that was defined during installation (samuser by default) is invalid.

Perform a Search with USM Web View

As an administrator or an operator, you can perform a USM Web View search using a keyword.

Follow these steps:

1. Access the Starting page (see page 146).
2. Enter a search term in the Search field and click Search.

   Note: The search field provides an autocomplete feature, which suggests search terms as you type.

   The search results (see page 151) display.

Advanced Search Queries

The topics in this section provide advanced methods for creating search queries.

CA SOI uses Apache Lucene and Apache Solr as the search platform. The complete syntax information can be found on the following websites:

- Apache Lucene
- Solr Wiki

Special Characters

You can define special characters that should be part of your query by escaping the special characters with backslashes (\). The special characters include the following: \ : ? + - && || {} [] () ! ^ * "

For example, to search for the text "(A:M)", you enter the following query:

```
\(A\:M\)\
```

Wildcards

You can use the following wildcards to substitute for single or multiple characters in search queries:

?

Performs a substitution on a single character.

Example: A query of "d?g" returns "dog" and "dig."

*****

Performs a substitution on multiple characters.

Example: A query of "rain*" returns "rainbow" and "rains."

Fuzzy Searches

A *fuzzy search* returns items that are similar to your search term. You add a tilde (~) to the end of your search query to perform a fuzzy search. For example, if you entered "well~" the following items return: "sell" and "tell."

You can add a value between 0 through 1 to force the search to find less or more similar terms where a value of 0 is less similar and 1 is more similar. The default value is 0.5.

For example, the following query forces the search for more similar matches to "well":

```
well~0.9
```

Proximity

You can create a search to find words that are within a specified number of words of each other. The following search looks for the words "XP" and "Vista" within 15 words of each other:

```
"XP Vista"~15
```

Boolean Expressions

You can include the following Boolean expressions to refine your searches:

AND

Specifies that both terms must be found anywhere within the document.

Example: The following query searches for all ssa_type of person with a value of "John":

```
John AND ssa_type:Person
```

+

Specifies that the term must be found anywhere within the document.

Example: The following query returns all pages that contain "Microsoft Windows":

```
+"Microsoft Windows"
```

OR

Specifies that either term can be found anywhere in the document.

Example: The following query returns all pages that contain "DB2" or "Microsoft Windows":

```
DB2 OR "Microsoft Windows"
```

NOT or !

Specifies that the term must not appear in the document.

Example: The following query returns all pages that contain "DB2" but not "Microsoft Windows":

```
DB2 NOT "Microsoft Windows"
```

You could enter the query as follows:

```
DB2 ! "Microsoft Windows"
```

-

Specifies that the term must not appear in the document.

Example: The following query returns all pages that do not contain "Microsoft Windows":

```
-"Microsoft Windows"
```

Note: The operators must be in the upper case for the search queries to work.

Groups

You can group parts of the query in parentheses to create subqueries. Subqueries are evaluated before the rest of the query. Consider the following example:

```
(DB2 or Oracle) AND Windows
```

In this query, all pages are returned that contain either "DB2" or "Oracle" only if the document also contain Windows.

Consider another example:

```
(DB2 AND Oracle) OR (XP and Vista)
```

In this query, a page returns if *either* of the following conditions are met:

- The page contains the "DB2" and "Oracle."
- The page contains "XP" and "Vista."

You can also group fields when creating your search query. Consider the following example:

```
Description:(+Cisco -Microsoft)
```

This query returns all pages in which the Description field value contains "Cisco" but does not contain "Microsoft."

Browse the USM Data with USM Web View

As an administrator or an operator, you can browse the USM data in the following ways:

- By CI type
- By CI attribute

Browse by CI Type

You can browse for objects by USM type.

Follow these steps:

1. Access the Starting page (see page 146).
2. Click Browse by CI Type, located in the Browse section.

   The Browse by CI Type options display.

   Note: Icons appear for CI types that currently appear in the Persistent Store only.
3. (Optional) Select a specific data source from the drop-down list.
4. Click a CI type.

   The search results (see page 151) for the selected CI type display.

