CA Service Operations Insight

Administration 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: Operations Console Basics 79

Chapter 8: Monitoring Services from the Dashboard 161

Chapter 10: Searching and Browsing USM Data with USM Web View on Mobile Device 219

Chapter 11: Scheduling Maintenance for Services and Resources 229

Appendix A: Working with CA Catalyst Reconciliation 239

Appendix B: Working with CA Catalyst Synchronization 253

Appendix C: Understanding REST Web Services 277

Chapter 1: About This Guide

The *Administration Guide* contains information about administrative and end user tasks that you can perform after installing the product. This guide introduces the key concepts and represents a logical administrator workflow. This guide shows how to secure components based on user roles in the organization; an overview of service modeling and the associated escalation and notification policy; an overview of alert and event management; use CA SOI to support the incident resolution process in the data center; and communicate the real-time health and availability of services to the required end users in a format they best understand. The guide also contains advanced information about customizing interfaces and troubleshooting.

Note: The *Administration 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 administrators who are responsible for configuring and maintaining CA SOI. Most operations described in this guide require administrator-level permissions in the product. Some procedures, such as viewing reports and viewing alert metrics on the Dashboard, are intended for operators, which is a non-administrator role. The *User Guide* provides operator procedures.

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.

Related Publications

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

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.

Connector Guide

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

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.

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.

User Guide

Provides information for nonadministrative users about using the product, such as responding to alerts and viewing reports.

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.

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

***Product_Name* Connector Guide**

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

Example: CA Spectrum Connector Guide

***Product_Nam*e Connector Readme**

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

Chapter 2: Introducing CA SOI

This section introduces the concepts and components of CA SOI.

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 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

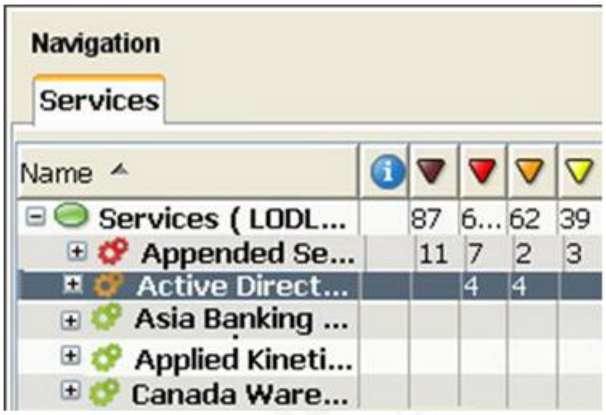
Severity indicates the condition of a CI as reported from the domain manager to CA SOI through alerts. If multiple domain managers send alerts for the same CI, the highest severity is used. CI severity helps determine the service impact by propagating the impact of the condition to related CIs in the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



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*.

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 (see page 107):** After installation, an administrator sets up security that defines the users and roles that will interact with the system.
2. **Define event policies (see page 145):** 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 (see page 148):** Establish the queues and policies that determine how operators visualize and manage alerts.
4. **Define the service (see page 131):** 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 (see page 117):** 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 153):** 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 79) and the Dashboard (see page 161).

10. **Report service details:** 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 in to CA SOI

Use a web browser to access the CA SOI Dashboard.

Follow these steps:

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

   ```
   http://UI server:port/sam/ui
   ```

   UI server

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

   port

   Specifies the port on which the UI Server listens.

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

   If you entered an SSL port, a security certificate dialog opens.

2. (Optional) Click Yes to accept the certificate for an SSL connection.

   The login screen opens.

3. Enter a valid user name and password.

   Note: You can use the default user name "samuser" that you defined during installation.

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

4. 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 the Monitoring Services from the Dashboard (see page 161).

   Administration tab

   Displays the Administration page, which lets you configure connectors and SA Manager settings.

   Note: For more information, see Configuring CA SOI (see page 41).

   Reports link

   Displays the BusinessObjects InfoView interface. You must configure reporting before the Reports link is available.

   Note: For more information, see Configure Reporting (see page 74).

Console link

Displays the Operations Console, where you can model services, monitor service status, and view and manage alerts. A Java application runs briefly when you start the Operations Console.

Google Earth link

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

Note: For more information, see View Services with Google Earth (see page 174).

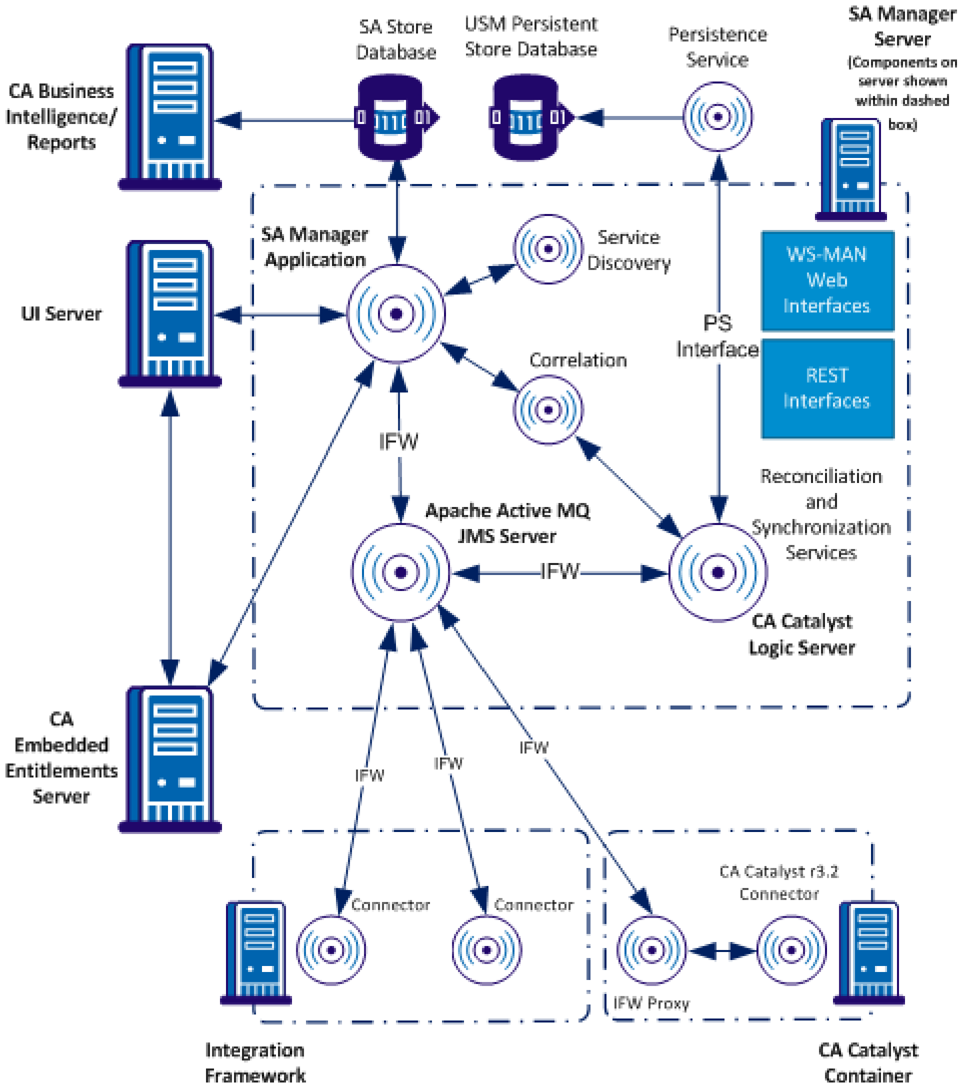
USM Web View link

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 203).

Product Architecture

The following graphic summarizes the product architecture:


SA Store Database
USM Persistent Store Database
Persistence Service
SA Manager Server (Components on server shown within dashed box)
CA Business Intelligence/ Reports
SA Manager Application
Service Discovery
UI Server
WS-MAN Web Interfaces
PS Interface
REST Interfaces
Correlation
IFW
Reconciliation and Synchronization Services
Apache Active MQ JMS Server
IFW
CA Catalyst Logic Server
CA Embedded Entitlements Server
IFW
IFW
IFW
CA Catalyst r3.2 Connector
Connector
Connector
IFW Proxy
Integration Framework
CA Catalyst Container

This section describes the key components in this diagram and their product function.

Integration Framework

The *integration framework (IFW)* is the mechanism that CA SOI uses to connect to domain managers and gather CI, service, topology, and state information. It exists on any system with a connector or the SA Manager, and it interfaces with the connector framework to prepare connector data for transmission to the manager components. The IFW contains a transformation engine that uses a connector policy to transform connector data to the USM format. The IFW also includes the infrastructure of the Event Management component. The component provides the mechanism for storing events from connectors for exposure to event policy and eventual display as alerts after event processing completes.

The IFW uses the Apache ActiveMQ message broker, which fully implements the Java Message Service (JMS) as its protocol.

ActiveMQ Server

Apache ActiveMQ is an open source (Apache 2.0 licensed) message broker that fully implements the Java Message Service 1.1. The ActiveMQ Server controls all messaging and communication from external sources. The server also receives alerts and CI information from connectors through the IFW and sends this information to various components for storage and analysis. This component is always installed with the SA Manager.

Connectors

A connector is software that provides the interface for the data exchange between the CA Catalyst infrastructure and a domain manager. Connectors are the gateway through which data is retrieved from various domain managers for a consolidated management. Each integrated product has its own connector that supports one or both of the following operation types:

Outbound from connector

> Outbound from connector operations obtain data (such as services, CIs, topology, alerts, and status) from the source domain manager. All connectors must implement outbound operations. Outbound data populates the CA Catalyst Persistence Store.
>
> Outbound data flows to one or more clients. Clients such as CA Catalyst consume the data to implement a unified view of data from multiple domain managers and their connectors.

Inbound to connector

Inbound to connector operations (also referred to as "southbound") use records in the CA Catalyst Persistent Store and the CA Catalyst Synchronizer to create, update, or delete items in the source domain manager. The inbound operations enable domain manager synchronization with the changes that CI reconciliation, CI creation, and CI updates initiate in other domain managers.

Many provided connectors support inbound operations. Connectors that implement inbound operations sometimes limit the implementation to a subset of the types and properties their outbound operations support.

A *bidirectional connector* supports both inbound and outbound operations. Outbound-only connectors contain one connector policy file that transforms the gathered data to the standard USM format. Bidirectional connectors contain two connector policy files that transform outbound data to the USM format and transform inbound data to the source format of the domain manager.

You can configure connectors and start and stop them by accessing the CA SOI Administration UI.

CA SOI also provides the following tools for defining custom integrations:

- The Universal connector that can retrieve services, CIs, and status events from various CA Technologies and third-party products. The Universal connector provides a web services interface that products can use to publish new services, CIs, and events, which are normalized to a common format and made available to the SA Manager.
- A connector SDK for developing custom connectors. The SDK includes a Sample connector, which provides the framework for writing a connector to integrate with important applications in your enterprise.
- An Event connector that collects events from low-level event sources, transforms them into the CA SOI alert format, and displays them as infrastructure alerts in CA SOI associated with existing or created CIs.

Note: For more information about the connectors provided, see the *Release Notes*. For more information about connector architecture and how to build custom integrations, see the *Connector Guide*. Each connector also ships with a connector-specific *Connector Guide* that contains information about connector installation, configuration, how the connector interprets data from its domain manager, and whether it supports inbound operations.

CA Event Integration

CA SOI uses the CA Event Integration technology to enable integrations with low-level event sources through the Event connector. The Event connector provides integration with several raw event sources:

- Windows Event Log
- CA NSM agent messages from a CA NSM Event Manager or Agent
- Log files
- CA OPS/MVS EMA alarms and CA SYSVIEW PM alerts
- HP Business Availability Center alerts
- Web services events
- SNMP traps

The Event connector configures automatically when you install it. However, you can add or edit integrations with specific sources by launching the CA Event Integration administrative interface in context from CA SOI.

CA Catalyst Infrastructure

CA SOI fully adopts the CA Catalyst integration platform as its infrastructure. CA Catalyst is the CA Technologies common integration platform that provides the groundwork for unifying data from all CA Technologies products and many third-party products. CA Catalyst is fully embedded in the SA Manager installation. CA Catalyst provides the following functionality:

- A common semantic schema for data from all integrated products
- CI reconciliation to ensure that resources managed in multiple products have a unified set of property values
- CI synchronization that triggers bidirectional connector updates to source domain managers according to CI reconciliation and other operations
- The ability to enact specific use cases (including use cases that were available in previous releases of CA Catalyst), and the ability to manipulate the infrastructure to configure custom use cases, reconciliation formulas, and synchronization rules

Unified Service Model

The *Unified Service Model (USM)* is the semantic schema that is used as the CA Catalyst and CA SOI infrastructure. Connectors transform all data that is collected from domain managers to the USM format before sending the data through CA Catalyst. The USM schema is stored in the CA Catalyst Registry.

USM is a high-level abstraction and generalization of IT management concepts that facilitate the semantic merging and interoperability of more specific domains. USM is developed to abstract and integrate information across many management products and domains. USM provides a single point for data federation, interoperability, and access to management data across an enterprise.

CA Catalyst provides the mechanisms to make all outbound from connector data adhere to the USM schema. CA SOI provides the interfaces to display the USM-compliant data.

Persistence Service

The Persistence Service enables other components to manipulate the Persistent Store. Operations such as reconciliation and synchronization require CA Catalyst components to modify the USM data. The Persistence Service enables interactions through a flexible interface that supports the following operations:

- Creating and storing USM data in response to incoming CIs from connectors
- Updating and deleting USM data in response to the reconciliation that the Logic Server performs
- Retrieving the USM details for display by the USM Web View
- Creating and updating USM data in response to operations initiated from the USM Web View

The Persistence Service provides an abstraction layer for working with data in the Persistent Store, which is the database record of USM data.

Logic Server

The CA Catalyst Logic Server provides the logic and the modules that carry out the following operations:

Reconciliation

Creates a unified set of properties and values from instances of a single entity that multiple connectors retrieve. The Logic Server reconciles CIs using formulas that define the property values to use. The policy rules that you can define include first non-null wins, majority wins, and data from a specific domain manager wins.

Synchronization

Detects the following CI changes within the Persistent Store:

- reconciliation
- CI creation in the USM Web View
- CI update or deletion in a source domain manager, or through some other method

Synchronization pushes the changes to applicable domain managers integrated through bidirectional connectors. Synchronization policies can create specific synchronization rules or use cases that keep source domain managers synchronized with the USM data.

The Logic Server lets CA Catalyst create and maintain a unified set of reconciled, correlated data in the Persistent Store. From the Operations Console, you can view the reconciled set of USM properties for any CI, named the reconciled sheet. You can also view the USM notebook for any CI. The notebook lists the reconciled sheet and the USM properties for each managed instance of the CI in source domain managers.

Registry

The CA Catalyst Registry is the repository for the USM schema and the policies that control the behavior of the Logic Server. You can access the Registry Administration UI from the CA SOI Administration UI to manipulate the Logic Server policies that control reconciliation and CI synchronization.

UCF Broker

The UCF Broker is a communication layer that controls access to the enabled bidirectional connectors, which can invoke inbound to connector operations on source domain managers. The Logic Server communicates synchronization changes to bidirectional connectors through the UCF Broker.

SA Store

The SA Store is the central repository for all CA SOI configuration and management data. It is a relational database from which the other CA SOI components retrieve their configuration policy and the read-write management data about the state of services and resources. The SA Store includes the following components:

- The CA Catalyst Persistent Store, which maintains a record of reconciled USM data (CIs, alerts, and relationships)
- Tables that contain data specific to CA SOI, such as escalation policies and service models

SA Manager

The SA Manager integrates the data that the connectors send:

- Correlates data so that CIs managed in multiple products are managed as one entity in CA SOI
  - Updates the Persistent Store with USM data
  - Provides correlation information to the Logic Server for reconciliation
- Manages CI and service status as follows:
  - Monitors the health and availability of managed CIs and services
  - Performs service impact and risk analysis
  - Monitors service-level agreements against defined thresholds
  - Updates the SA Store with analysis results and state changes
- Provides event and alert management functionality as follows:
  - Event policies to filter, correlate, and enrich events in the event store
  - Federated query of events across all integrated domain managers
  - Management of service impacting and all non-service impacting alerts
  - Alert queues to manage alerts by common properties
  - Escalation policies that can automate the response to alert occurrence, such as creating a help desk ticket, sending an email, and running a custom script or a CA Process Automation process

UI Server

The User Interface Server (UI Server) is the server that hosts the user interface applications. The UI Server is hosted within a web server, and you can deploy multiple UI Servers in a single CA SOI installation to support load balancing.