Browse by CI Attribute

You can browse for objects by a specific USM attribute.

Follow these steps:

1. Access the Starting page (see page 146).
2. Click Browse by CI Attribute, located in the Browse section.

   The available CI attributes display in an alphabetical format.
3. Click a CI attribute.

   The Browse Attribute page displays.
4. You can do any of the following:
   - Select a result from the top ten results, which display based on highest occurrence in the repository.
   - Enter an attribute search value in the field and click Search.

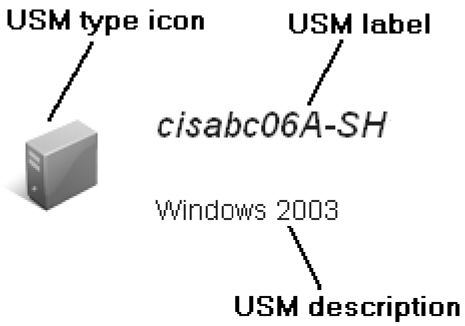
   The search results (see page 151) display.
5. (Optional) Click Start Again to return to the Starting page.
6. (Optional) Click Back to the list of attributes to return to the Browse by CI Attribute page.

Results and USM Properties

As an administrator or an operator, after you search (see page 146) or browse (see page 149) the database, you can view the search results and USM properties.

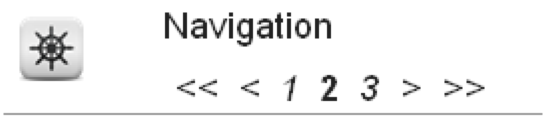
Work with Results in USM Web View

As an administrator or an operator, you can browse and search results in USM Web View. The results display as a list of object entries where each entry displays the USM type icon, label, and description as shown in the following graphic:



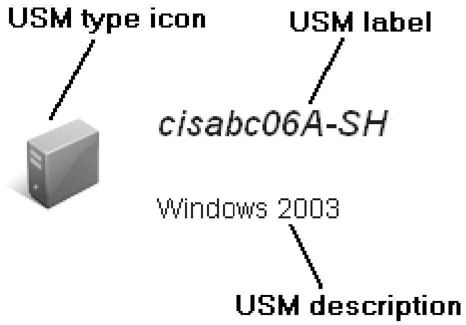
You can do the following on the results page:

- Click an object to display the USM properties (see page 153) for the selected object.
- Click More/Less Results per page to change the number of items displayed per page.
- Click More Options and do any of the following:
  - Select a data source (domain manager) and a CI type from the Narrow Search drop-down list to filter the results.
  - Click RSS feed 📶 to subscribe to the RSS feed (see page 159) for the current results.
  - Click Add/Remove to favorite views to add/remove the current search to your favorites (see page 158).
- Click the Navigation controls to page through the results. The following graphic shows typical navigation controls:



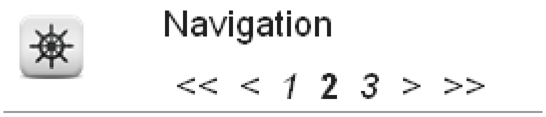
Work with Results in USM Web View

As an administrator or an operator, you can browse and search results in USM Web View. The results display as a list of object entries where each entry displays the USM type icon, label, and description as shown in the following graphic:



You can do the following on the results page:

- Click an object to display the USM properties (see page 153) for the selected object.
- Click More/Less Results per page to change the number of items displayed per page.
- Click More Options and do any of the following:
  - Select a data source (domain manager) and a CI type from the Narrow Search drop-down list to filter the results.
  - Click RSS feed 📶 to subscribe to the RSS feed (see page 159) for the current results.
  - Click Add/Remove to favorite views to add/remove the current search to your favorites (see page 158).
- Click the Navigation controls to page through the results. The following graphic shows typical navigation controls:



Work with USM Properties in USM Web View

As an administrator or an operator, you view the USM properties page. The page displays the USM properties for the selected CI, which can be a service, alert, relationship, and so on.