CA SOI has the following user interfaces:

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. Administrators use this interface to define users and user groups, set role-based security, create and maintain service definitions, and more.

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.

Mobile Dashboard

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

Report Console

Displays several types of scheduled and on-demand reports for service data in a portal-style interface. The reports provide service stakeholders with historical information that includes details about the availability and risk of a service.

Administration tab

Provides the tools to maintain connectors and SA Manager settings. The Administration tab also lets you configure single sign-on using CA EEM, email notifications, and other administrative functions.

USM Web View

Lets you browse and search all USM data in the Persistent 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.

Debug Pages

The CA SOI Debug pages let you test and debug various CA SOI components. For more information, see the *Troubleshooting Guide*.

CA EEM

CA Embedded Entitlements Manager (CA EEM) provides role-based authentication services for the CA SOI user interfaces and supports single sign-on across most interfaces. Single sign-on (SSO) requires all applications participating in SSO to use the same CA EEM server.

CA Business Intelligence

CA SOI implements BusinessObjects, which is a third-party business intelligence platform that provides interactive reporting. CA Business Intelligence hosts predefined CA SOI reports, which include scheduled and on-demand reports.

Chapter 3: Configuring CA SOI

This section describes the functionality available from the Administration tab of the Dashboard.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

This section contains the following topics:

Connector Configuration Tasks

As an administrator, you can view a connector status, edit a connector configuration including the CMDB connector, and change the connector properties.

For more information about working with connectors, see the *Connector Guide*.

View Connector Status

As an administrator, you can view the Connector Status table, which lists all the connectors available to CA SOI. From this table, you can monitor the IFW and connector status.

Follow these steps:

1. Click the Administration tab, and select Connector Configuration.

   The Connector Status table displays with the following columns:

   Connector Service

   Displays the name of the server where the IFW is installed. The IFW exists on every system that has at least one connector installed, and it connects to the domain manager that CA SOI is monitoring.

   Status

   Displays one of the following states for the IFW on the connector server:

   Online/Offline

   Indicates that the IFW is running or not running.

   Initializing

   Indicates that the IFW is starting up.

   Handshake

   Indicates that the IFW was started and is waiting for CA SOI to contact it.

   Closing

   Indicates that the IFW is shutting down.

   Connector

   Displays the connector identifier using the following format:

   connector_mdrproductvalue@product_host. The connector runs on its installed system, communicates with the individual domain manager, collects data from it, and lets the IFW process this data. The connector identifier typically includes a unique ID number for each connector and the system on which the integrated domain manager is installed.

Status

Displays one of the following states:

Online\Offline

Indicates that the connector is running or is not running.

Initializing

Indicates that the connector is starting. This state is short-lived during which connectors initialize their connections to domain managers and build their caches before switching to the Online status.

Handshake

Indicates that the connector was started and is waiting for CA SOI to contact it.

Closing

Indicates that the connector is shutting down.

Source Description

Contains information about the source domain manager with which the connector integrates, specifically on which system the domain manager is running.

Connector Description

Contains the connector identifier and version number.

2. Click one of the server names in the Connector Service column.

   The read-only details page opens and displays the following details about the IFW on each connector server:

   Note: The tree view in the Administration Pages pane is expanded, and the selected server is highlighted under the Connector Configuration node. You can also navigate to this details page by clicking the tree nodes.

   CA Service Operations Insight Integration Framework Status

   Indicates the status of the IFW on the system.

   Messaging Service Properties

   Displays information regarding the ActiveMQ messaging service that controls the exchange of information between the connector, the IFW, and manager components.

Connector Status

Contains status information about the connectors that are installed on this system.

UCF Broker 1/UCF Binding 1

Contains information about UCF, or the common CA Catalyst connector framework.

3. Select Connector Configuration in the tree to return to the Connector Configuration page.

4. Select one of the connector identifiers in the Connector column.

   Note: The tree view in the Administration Pages pane is expanded and the selected server is highlighted under the Connector Service node. Also, you can navigate to this details page by clicking the tree nodes.

   For more information about editing the connector, see Edit Connector Configuration (see page 44).

Edit Connector Configuration

As an administrator, you can change the configuration settings, navigate to the Connector Configuration page on the Administration tab in the CA SOI Dashboard. Connectors are initially configured when you install them.

Follow these steps:

1. Click the Administration tab and the Connector Configuration option.

   The Connector Configuration page opens and displays the Connector Status table.

2. Click one of the connector names in the Connector column.

   The connector details page opens and displays a number of tables with additional details about the connector and the server where it is installed. Many connectors also have a read-only Connector Type Data table that displays information such as the supported CI types.

   Note: If your connector supports Scheduler Configuration and has the scheduler property enabled, then the button is available. For more information about Scheduler Configuration availability, see the connector documentation provided with your connector.

   Important! The CA:00056_service-discovery@*servername* entry on the SA Manager server represents the Service Discovery component. This entry always has blank Connection Details. Do not edit any of the connector controls for this entry.

3. (Optional) Edit the following settings in the Connector Controls column as necessary, and click Save:

   dns_resolution

   Specifies whether to use DNS resolution to resolve device names. If a reliable DNS mechanism is not in place (for example, no DNS server on the network, or configuration items (CIs) not defined to the DNS), disable DNS lookups to prevent CI resolution and normalization failure.

   Default: on

   useAlertFilter

   Specifies whether to filter alerts based on their existence in a managed service in CA SOI. If the control is turned on, the connector only sends domain manager alerts that are associated with a CI that is part of an existing managed service in CA SOI. If the control is turne*d* off, the connector forwards all alerts from the domain manager, regardless of whether they relate to a service.

   Default: on

   Note: For CA SOI r3.1 and later, the IFW no longer requires or uses EVENT_FILTER requests. The IFW now sends the alerts (managed or unmanaged) that the connectors report to the SA Manager. CA SOI ignores the global setting sendAllAlerts (in the IFW configuration file) and the connector-specific setting useAlertFilter (on the Administration tab Connector Configuration page). CA SOI now behaves as if sendAllAlerts=1 and useAlertFilter=0, regardless of the actual settings.

   getCIsAtStartUp

   Specifies whether to rediscover CIs every time the connector starts. This control is enabled by default so that connectors always provide a current record of all CIs from their domain managers. You can turn this control off if the connector does not support collecting CIs at startup, such as the Universal or SNMP connector.

   Default: on

   isRemotable

   Specifies whether to allow the connector framework to access the connector remotely for create, update, and delete operations on the source domain manager.

   Default: on

   useServiceFilter

   Specifies whether to send all relationships to CA SOI or only the ones associated with modeled services. Set the control to true to run relationships through a service filter and receive only the relationships associated with modeled services.

   Default: on

getRelationshipsAtStartup

Specifies whether to rediscover relationships every time the connector starts. This control is turned off by default so that relationships are only obtained and imported as a part of service model imports. You should only enable this control if you require relationship CIs outside of imported service models, for example, if you define an Unmanaged Relationship Service Discovery rule.

Default: off

performDeltaProcessing

Specifies whether to process and publish deltas on CIs between the time the connector or SA Manager was last stopped or restarted. When enabled, this setting also performs delta processing on relationships if the getRelationshipsAtStartup property is enabled.

Default: on

4. Select any field in the Connection Details, Connector Instance Data, and Launch in Context Details tables, edit the configuration setting, and click Save in the same table.

   The changes are saved. Verify that any changes you make the connection settings do not break the connection. For example, if you modify a Host field in the Connection Details, first confirm that the domain manager is installed and configured on the new host.

   Note: For information about the connector parameters for each connector, see the *CA Catalyst Connector Guide* provided with the specific connector package.

5. Click Stop and wait until the connector status changes to Offline.

6. Click Start and wait until the connector status changes to Online.

   The connector is restarted. Depending on the type of connector, it can take a few minutes before the connector Status displays Online.