You can do the following in the Navigation section:

- Click Search again to return to the Starting page (see page 146).
- Click Relationships to jump to the Relationships section.
- Click Alerts to jump to the Alert section.
- Click Go back to return to the search results (see page 151).

You can do the following in the USM Properties section:

- Click Show/Hide Empty Properties to toggle USM properties that have no value entered.
- Click Override Properties to enter or override specific USM properties.

  Note: Overriding the USM properties creates the Update to Persistent Store (rest-api) data source for that CI.
- Click Delete relationship to delete a manually created relationship (see page 156).
- Click Delete entity to delete a manually created CI (see page 157).
- Click Delete manual overrides to delete any manually-entered USM properties (see page 158) using Override Properties.
- Click Correlate to manually correlate the CIs with another CI or recorrelate the CI.
- Click More options and do any of the following:
  - Select a data source from the drop-down list.
  - Click the search link to search for more items of the same type.
  - Click RSS feed to subscribe to the RSS feed (see page 159) for updates performed on the current CI.
- Click a property to display search results (see page 151) for all CIs with the same USM property value.

The Relationships section shows the relationship of the current USM object to other USM object. The data appears depends on the CI type (service, alert, relationship, and so on).

You can do the following in the Relationships section:

- Click Show/Hide Empty Relationships to toggle showing empty relationships.
- Click From this CI or To this CI to create a relationship (see page 154), which is creating an association between CIs.
- Click any relationship items to display its properties.

The Alerts section displays current alerts on all domain managers and on the currently displayed domain manager. The data that displays varies, depending on the CI type (service, alert, relationship, and so on).

You can do the following in the Alerts section:

- Click Show/Hide Empty alerts to toggle whether to display information if there is no alert.

You can view the USM XML content for the current USM object by clicking View USM XML content.

Create and Manage Relationships with USM Web View

As an administrator or an operator, you can create and delete CI relationships with USM Web View on your PC.

Create Relationships

You can create relationships to establish associations between CIs. When you create relationships, consider the following nonrecommended scenarios that the Web View does not prevent:

- Circular relationships are not supported. Circular relationships connect the same CIs in opposite directions. For example, if Service A manages Service B through a relationship, do not create another relationship between the services where Service B is required by Service A.
- Do not create multiple relationships between the same CIs that follow the same direction (with the same source and target).

Follow these steps:

1. Perform a search or browse (see page 149) for the CI that you want to be the source in the relationship.

   The USM Properties page opens for the CI you select.

2. Click From this CI or To this CI in the Relationships section to create the correct directional relationship.

   The Create New Relationship page displays.

3. Complete the following mandatory fields:

   Semantic

   Specifies the relationship type. Select one of the BinaryRelationship types defined in the USM schema.

   Source

   Defines the source CI in the relationship. This field is already populated with the CI you originally selected. You can change the source CI if necessary.

   Target

   Defines the target CI in the relationship. Click the field to open an embedded instance of the USM Web View Starting page from which you can find and select the target CI. Click the Select this link when you find the appropriate CI to populate the Target field.

   All required fields are defined.

4. Complete the remaining optional fields.

   Note: The remaining optional fields vary depending on the CI selected.

5. (Optional) Complete any of the optional fields as necessary. For more information, see the descriptions to the right of each field.

6. Click Submit Changes.

   The relationship is created between the CIs within the service defined in the scope field. If the CIs did not already exist in the service, they are added with the new relationship.

Note: Creating/modifying entities using the USM Web View creates/modifies CIs/relationships in the same way as they would be created by a separate connector, which shows up as the “Update of the Persistent Store” data source. The properties in these entities take priority over properties from other connectors in the reconciliation process, and therefore they “override” the values from other connectors.

Delete Relationships

You can delete a relationship that was manually created in USM Web View using Create relationship on the USM Properties page.

Follow these steps:

1. Search (see page 146) or browse (see page 149) to locate the relationship object.
2. View the USM properties (see page 153) for the relationship object.
3. Click More options.
4. Select Update of the Persistent Store(rest-api) from the By Data Source drop-down list.
5. Click Delete relationship.

   The relationship is deleted.

Manage CIs with USM Web View

As an administrator or an operator, you can create, delete, and correlate CIs with USM Web View on your PC.

Create CIs

You can manually create CIs on the Starting page.

Follow these steps:

1. Access the Starting page (see page 146).
2. Select the USM type from the drop-down list in the Create section.
3. Click Create.

   The CI creation page displays.
4. Complete the mandatory fields and the optional fields and click Submit Changes.

   The CI is created in the Persistent Store.

Delete CIs

You can delete CIs that were manually created in USM Web View using Create a new CI on the Starting page (see page 146).

Follow these steps:

1. Search (see page 146) or browse (see page 149) to locate the CI.
2. View the USM properties for the CI.
3. Click More options.
4. Select Update of the Persistent Store(rest-api) from the By Data Source drop-down list.
5. Click Delete entity.

   The CI is deleted.

Correlate CIs

Correlation is the act of comparing CIs to determine equivalencies—whether the CIs represent the same underlying entity. You can recorrelate objects or pick CIs and manually correlate them.

Note: You can only correlate CIs that are of the same type.

To correlate CIs

1. Search or browse (see page 149) objects and navigate to the USM Properties page (see page 153).
2. Click Correlate in the USM Properties section.
3. Click in the Correlate with field.

   An embedded instance of the Web View Starting page displays, from which you can find the CI to correlate.

4. Search or browse objects to find the correlation CI.
5. Click on the CI to view the details.
6. Click the Select this link when you find the appropriate CI to correlate.

   The Source Entity field populates with the selected CI.

7. Click Merge Selected Entities.

To recorrelate a CI

1. Search or browse (see page 149) objects and navigate to the USM Properties page (see page 153).
2. Click Correlate in the USM Properties section.
3. Click Re-correlate this entity.

   The correlation engine recorrelates the CI against all projection sheets in the Persistent Store.

Delete Manual Overrides with USM Web View

As an administrator or an operator, you can delete properties entered manually on the USM Properties (see page 153) page, which deletes the Update to Persistent Store(rest-api) data source that was created along with the custom properties.

Follow these steps:

1. Search (see page 146) or browse (see page 149) to locate the CI.
2. View the USM properties (see page 153) for the CI.
3. Click More options.
4. Select Update of the Persistent Store(rest-api) from the By Data Source drop-down list.
5. Click Delete manual overrides.

   The manual overrides are deleted.

Results and USM Properties

As an administrator or an operator, after you search (see page 146) or browse (see page 149) the database, you can view the search results and USM properties.

Favorite Views in USM Web View

As an administrator or an operator, you can save views to a favorite list that you can easily access from the Starting Page.

Create Favorite Views

After searching or browsing the USM data, you can save the results to a favorites list that appears on the Starting Page (see page 146).

Follow these steps:

1. Search or browse (see page 149) the USM data to generate a results list.
2. Click More options.
3. Click Add to favorite views.

Delete Favorite Views

You can remove a favorite view from either the Starting Page (see page 146) or from the view itself:

- To remove a favorite view from the Starting Page, mouse over a favorite link and click Remove view 🗑.
- To remove a favorite view from the view itself, click More options and click Remove from favorite views.

Subscribe to RSS Feeds in USM Web View Mobile

As an administrator or an operator, you can subscribe to RSS feeds using USM Web View on your mobile device.

Really Simple Syndication (RSS) feeds let you stay informed by having relevant and up-to-date information sent to you directly from the web sites in which you are interested. With RSS feeds, you do not need to keep checking back to a particular website to see if it has been updated. Simply subscribe to the RSS feed, much like you would subscribe to a magazine, but instead of being delivered to your physical mailbox each time the magazine is published, the information is delivered to you via an RSS feed every time your subscribed website is updated.

To subscribe and read RSS feeds you need an RSS feed reader. There are many different programs and plug-ins to view RSS feeds from such as Outlook, your internet browser (Internet Explorer, Firefox), web-based readers (My Yahoo!, Google Reader), desktop-based readers (Feed Demon), and cell phone readers. After you have subscribed to a feed, the RSS feed reader is able to check for new content at specified time intervals and retrieve the updates.