Important! Do not perform rapid start and stop operations on the connector. Each stop and start sends the corresponding command to the connector. Rapid start and stop operations from the interface can cause these commands to queue on the connector and cause the connector to start and stop repeatedly until all commands in the queue are processed.

Configure the CA CMDB Connector

To ensure that CA CMDB View works properly with the CA Service Desk connector version 3.2, it is necessary to add LicURL information to the CA CMDB connector configuration file.

Follow these steps:

1. Locate the ServiceDeskManagerConnector.conf connector configuration file.

   The configuration file is located in the Catalyst registry in: topology\physical\ContainerName\modules\configuration.

   If the Catalyst container was configured during the installation to use a file-based registry (which is the most common way for a CA SOI solution), then the location is: CatalystContainerHome\registry\topology\physical\<ContainerName>\modules\configuration.

   If a Catalyst server is being used for the registry, then it is a similar directory accessible through the Catalyst Admin UI (or ws02 registry UI).

2. Add the following element to the configuration file:

```
<LaunchInContextUrls>
    <LicUrlTarget>
     <Label>Service Desk Manager</Label>
     <Type>CI</Type>

    <Url>http://CMDB-HOST:8080/CAisd/pdmweb.exe?OP=SHOW_DETAIL+FACTORY={UrlPa
    rams}+PERSID={MdrElementID}</Url>
    </LicUrlTarget>
</LaunchInContextUrls>
```

   This will allow you to launch the CA Service Desk Manager Web Client in the context of a CI in the CA SOI console.

   Note: If you save the configuration from the Catalyst Admin UI, CA Catalyst alters the configuration slightly, adding the 'ns2' namespace to the elements. It also adds an empty section for LaunchInContextUrls:
   `<ns2:LaunchInContextUrls\>`

   Make sure you delete this section.

Configure the IFW Configuration File

As an administrator, you can change the connector-related settings that are saved in the IFW configuration file (SOI_HOME\resources\Configurations\SSA_IFW_HostName.xml). The settings are applicable to all connectors running under that IFW. You can configure the IFW configuration file to change these settings globally for all connectors on the system. For example, changing the alert filter setting at the IFW level automatically overrides the individual alert filter settings for all the connectors that are installed on that IFW system.

Follow these steps:

1. Open the SOI_HOME\resources\Configurations\SSA_IFW_HostName.xml file on a system with the IFW installed (any system with connectors or the SA Manager).
2. Change the value for the appropriate parameters in the ConnectorConfig section as follows, and save and close the file when finished:

   Important! Use caution when changing these settings, and change documented settings *only*.

   retryCount

   Defines how many times to retry connecting to the ActiveMQ Server component on the SA Manager when the connection fails. Before changing the default retry settings, consider that the amount of time a connector waits for the ActiveMQ Server connection reflects the amount of queued data that will consume memory in the IFW until the connection is reestablished.

   Default: 5

   retryInterval

   Defines the number of seconds between retrying to connect to the ActiveMQ Server.

   Default: 30

   dns_resolution

   Defines whether to use the DNS lookups for the CI name resolution. The default value of 1 turns on DNS lookups for all connectors on the system. When set to 1, you can also manage DNS lookup settings by connector if you want to use different settings for each connector. Change this value to 0 to disable the DNS lookups for all connectors. When you set this value to 0, you cannot manage DNS lookup settings by connector; DNS is always disabled for all connectors.

   Default: 1

   Note: For more information about managing DNS lookup settings by connector, see Edit Connector Configuration and the *Implementation Guide*.

sendAllAlerts

Defines whether to filter or send alerts that are not associated with a managed service. The default value of 1 sends all alerts from all connectors. Change the value to 0 to let you specify this behavior by connector.

Default: 1

Note: For CA SOI r3.1 and later, the IFW no longer requires or uses EVENT_FILTER requests. The IFW now sends the alerts (managed or unmanaged) that the connectors report to the SA Manager. CA SOI ignores the global setting sendAllAlerts (in the IFW configuration file) and the connector-specific setting useAlertFilter (on the Administration tab Connector Configuration page). CA SOI now behaves as if sendAllAlerts=1 and useAlertFilter=0, regardless of the actual settings.

throttleConnectorStartup

Defines whether to initialize connectors on the system simultaneously or one after another. The default setting of 0 initializes all connectors simultaneously. You can change this setting to 1 for connectors to initialize sequentially, which can improve the performance. The setting can also prevent memory overuse if there are multiple connectors on the system that manage large amounts of CIs.

Default: 0

3. Restart the CA SAM Integration Services service.

Connector Removal

You can either permanently or temporarily remove a connector from the CA SOI database and all interfaces:

- Permanently remove an uninstalled connector (see page 50).
- Temporarily disable an installed connector (see page 50).

Remove an Uninstalled Connector

After you uninstall a connector, remove the database references using the Administration tab. This also removes the connector database entry and the connector name from the list of connectors in the tree view.

If the connector comes back online after the operation is completed, the connector reregisters with CA SOI.

Follow these steps:

1. Select the Administration tab and the Connector Configuration option.
2. Select the name of an offline connector in the Connector column.

   Note: You cannot remove an online connector.
3. Click Remove Connector and confirm the deletion.

   The selected connector registration is permanently removed from the CA SOI database, and the connector name is removed from the tree on the Administration tab.

Disable an Installed Connector

You can disable an installed connector if you want to remove connector records temporarily, but keep the connector installed for potential future use.

Important! To ensure data integrity, perform this operation after business hours for connectors with a large amount of CIs and relationships. Removing the database information for these CIs and relationships locks the system for approximately ten minutes for every 100,000 CIs managed by the connector.

Note: If you are using CA Service Desk with the auto clear alerts option enabled, then shut down or remove a connector, CA SOI automatically changes the cleared alerts to the selected status. You cannot undo this operation. For more information, see the *Implementation Guide*.

Follow these steps:

1. Select the Administration tab and the Connector Configuration option.
2. Verify that the Connector Service status is Online for the connector to disable.

   The IFW for the connector must be running for the disable operation to work. If it is not running, start the CA SAM Integration Services service on the connector system.
3. Select the connector to disable.
4. Click Stop if the connector appears as Online.

   Note: You cannot disable an online connector.

5. Click Remove Connector after the connector appears as Offline and confirm the disable.

   The selected connector's registration is removed from the CA SOI database and the connector name is removed from the tree on the Administration tab. However, if the connector is still installed, all of its required files still exist in case you want to re-enable the connector.

Enable a Disabled Connector

You can enable a connector that you previously disabled to bring it back online and collect data from its domain manager again.

Follow these steps:

1. Open the connector configuration file that in the SOI_HOME\resources\Configurations folder on the connector system.

   The format of the connector configuration is typically the connector name followed by the connector system name (for example, sampleConnector_server1.xml).

2. Change the State property value from not Enabled to Enabled and save the file.
3. Restart the CA SAM Integration Services service on the connector system.

   The connector entries reappear in the Connector Configuration tree and in all other interfaces, and the connector begins collecting data from its domain manager.

Connector Removal Success and Failure Messaging

CA SOI provides an Administration tab confirmation message that indicates success or failure upon connector removal.

Note: This procedure assumes that you have already uninstalled the connector and are trying to remove its data from the CA SOI interfaces.

Follow these steps:

1. On the Dashboard, click the Administration tab.
2. Click the plus sign (+) next to the Connector Configuration.
3. Click the plus sign (+) next to a connector.
4. Click the connector.
5. If the connector is still online, click Stop.
6. Click Remove Connector.

   A confirmation appears at the top of the page that provides the connector removal success or failure.

View SA Manager Details

As an administrator, you can view details about the SA Manager to help troubleshoot messaging and database connection issues. You can also access the Web Server Debug page and server log pages from this page. For more information about troubleshooting and using the CA SOI debug pages, see the *Troubleshooting Guide*.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to the CA Service Operations Insight Manager Configuration option.
3. Click the name of the server you want details about.

Configure CA Embedded Entitlements Manager Single Sign-On

As an administrator, you can enable single sign-on with CA EEM. The SA Manager and UI Server use CA EEM to authenticate user credentials against multiple applications.

Establish or update CA EEM connection settings in the following circumstances:

- You did not define CA EEM connection settings during the CA SOI installation.
- The password for the EiamAdmin user changes.