Your search and browse results allow you to subscribe to RSS feeds that allow you to monitor changes to CIs or queries by receiving the changes directly to an RSS reader.

Query feeds are based upon keyword, USM type, USM attribute, or CI relationship; the feeds update when a new item matches the query you subscribed to via RSS.

Consider the following issues:

- Internet Explorer 7 does not support authenticated RSS feeds.
- Internet Explorer 8 supports RSS authentication feeds; however, due to an apparent bug, password-protected feeds may not update correctly and no solution is available.
- Microsoft Outlook 2007 may have problems with certain RSS feeds. If you experience problems, refer to a possible solution at http://support.microsoft.com.

To subscribe to an RSS feed, do one of the following:

- On a PC browser click RSS.
- On a mobile device, click RSS .

The result is dependent on your user agent and operating system settings. You can choose to read feeds in your browser, feed reader, and so on. On some mobile platforms, notably the iPhone, you are redirected to a web-based feed reading service. By default, clicking the icon opens the appropriate feed in your browser. From there, you can subscribe to the feed in your browser or copy the URL into an external application such as a feed reader.

You can browse to a specific CI and click the RSS icon for that CI to subscribe to a feed that reports changes on that CI. Click the appropriate icon to subscribe for CI updates, alerts on the CI, or alerts on the associated service. For example, you could subscribe to a feed that updates every time an alert occurs on a specific service. You can also subscribe for updates on a search result if you run a search or browse by a specific CI type. For example, you could browse the alert type and subscribe to a feed that updates every time an alert occurs.

Chapter 8: Searching and Browsing USM Data with USM Web View on Mobile Device

The topics in this section describe how to search and browse for USM data using USM Web View. You can access USM Web View through your mobile device.

This section contains the following topics:

Access the USM Web View Mobile Starting Page

As an administrator or an operator, you can search or browse for USM data and create CIs.Access the USM Web View Starting Page on your mobile device.

Follow these steps:

1. Open a web browser and enter the following URL:

   `http://`*`UI server`*`:`*`port`*`/ssaweb/m`

   UI server

   Defines the name of the system where the UI Server is installed.

   port

   Defines the port on which the specified server listens.

   Note: The default port is 7070 for a non-SSL connection, and 7403 for an SSL connection.

2. Enter your login credentials and click OK.

   Note: The user validation for USM Web View only verifies users that are defined in CA EEM. Therefore, the administrator that was defined during installation (samuser by default) is invalid.

Perform a USM Web View Mobile Search

As an administrator or an operator, you perform a search using a keyword and optionally on a specific domain manager on your mobile device.

Follow these steps:

1. Access the Starting page (see page 161).
2. Enter a search term in the Search the IT repository field.

   Note: For information about creating advanced queries, see Advanced Search Queries (see page 147).
3. (Optional) Click Expand ▲ and select a domain manager from the drop-down list.
4. Click Start searching ➪ .

   The search results (see page 164) display.

Browse the USM Data with USM Web View Mobile

As an administrator or an operator, you can browse the USM data using USM Web View in the following ways on your mobile device:

- By type
- By attribute

Browse by CI Type

You can browse for objects by type.

Follow these steps:

1. Access the Starting page (see page 161).
2. Click Go ➡ to the right of Browse by CI Type.

3. Click Go ➡ to the right of the entity you want to browse.

   The available USM types display.

4. Click Go ➡ to the right of the USM type.

   The search results display (see page 151).

Browse by CI Attribute

You can browse for objects by attribute.

Follow these steps:

1. Access the Starting page (see page 161).

2. Click Go ➡ to the right of Browse by CI Attribute.

   The browse entities by attribute page displays.

3. Click Go ➡ to the right of an attribute.

   The Browse by CI Attribute page displays.

4. Click Go ➡ to the right of a USM attribute.

   The Browsing by page displays.

5. Enter a value for the selected attribute and click Submit ⇨.

   The search results display (see page 151).

Results and USM Properties in USM Web View Mobile

As an administrator or an operator, after you search (see page 162) or browse (see page 162) the database using USM Web View, you can view the search results and USM properties on your mobile device.