Note: Other changes to the CA EEM server can also require you to update the CA EEM configuration settings.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to the CA Service Operations Insight Manager Configuration or CA Service Operations Insight UI Server Configuration option.
3. Click the plus sign (+) next to the server you want to configure.
4. Click the EEM Configuration option.
5. Specify the following parameters:

   Note: If you do not know these values, refer the Installation Worksheet for the CA EEM values. For more information, see the *Implementation Guide*.

   EEM Server Host

   Defines the name of the server where CA EEM is installed.

   User Name

   Defines the name of the CA EEM administrator user (typically EiamAdmin).

Password

Defines the password of the CA EEM administrator user.

Application Name

Defines the application name CA EEM uses for CA SOI user management. The entry uses the following format: SOI_*soi_server_name*.

Change Password Allowed

Specifies whether users can change their password from the CA SOI interface. Select this box from the UI Server EEM Configuration page to enable password changes from the CA SOI interface.

6. Click Test to verify that the settings are valid on the CA EEM server, and click Save.
   - If you clicked Test, the settings are temporarily applied and your user credentials are validated. If errors are displayed, fix them before saving or retesting.
   - If you clicked Save, the settings are saved and a confirmation message displays.
7. (Optional) Click Launch EEM to open the CA EEM login page.

   The login page opens and the CA SOI instance you specified in the Application Name field is added to the CA EEM login page Application drop-down list.

Important! Update the CA EEM configuration settings for the SA Manager, and the UI Server.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

CA SiteMinder Single Sign-On

You can use CA SiteMinder to enable single sign-on across products that are using the same CA EEM server. For example, if you log in to CA Spectrum and use the same browser to log in to CA SOI, the CA SiteMinder session token is passed to CA SOI through CA EEM. You do not have to log in again.

To use this feature, use the same CA EEM server to manage users for multiple products, then integrate the CA EEM server with CA SiteMinder.

Configure Email and Failure Notifications

As an administrator, you configure email for CA SOI notifications, including failure messages.

Configure Email

As an administrator, if a *mailhost* DNS alias for the email server does not exist, you provide a server name so that CA SOI can send email notifications. Mailhost is a common DNS alias for the email server, and is the default setting in CA SOI. These settings are also used to update settings in Registry used by CA Catalyst components. CA Catalyst sends a notification email if there is an error during CI reconciliation or synchronization.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to the CA Service Operations Insight Manager Configuration or CA Service Operations Insight UI Server Configuration option.
3. Click the plus sign (+) next to the server you want to configure.
4. Click the Email Configuration option.
5. Complete the fields and click Save.
6. Depending on the server you configured, restart the CA SAM Application Server service or the CA SAM User Interface Server service.

Important! Set or update the email configuration settings for both the SA Manager and UI Server.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

Configure Failure Email Notifications

As an administrator, you can configure email notifications to a specified administrator or administrators when certain failures occur. CA SOI also provides logging for the failures:

- The action mechanism fails due to a third-party server connection error. The action mechanism relies on a connection to external servers for the help desk (CA Service Desk), workflows (CA Process Automation), and so on. CA SOI now notifies a specified administrator when the connectivity is lost for more than a specified number of minutes.
- The SA Manager fails due to looping errors. For more information, see Loop Detection during Impact Analysis (see page 56).
- A connection to the SA Store database fails.
- A connector status changes or fails. For more information, see Connector Shutdown Notifications (see page 56).
- After a configured retry duration period, an escalation policy action fails.

The email notifications provide a description of the problem and troubleshooting tips to resolve the problem.

For any failure, CA SOI updates the soimgr.log file with failure information.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Error Notification Configuration.
5. Enter the full email address for the administrator.

   Note: Enter multiple email addresses separated with commas (,).
6. For each notification section, perform the following actions:
   a. Select Yes from the drop-down to turn on email notifications.
   b. Enter the number of minutes until CA SOI sends the email notification.
   c. **Note:** The minimum value is 1 minute.

Loop Detection During Impact Analysis

CA SOI detects loops during an impact analysis. An administrator can configure CA SOI to send an email notification when the SA Manager fails due to looping.

When CA SOI detects a loop in a service or service hierarchy, the SA Manager marks that service as being in TEST mode. This blocks the service state propagation and, in effect, takes the service offline. If the email notification is enabled for the SA Manager events, then CA SOI generates an email. The email contains the name of the service that CA SOI detected the loop in and the SA Manager that CA SOI detected the loop on. To return the service to a production state, edit and then save the service.

When CA SOI detects a loop during an impact analysis, CA SOI appends the following message with the name and internal model handle to the soimgr.log file. CA SOI appends a message each time that CA SOI detects looping.

```
*********************************************************************************
*********************************************************************************
*********************************************************************************
ATTENTION! Loop detected in service 'XYZ' Setting all service properties for
MH(0x10000000003) to TEST
*********************************************************************************
*********************************************************************************
*********************************************************************************
```

Connector Shutdown Notifications

CA SOI provides notifications and detailed logging when a connector shuts down. CA SOI logs and sends an immediate notification to the administrator in the event any connector goes offline for any reason. You can set an interval where CA SOI consolidates all failed connector information into one notification. The improved and faster notification mechanism provides comprehensive information about the connector shutdown behavior, including any appropriate reason for the shutdown. The information in the log messages helps you troubleshoot connectors, audit the connector status in your infrastructure, and take any prompt actions. You can review the related log files to find more information about any anomaly that you encounter in the connector behavior. The easy identification of the problem that is associated with the connector also lets you manage your domain managers more efficiently.

The enhanced connector notification and logging mechanism, therefore, helps you as follows:

- Logs the appropriate reason (for example,connector failure or an IFW shutdown) for the connector shutdown in the log file, SAM-IntegrationServices_wrapper.log. You can review the log file to locate and analyze the message information.

- Includes the shutdown message in the connector status notification as part of the *heartbeat* message. The heartbeat message is logged into the <*ConnectorName*>_HEARTBEAT_PUB.txt. You can review this file to see the message included in the statusDesc property.
- Displays the reason for the connector shutdown in the Administration UI and Console.
- Sends an email notification to the CA SOI administrator about the connector shutdown.

Configure Help Desk Integration

As an administrator, you can configure CA SOI to communicate with CA Service Desk, BMC Remedy IT Service Management Suite, HP Service Manager, ServiceNow, or a custom help desk application.

After you complete this configuration, CA SOI can create help desk tickets that are automatically based on alert escalation policies and their associated actions.

For help desk product integration procedures, see the *Implementation Guide.*

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Help Desk Configuration.
5. Select or enter the appropriate information in the following fields:

   Help Desk Type

   Specifies the type and version of help desk software you want to integrate with CA SOI.

   Server

   Specifies the name of the help desk host server.

   Note: Install the Service Desk Web Services component on the CA Service Desk server for the integration with CA Service Desk to work.

   Server Port

   Specifies the port number that the help desk host server uses.

   Launch in Context Port

   (CA Service Desk Only) Specifies the port number that is configured on the help desk host server to launch the ticket detail page.

User

Specifies the user account with which to access the help desk.

Password

Specifies the password that corresponds with the help desk user account.

SSL

Specifies whether to use SSL to communicate with the selected help desk application.

Note: Import an SSL certificate from the help desk application or CA Process Automation (if you selected BMC Remedy or HP Server Manager) into the CA SOI trust store for the SSL connection to work. For more information about importing the SSL certificate, see the *Implementation Guide*.

6. (Optional and available only if CA Service Desk integration with Polling is off and SDM Notifications ON) Click the button that is available:

   Resync

   Synchronizes the CA Service Desk Manager ticket statuses. Use when the Service Desk Manager server is restarted to ensure that the ticket statuses are synchronized.

   Refresh Status

   Refreshes and displays the status of the Resync button. This button is available only while a resync is in progress.

7. Click Test to verify that CA SOI can connect to the selected help desk application.

   A message confirms the connection.

8. Click Save.

   CA SOI is configured to communicate with the specified help desk application.

   The updated configuration file is in the SOI_HOME\tomcat\custom\help-desks.xml folder on the SA Manager server.

9. Restart the CA SAM Application Manager service and verify that all changes function correctly.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

More Information:

Edit Help Desk Configuration (see page 59)

Edit Help Desk Configuration

After you configure integration with a help desk product, you can configure global preferences for a help desk configuration. You can also create and maintain custom help desk and announcement properties. For more information about integrating CA SOI with help desk products, see the *Implementation Guide*.

Follow these steps:

1. Select Tools, Help Desk Configuration in the Operations Console.

   If the Help Desk Status entry is Not Configured, then the connection to a help desk is not configured correctly in the Administration UI. You can still set the help desk configuration in this dialog, but it does not go into effect until a valid help desk connection is established.

2. Select the type of help desk in the Help Desk Type drop-down list.

   Note: If you select BMC Remedy or HP Service Manager, the General tab becomes unavailable. You configure these options for BMC Remedy or HP Service Manager in the CA Process Automation form used to configured BMC Remedy or HP Service Manager server settings. For more information, see the *Implementation Guide*.

3. Set the following properties in the General tab and click Save:

   Auto clear alert

   Specifies whether to clear the alert automatically in CA SOI when the corresponding help desk ticket changes to the selected status in the help desk.

   Auto change trouble ticket status when alert is cleared

   Specifies whether to change the help desk ticket status automatically to a specified value when the corresponding alert in CA SOI clears.

Enable Polling

Specifies whether to poll the help desk application for synchronization. If you select this option, specify a polling interval in the Polling interval for synchronization field. Enable polling if you selected to automatically clear an alert based on ticket status, and the help desk product cannot perform activity notifications triggered by certain user actions and call external binaries as a result of these actions. If this functionality is absent in the help desk, CA SOI must poll the help desk to query for ticket closure.

The help desk configuration is saved.

4. (Optional) Click the Ticket Properties or Announcement Properties tab and add a custom ticket or announcement properties.

   On this tab, you can also edit or delete existing custom tickets or announcement properties.

Add Custom Ticket or Announcement Properties

You can add custom ticket or announcement properties. You make the properties available for the create ticket or announcement actions.

Note: If you added custom ticket properties using other methods in previous releases (such as through CA Event Integration or the SD-ticketProps.xml file), migrate the custom properties to the Help Desk Configuration dialog.

Follow these steps:

1. Click the Ticket Properties or Announcement Properties tab on the Help Desk Configuration dialog (see page 59).

   The current list of available ticket or announcement properties appears.

2. Click ⊕.

3. Complete the following fields and settings:

   Property Name

   Defines the name of the property in the help desk.

   Property Label

   Defines the property name to display on the Create Action dialog.

   Value Type

   Specifies whether the value for the custom property should be selectable from a drop-down list or definable in a text field.

Required Property

Specifies whether the property should be required in all ticket or announcement actions.

Show Create Option

Specifies whether to display the 'Create Object if not present' check box for the property to provide the option to create the object in the help desk if it does not currently exist.

4. (Drop-down value type only) Define the values to make selectable for property assignment in the 'Drop down values' pane as follows:

   - Select potential values from the 'Available property values' list and move them to the 'Allowable values for this property' list. Any of the expandable runtime tokens take the specified value from the alert to populate the property. Both CA SOI and USM alert properties are available as expandable runtime tokens. The list contains CA SOI properties; click More to view the full list of available USM and CA SOI properties.
   - Click New to add custom potential values to the 'Allowable values for this property' list.

5. Complete the following fields and click OK:

Default Value

(Optional) Defines the default value that is displayed when adding the property to an escalation action. This property must exist in the 'Allowable values for this property' list if the value type is a drop-down list.

Data Type Mapping

(Optional) Defines the object type to use for ticket creation that is based on the custom property value. Available values are ASSET, CONTACT, GROUP, STRING, and TEMPLATE. For example, if you create an EmergencyContact custom property and map it to the CONTACT data type, the help desk looks up any CONTACT with the matching value for this property and uses that object for ticket creation.

Hint Text

(Optional) Defines the text that appears when you click the Hints link next to the property when adding it to an escalation action.

The property appears in the Current List of Properties pane in the Ticket Properties or Announcement Properties tab.

Value Mapping

The values for priority and severity are different in CA SOI and CA Service Desk. The following tables show how the values equate to each other. The value mapping happens automatically when the expandable runtime tokens are used. You are responsible to implement the mappings when setting custom property values.

Priority

The priority value from CA SOI is the maximum priority of all of the services that the alert impacts. The service priority value is set for each service. The value is located in the Operations Console on the Information tab of the Component Detail pane.

CA SOI value	CA Service Desk value
0	5
7	4
8	3
9	2
10	1

Impact

The impact value from CA SOI is the maximum impact of all the services that the alert impacts. CA SOI sets the impact value and it is located in the Operations Console on the Alert Details tab of the Component Detail pane.

The CA Service Desk impact is the greatest with lower numbers.

CA SOI value (Low to High)	CA Service Desk value (Low to High)
1 (Slight)	5 (One Person)
2 (Moderate)	3 (Single Group)
3 (Severe)	2 (Multi Group)
4 (Down)	1 (Entire Org)

Severity

The severity value from CA SOI is the severity of the alert. This value is located in the Operations Console on the Alert Details tab of the Component Detail pane.

CA SOI value (Low to High)	CA Service Desk value (Low to High)
1 (Minor)	1 (Escalation)
2 (Major)	3 (Manager Escalation)
3 (Critical)	4 (HD Mgr. Escalation)
4 (Down)	5 (All Hands Escalation)

Configure Synchronization

As an administrator, you use the Synchronization Configuration page to enable or disable the following synchronization use cases:

- Synchronize the Cleared and Acknowledged alert properties (see page 256) in CA SOI and CA NSM, CA Spectrum, and Microsoft SCOM
- Synchronize services, CI types, and relationships (see page 262) in CA SOI and BMC Atrium or CA CMDB
- Synchronize maintenance mode status (see page 268) with connectors that support inbound to connector operations on the IsInMaintenance USM property, and set the reconciliation formulas for the IsInMaintenance property

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Synchronization Configuration.
5. Enable or disable the component synchronization for alerts, services, or maintenance mode.
6. Click Save.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

More Information:

Working with CA Catalyst Synchronization (see page 253)

Configure CA Process Automation Integration

As an administrator, you configure a connection with a CA Process Automation installation to invoke CA Process Automation Forms and Processes in an alert escalation action. For example, when an alert occurs specifying that a system is down, you can configure escalation policy to invoke a CA Process Automation Form or Process that restarts the system.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Process Automation Server Configuration.
5. Complete the fields and click Save.

   Note: Import a CA Process Automation certificate into the CA SOI trust store for the SSL connection to work. For more information about importing the CA Process Automation certificate, see the *Implementation Guide*.
6. (Optional) Click Launch Process Automation Web Admin.
7. Log in and create forms for any processes that you want to run as an alert escalation action. Processes must have an associated form to include in escalation actions.

Note: For more information about defining CA Process Automation Forms for Processes, see the CA Process Automation documentation. The documentation is provided on the CA SOI bookshelf.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

Configure Auditing Levels

As an administrator, you change or disable the auditing level for various CA SOI components such as CIs, policies, and events. The audit records are stored in the CA SOI database.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Audit Configuration.
5. You can perform the following actions on this page:
   - Select a default audit level setting for all components or disable auditing entirely.
   - Override the default settings by selecting the auditing options in any section.

   Note: The Generic Type audit is for customized implementations. For more information, contact CA Support.
6. Click Save.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

Configure Global Settings

As an administrator, you configure global settings that determine various default behaviors:

- maintenance mode impact and domain manager maintenance settings propagation
- alert clearing and unknown alerts
- root cause analysis source
- service model granularity and automatic policy maintenance
- escalation policy/actions retry behavior
- projection sheets maximum number

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Global Settings.
5. Make the appropriate selections from the drop-down lists and fields.

   The Global Settings page provides detailed information about each field; however, the following fields require additional information:

   Maintenance Mode Settings

   Propagate Maintenance Impact

   Note: Changing a Global Settings flag while the SA Manager is running only impacts future alerts—it does not affect existing alerts and associated services.

   Propagate Domain Manager Maintenance Settings

   The maintenance setting from the SA Manager can also propagate to other domain managers, depending on your configured reconciliation and synchronization formulas.

   Root Cause Analysis Setting

   Controls the source for root cause analysis. Select CA SOI, Combination, or Domain Manager.