Work with Results

The browse and search results display as a list of object entries.

You can do the following on this page:

- Click RSS feed to subscribe to an RSS feed for the current search results. For more information, see Subscribe to RSS Feeds (see page 159).
- Click Go to the right of a CI to display the USM properties for the CI.
- Click Expand for Other Data Repositories to display available domain managers. Click Go to the right of a domain manager to repeat the current search for the selected domain manager.
- Click paging controls (if active) to navigate the results page. The USM properties page displays the USM properties for the selected USM object.

Work with USM Properties

The USM Properties page displays the USM properties for the USM object. You can perform searches related to the object's properties and manually created relationships with the object.

You can do the following in the banner and USM Properties section:

- Click the USM type icon to display all USM objects of that type in the current MDR.
- Click RSS feed to subscribe to an RSS feed. For more information, see Subscribe to RSS Feeds (see page 159).
- Click Override Properties to override the current attributes with values you enter.
- Click Go to the right of a USM property to display the USM property value and allow you to search for other CIs with the same property.

You can do the following in the Alerts on this MDR section:

- Click Go ➡ to the right of an alert under Alerts on All MDRs to display the alert's USM properties, alerted item, and alerted service.

You can do the following in the Edit actions section:

- Click Go ➡ to the right of Create new relationship to create a new USM relationship (see page 165).
- Click Go ➡ to the right of Delete relationship to delete the relationship (see page 167).
- Click Go ➡ to the right of Delete entity to delete the CI (see page 168).
- Click Go ➡ to the right of Delete manual overrides to delete any manually-entered USM properties (see page 169) using Override Properties.

Manage Relationships with USM Web View Mobile

As an administrator or an operator, you can create and delete CI relationships using USM Web View on your mobile device.

Create Relationships

You can create relationships to establish associations between CIs. When you create relationships, consider the following:

- Circular relationships are not supported.
- Do not create multiple relationships between the same CIs that follow the same direction (with the same source and target).

Follow these steps:

1. Perform a search (see page 162) or browse (see page 162) for the CI that you want to be the source in the relationship.

   The Properties page opens for the CI you select.

2. Click Go ➡ to the right of Create New Relationship.

3. Complete the following required fields:

   Note: The CI property fields vary depending on the entity type you select. To view information about a CI property, mouseover the question mark ? to the right of a CI property.

   Semantic

   Defines the relationship type. Select one of the BinaryRelationship types defined in the USM schema.

   Source

   Defines the source CI in the relationship. This field is already populated with the CI you originally selected. You can change the source CI if necessary.

   Target

   Defines the target CI in the relationship. Enter the hexadecimal string contained in the URL of the USM Properties page for the target CI.

4. (Optional) Complete any of the optional fields as necessary. To view information about a CI property, mouseover the question mark ? to the right of a CI property.

5. Click Submit changed values ✓.

   The relationship is created between the CIs within the service defined in the scope field. If the CIs did not already exist in the service, they are added with the new relationship.

Delete Relationships

You can delete a relationship that was manually created in USM Web View using Create relationship on the USM Properties page.

Follow these steps:

1. Search (see page 162) or browse (see page 162) to locate the relationship object.
2. View the USM properties (see page 164) for the relationship object.
3. Click Expand ▲ for Other Data Repositories to display data sources.
4. Click Go ➡ to the right of Update of the Persistent Store.
5. Click Go ➡ to the right of Delete relationship.

   The relationship is deleted.

Manage CIs with USM Web View Mobile

As an administrator or an operator, you can create and delete CIs with USM Web View on your mobile device.

Create CIs

You can manually create CIs on the Starting page.

Note: You cannot create CIs that correlate to existing CIs.

Follow these steps:

1. Access the Starting page (see page 146).
2. Click Go ➡ to the right of Create a new CI.

   The USM types display.

   Click Go ➡ to the right of a USM type.
3. Complete the fields.

   Consider the following:

   - The CI property fields vary depending on the entity type you select. To view information about a CI property, mouseover the question mark ? to the right of a CI property.
   - Fields marked with an asterisk (*) are for correlation. You must complete at least one of these fields.
4. Click the button to the right of Create entity.

Delete CIs

You can delete CIs that were manually created in USM Web View using Create a new CI on the Starting page (see page 146).

Follow these steps:

1. Search (see page 162) or browse (see page 162) to locate the CI.
2. View the USM properties (see page 164) for the CI.
3. Click Expand ▲ for Other Data Repositories to display data sources.
4. Click Go ➡ to the right of Update of the Persistent Store.
5. Click Go ➡ to the right of Delete entity.

Delete Manual Overrides with USM Web View Mobile

As an administrator or an operator, you can delete properties entered manually on the USM Properties page. This deletes the Update to Persistent Store(rest-api) data source that was created along with the custom properties.

Follow these steps:

1. Search (see page 162) or browse (see page 162) to locate the CI.
2. View the USM properties (see page 164) for the CI.
3. Click Expand ▲ for Other Data Repositories to display data sources.
4. Click Go ➡ to the right of Update of the Persistent Store.
5. Click Go ➡ to the right of Delete manual overrides.

Subscribe to RSS Feeds in USM Web View Mobile

As an administrator or an operator, you can subscribe to RSS feeds using USM Web View on your mobile device.

Really Simple Syndication (RSS) feeds let you stay informed by having relevant and up-to-date information sent to you directly from the web sites in which you are interested. With RSS feeds, you do not need to keep checking back to a particular website to see if it has been updated. Simply subscribe to the RSS feed, much like you would subscribe to a magazine, but instead of being delivered to your physical mailbox each time the magazine is published, the information is delivered to you via an RSS feed every time your subscribed website is updated.

To subscribe and read RSS feeds you need an RSS feed reader. There are many different programs and plug-ins to view RSS feeds from such as Outlook, your internet browser (Internet Explorer, Firefox), web-based readers (My Yahoo!, Google Reader), desktop-based readers (Feed Demon), and cell phone readers. After you have subscribed to a feed, the RSS feed reader is able to check for new content at specified time intervals and retrieve the updates.

Your search and browse results allow you to subscribe to RSS feeds that allow you to monitor changes to CIs or queries by receiving the changes directly to an RSS reader.

Query feeds are based upon keyword, USM type, USM attribute, or CI relationship; the feeds update when a new item matches the query you subscribed to via RSS.

Consider the following issues:

- Internet Explorer 7 does not support authenticated RSS feeds.
- Internet Explorer 8 supports RSS authentication feeds; however, due to an apparent bug, password-protected feeds may not update correctly and no solution is available.
- Microsoft Outlook 2007 may have problems with certain RSS feeds. If you experience problems, refer to a possible solution at http://support.microsoft.com.

To subscribe to an RSS feed, do one of the following:

- On a PC browser click RSS .
- On a mobile device, click RSS .

The result is dependent on your user agent and operating system settings. You can choose to read feeds in your browser, feed reader, and so on. On some mobile platforms, notably the iPhone, you are redirected to a web-based feed reading service. By default, clicking the icon opens the appropriate feed in your browser. From there, you can subscribe to the feed in your browser or copy the URL into an external application such as a feed reader.

You can browse to a specific CI and click the RSS icon for that CI to subscribe to a feed that reports changes on that CI. Click the appropriate icon to subscribe for CI updates, alerts on the CI, or alerts on the associated service. For example, you could subscribe to a feed that updates every time an alert occurs on a specific service. You can also subscribe for updates on a search result if you run a search or browse by a specific CI type. For example, you could browse the alert type and subscribe to a feed that updates every time an alert occurs.

Chapter 9: Troubleshooting

This section contains troubleshooting information for common problems categorized by CA SOI component.

This section contains the following topics:

Access - Unable to Start the Operations Console

Symptom:

When I try to open the Operations Console, the message "Unable to Launch Application" appears.

Solution:

Verify that you are using a Java version of 1.6.0_24 or above; if not, upgrade to a supported version. If the automatic installation does not work, manually download and install the latest JRE from the Java website and try to launch the Operations Console again.