   Consider the following:

   - If you select Combination, CA SOI uses both itself and the domain manager to determine the root cause.

- The Domain Manager and Combination modes require that the domain manager and its connector both support sending the root cause analysis information to CA SOI. For current root cause analysis support see the *CA SOI Release Notes* and the product-specific *Connector Guide* that is provided with each connector.

For more information about working with the root cause analysis mode, see the *Event and Alert Management Best Practices Guide*.

Modeler Settings

Default Service Model Granularity

Select Normal to use a normal granularity service model, which employs explicit modeling and does not aggregate alerts from child CIs not included in the service model.

Select Low to use low granularity so the service model employs implicit modeling and aggregates alerts from child CIs not included in the model.

Maximum Number of Projection Sheets per Notebook for a Connector Setting

When a connector imports CIs into CA SOI, CA SOI can correlate the CIs to existing CIs if their correlation keys match. Typically, you expect CA SOI to correlate a CI from one connector to a CI from another connector. However, there may also be duplicate CIs from the same connector matching and being correlated to the same CI on CA SOI.

When CA SOI imports duplicate CIs from the same connector, CA SOI can create duplicate projection sheets for each CI in the notebook. You can limit the number of projection sheets CA SOI creates by adjusting this setting. For more information about projection sheets and notebooks, see the *Administration Guide*. The suggested value of 1 indicates that CA SOI creates one projection sheet for each unique CI (from the same connector) in the notebook.

CA SOI updates soimgr-debug.log with a warning about duplicated CIs from the same connector.

CA SOI updates the SOI_HOME\tomcat\logs\ci-invalid.log file with the USM attributes for the duplicate CIs. Even if you set the maximum number of projection sheets higher than one, CA SOI updates the log file any time the number of sheets is greater than one.

6. Click Save.

7. Restart the CA SAM Application Server service for the change to take effect.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

View UI Server Connection Details

As an administrator, you view details about the CA SOI UI Servers that are connected to this SA Manager server and active user sessions and enable debugging. Typically, you have one UI Server for each SA Manager, but multiple UI Servers are supported.

Note: You can perform this procedure on the SA Manager server only. The UI Server has a similar feature where you can view details about the users that are logged in to the Operations Console.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click UI Server Connection Details.

   A table displays that provides details about each active user session.
5. (Optional) Click the link in the Debug column to switch between enable and disable for the corresponding UI server.

   When the Debug option is set to enable, client debugging is enabled and the ClientPollServlet outputs all requests and other activity for that client.

More information:

View Client Details (see page 71)
Open the Client Debug Console (see page 73)

View and Manage the UI Server Connection Log

The CA SOI installation application installs a client.log file on the SA Manager. By default, it is located at SOI_HOME\tomcat\webapps\sam\console\logs.

The client.log file contains an entry for every user who logs in to the Operations Console. The Client Log page allows you to view the contents of client.log file. You can also use this page to clear the log and remove old entries.

Note: You can perform this procedure on the SA Manager only. The UI Server has a similar feature where you can view and manage the users that are connected to the Operations Console.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click UI Server Connection Log.
5. (Optional) Enter a number in the 'Purge entries older than # days' field, and click Go.

   The log entries older than the specified number of days disappear from the log.
6. (Optional) Click Clear Log to clear the log entries.

Configure JNLP

As an administrator, you can change the JRE requirements for starting the Operations Console. You can edit any of the default Java Network Launching Protocol (JNLP) settings.

The default memory amount that CA SOI allocates to the Operations Console deployment is 512 MB. This setting may not be sufficient in larger environments where CA SOI manages many services and CIs are staged.

CA SOI notifies you with a message when the Operations Console is using 80 percent (410 MB). CA SOI displays subsequent messages on the status bar.

CA SOI does not force Operations Console to have the same JRE version as the UI Server. You can upgrade the UI Server to a newer JRE version and upgrade the user desktops later. The installed JRE version with the UI Server is 1.7.0_11 and the minimum JRE that is required for the Operations Console is 1.6.0_24.

The default minimum JRE is 1.6.0_24. If a user does not meet the minimum JRE requirement, the Console link is not available on the Dashboard and a message appears that explains the problem.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to the CA Service Operations Insight UI Server Configuration option.
3. Click the plus sign (+) next to the server you want to configure.
4. Click JNLP Configuration.
5. Edit the settings in one or more of the following fields and click Save:

   Required Minimum JRE Version

   > Displays the oldest version of the Java Runtime Environment (JRE) that can be used to start CA SOI.
   >
   > **Default**: 1.6.0_24

   Minimum client memory usage (megabytes)

   > Displays the minimum amount of memory allocated for starting CA SOI.
   >
   > **Default**: 64

   Maximum client memory usage (megabytes)

   > Displays the maximum amount of memory allocated for starting CA SOI.
   >
   > **Default**: 512
   >
   > **Note:** The suggested value for large implementations is 1024 MB.

   The JNLP configuration settings update in the custom-jnlp-config.xml file.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

View Client Details

As an administrator, you can view the Client Details page that lists the users that are currently logged in to the Operations Console. From this page you can also log off users from the Operations Console and send a message to a user.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to the CA Service Operations Insight UI Server Configuration option.
3. Click the plus sign (+) next to the UI Server whose client details you want to view.
4. Click Client Details.

   A table of all clients currently logged in to the Operations Console displays.

Note: You can only perform this procedure on the UI Server. The SA Manager has a similar feature where you can view details about the UI Servers that are connected to it.

More information:

View UI Server Connection Details (see page 68)

Send a Message to a User

You can send a message similar to an email message to any user who is logged in to the Operations Console.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to the CA Service Operations Insight Manager Configuration or CA Service Operations Insight UI Server Configuration option.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Client Details.
5. Click the check box next to one or more users to whom you want to send a message, and then click Send Message.
6. Enter the message and click Send.

Set Client Debug Status

You can enable or disable tracing of HTTP activity for each client session for troubleshooting purposes.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to the CA Service Operations Insight UI Server Configuration option.
3. Click Client Details.

   The Debug column shows whether debugging is enabled or disabled for each client session.
4. Click the link in the Debug column to toggle enable and disable for any user.

More information:

Open the Client Debug Console (see page 73)

Log Off Clients

As an administrator, you can log off other clients when you perform maintenance on the SA Manager or UI Server, or to upgrade the software.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to the CA Service Operations Insight UI Server Configuration option.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Client Details.
5. Click the check box next to one or more user names and click Log Off Clients, then confirm the log off.

Open the Client Debug Console

Important! The Debugging Console is designed to be used only with help from CA Technical Support.

For more information about using the debug pages, see the *Troubleshooting Guide*.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to the CA Service Operations Insight UI Server option.
3. Click the name of the server you want to debug.
4. Click Debugging And Logs.

More information:

Set Client Debug Status (see page 72)
View UI Server Connection Details (see page 68)

Configure Mobile Dashboard Integration

As an administrator, if you want to launch the Mobile Dashboard from the Administration UI and to enable use of the $[Mobile UI URL] runtime token, you configure the Mobile Dashboard connection information.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Mobile Dashboard Server Configuration.
5. Complete the server and port fields.

   Note: Unless you performed a custom installation, the Mobile Dashboard resides on the system where you installed the UI Server.

6. (Optional) Click Launch Mobile Dashboard to test that the URL launches successfully.
7. Click Save.
8. Restart the CA SAM Application Server service for the change to take effect.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

Configure Reporting

Note: You must have CA Business Intelligence and CA SOI reports installed before configuring reporting. For more information, see the *Implementation Guide*.

As an administrator, you enable the report functionality and configure CA SOI to access the BusinessObjects report server.

You can also configure CA SOI to automatically synchronize CA SOI and the BusinessObjects users. User synchronization lets you add or remove a user in the Operations Console and have CA SOI automatically add or remove the user from CA Business Intelligence access.

Follow these steps:

1. Click the Administration tab on the Dashboard.
2. Click the plus sign (+) next to CA Service Operations Insight UI Server Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Report Configuration.
5. Enter the appropriate information in the following fields and click Save:

   Note: Refer to your Installation Worksheet in the CA Business Intelligence section for these values.

   Report Server

   Specifies the server name where CA Business Intelligence and the CA SOI Reports component are installed.