If you are using a supported Java version, try clearing the JNLP cache.

Follow these steps:

1. Launch the Java Control Panel.
2. Click the View button in the Temporary Internet Files section.
3. Right-click the extra CA SOI applications in the list, and select Delete.

Access - Proxy Server Prompt Opens When Accessing the Operations Console

Symptom:

Every time I open the Operations Console, I must enter credentials in a proxy server prompt.

Solution:

You must configure your Java settings to use your browser settings or establish a direct connection when starting Java applications.

Follow these steps:

1. Launch the Java Control Panel.
2. Click Network Settings.
3. Select 'Use browser settings' or 'Direct connection', and click OK.
4. Click OK on the Java Control Panel.

Glossary

alert

An *alert* is a message on the Operations Console that reports a fault condition that is associated with a resource or service.

alert queue

Alert queues are user-defined alert groups. CA SOI auto-assigns alerts to a particular alert queue based on user-defined policy, which can include alert content and associated CIs.

availability

Availability is an abstracted measure of service uptime and downtime that is based on the health of the service.

configuration item (CI)

A *configuration item* (*CI*) is a managed resource such as a printer, software application, or database. Configuration items support services. A synonym for a configuration item is a *resource.*

Connector

A *connector* is software that provides the interface for the data exchange between the CA Catalyst infrastructure and a domain manager.

correlation

Correlation is the act of comparing CIs to determine equivalencies—whether the CIs represent the same underlying entity.

domain manager

A *domain manager* is a management application that provides information to CA Catalyst and CA SOI using a connector.

FIPS 140-2 (Federal Information Processing Standard)

FIPS 140-2 (Federal Information Processing Standard) describes US Federal government requirements that IT products should meet for sensitive but unclassified use.

health

Health is a reflection of the worst state that of either Quality or Risk. Health provides a high-level summary of the service health according to those metrics.

infrastructure alert

A domain manager reports an *infrastructure alert*, which is a fault condition on a CI in CA SOI.

JNLP

Java Network Launch Protocol

quality

Quality indicates the level of excellence that consumers of an IT service experience, whether the consumers are customers, end users, or other IT services. The levels of quality are Operational, Slightly Degraded, Moderately Degraded, Severely Degraded, Down, and Unknown. The highest propagated impact of an associated quality alert determines the service quality value.

resource

A *resource* is a managed resource such as a printer, software application, or database. Resources support services. A synonym for a resource is a configuration item (CI).

risk

Risk indicates the likelihood of delivering the quality of service that is required to support the overall business objectives. The highest propagated impact of an associated risk alert determines the service risk value.

root cause alert

A *root cause alert* is an alert that CA SOI determines after analyzing the alerts associated with a service which is based on one of the following criteria:

1. A triggered root cause rule determining the alert that is the true root cause of the service degradation which is based on relationships and topology.
2. The alert with the highest impact if no root cause rules have been triggered.

SA Manager

The *SA Manager* (also called SAM Application Server) is the primary management component in CA SOI. The SA Manager monitors the health and availability of managed resources and services. The SA Manager also processes events from connected applications and performs service impact and risk analysis.

service

A *service* typically consists of several CIs, which are grouped to represent entities like web server farms or clusters. Services can also contain *subservices*, which are subordinate service models. Service models typically represent high-level abstract entities like a web-based retail transaction service, an application server service, or a source control service. You can define any service type with CA SOI as long as one of the integrated domain managers monitors the service components.

service alert

A *service alert* is an alert condition that CA SOI generates based on analysis of a modeled service that it is monitoring.

service model

A *service model* is a definition of a service or other entity in your enterprise. It is a logical grouping of resources, associations, dependencies, and policies.

service-level agreement

A *service-level agreement* (SLA) is a contract that specifies the service expectations of internal or external customers. An example is the downtime that is acceptable for various resources.

severity

Severity indicates the condition of a CI as reported from the domain manager to CA SOI through alerts.

UI Server

The User Interface Server (*UI Server*) is the server that hosts the user interface applications.