   Report Port

   Specifies the port number on which the report server is listening. If you used the default port when installing CA SOI, it is set to 8080 for report servers using Tomcat. If you are using an IIS server as the report server, the port can be set to 80 only. If you try to use a port other than 80 for the IIS report servers, you cannot save the settings on this page.

Report URL

Specifies one of the following URLs for the InfoView interface on the report server:

- (Report servers using IIS) /InfoViewApp/logon.aspx
- (Report servers using Tomcat) /InfoViewApp/logon.jsp

Enable SSL

Specifies whether to use SSL to communicate with the specified report server. Select this check box if the report server is configured to use SSL.

CMS Port

Specifies the BusinessObjects CMS Server port. The CMS communicates with other BusinessObjects Enterprise servers through the specified port.

Default: 6400. If you leave the field blank, CA SOI uses the default value.

N-tiered SAP BusinessObjects Enterprise Configuration

Specifies whether to use an N-tiered BusinessObjects Enterprise, which is configured to deploy on multiple servers. In this case, the Web Tier (InfoViewApp Server) and Intelligence Tier (CMS Server) can be on different servers.

Intelligence Tier Server

Specifies the Intelligence Server (CMS Server) for adding and deleting users.

Enable automatic additions to the CA Service Operations Insight report group

Specifies whether users added or removed from the Operations Console are automatically added to or removed from BusinessObjects and the SOI Reports group on the report server.

Notes:

- If you create users in the Operations Console and then select this option, the users are added to the SOI Reports group after you restart the CA SAM Application Server service.
- The users that are automatically added to the BusinessObjects SOI Reports group are assigned a temporary password of SAM*userid* (for example, if the user name is jeromeG, the password is also SAMjeromeG). The first time the user logs into BusinessObjects, the user is prompted to change the password. The new password must conform to the restrictions defined on the report server.
- Do not use the users in the CA SOI Super Users group (including the "samuser" super user) to run reports.

- Do not use the BusinessObjects administrator user (Administrator by default) to run reports.
- If you configure the automatic addition of CA SOI users for reports, do not create a user in CA SOI with the same name as the BusinessObjects administrator user (Administrator by default). The same name can cause problems with the BusinessObjects administrator user.

Enable automatic removal from the CA Service Operations Insight report group

Specifies whether members of the SOI Reports group (on the BusinessObjects report server) are automatically deleted from the group and BusinessObjects user list when they are deleted using the Operations Console.

Note: Users that are removed using this functionality are deleted from *all* user groups—not only the SOI Reports group.

User Name/Password

Specifies a user with administrator privileges on the CA Business Intelligence report server. This user must have the right to create users on the CA Business Intelligence report server.

Note: If you configured CA Business Intelligence with LDAP, you have an enterprise user in CMC.

6. Click Save, then click Refresh at the top of the page.

   The Reports link becomes active at the top right of the interface. Click the link to access the reporting interface on the CA Business Intelligence report server.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

Configure Metric Definition

As an administrator, you configure the service health definition to determine the health level that determines when a service is down.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to the CA Service Operations Insight UI Server Configuration option.
3. Click Metric Definition Configuration.
4. Select a health level that determines when a service is down from the drop-down list and click Save.

Note: If the Administration tab changes do not save or the fields clear when you click Save or Test, adjust your browser settings. One of the following actions should solve the problem:

- Add the CA SOI URL to your trusted sites and lower the privacy to accept all cookies. For more information about trusted sites and privacy settings, see your browser documentation.
- Add the domain name of the CA SOI UI Server and SA Manager (for example, company.com) to the privacy managed websites and set to Allow. For more information about managing privacy settings, see your browser documentation.

Configure USM Web View Integration

As an administrator you configure the USM Web View URL setting, which enables the USM Web View link on the Dashboard. The URL also enables use of the $[USM Web View URL] runtime token to invoke USM Web View as part of an escalation action

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI UI Server Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click USM Web View Configuration.
5. Complete the server and port fields. Unless you performed a custom installation, USM Web View resides on the system where you installed the UI Server.
6. Click Save.
7. Restart the CA SAM Application Server service for the change to take effect.

Launch Web Server Scripts

As an administrator, you enable launching of web server scripts. This functionality was previously disabled due to a security issue.

Follow these steps:

1. Locate and open the following file on the UI Server:

   SOI_HOME\jsw\conf\soi-user-interface.conf

2. Add the following entry:

   ```
   wrapper.java.additional.22=-DALLOW_WEB_SERVER_SCRIPT=1
   ```

3. (Optional) Add a parameter to allow the script execution in a specified folder only:

   ```
   wrapper.java.additional.23=-DWEB_SERVER_SCRIPT_PATH="Path"
   ```

   Path

   > Specifies the full path of a folder on your UI Server.
   >
   > **Example:** "C:/SOIUI/serverscripts"

   Note: The additional parameters numbers, 11 and 12, assume that, before this change, the last additional parameter was 10. In general, you increase each new parameter number by one.

4. Restart the CA SAM User Interface Server service to activate the change.

   Note: If WEB_SERVER_SCRIPT_PATH is configured, the script must be in the specified folder (or one of its subfolders).

Chapter 4: 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 29).

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.

Introduction to the Operations Console

The Operations Console is the user interface that provides most of the CA SOI functionality. The Operations Console is where you define and maintain services, create user groups and assign them access privileges, create event policies and alert queues, manage alerts that warn about fault conditions, and more.

The Operations Console is a unified alert console with features that let you centralize the management of all actionable conditions within a single interface. This provides a single view for your operations teams to consider the conditions requiring attention, and a single escalation point for those conditions to reduce the overhead associated with alarm management across multiple domains and to help ensure consistent policies are always applied.

The Operations Console is comprised of three panes that display information about your services, customers, users, and alerts: the Navigation pane, the Contents pane, and the Component Detail pane. The information displayed in each of the panes depends on the items selected in the other panes. Selected items in the Navigation pane determine what is displayed in the Contents pane. Likewise, selected items in the Contents pane determine the information shown in the Component Detail pane.

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 services, alerts, customers, or users, depending on the tab 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 98) 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 100).

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.

When you select Users, the Contents pane displays the following tabs that contain information about users:

Users List

Lists user name and type information for users in the group selected in the Navigation pane.

Privileges

Lists access privileges that you can assign to user groups.

Service Access

Lists services to which the selected user group has access.

Alert Queues Access

Lists alert queues to which the selected user group has access.

When you select Customers, the Contents pane displays the following tabs that contain information about customers:

Alerts

Shows alerts for the customer (or sub-customer) selected in the Navigation pane. Only alerts from the services that are assigned to the selected customer are shown in the tab. Select an alert to display details about it in the Component Detail section. For example, select the Customer Impact tab to view all the customers that the selected alert is impacting.

Services

Displays services associated with the customer (or sub-customer) selected in the Navigation pane.

List

Displays a list of sub-customers for the selected customer.

Information

Displays information (such as customer name, priority, identity, and description) about the selected customer (or sub-customer).

Component Detail Pane

The Component Detail pane in the lower right of the Operations Console displays detailed information about alerts, resources, services, service impact, customer impact, users, or user groups. 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 selections in the Contents pane and access privileges:

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, role-based security for user groups, associated escalation policies, connector status, and granularity) 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. You can set service or CI properties such as Operational Mode, Priority, Location, maintenance schedules, and access privileges from the Information tab.

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 from the List, Services, or Topology tab.

USM Notebook

Shows the USM properties of the CI from the perspective of all data sources and the reconciled set of USM properties. When cross-type correlation occurs, you can see the USM properties for all correlated types, not just the reconciled sheet type, on the USM Notebook tab. To view USM properties for a projection sheet of a different CI type than the reconciled sheet, select that type from the Type drop-down list on the USM Notebook tab. Entries exist for the reconciled sheet, the CA SOI CI projection sheet, and any other projection sheet of different types.

SOI Properties

Shows the CA SOI-specific properties of the selected CI. These properties are unique values that CA SOI uses to identify each entity.

Status Bar

The Status bar at the bottom of the Operations Console provides status information about the current CA SOI connection. The Status bar contains the following buttons:

🔌

Opens the Connection Status dialog, which displays the current connection status of all CA SOI components (SA Manager, UI Server, connectors, and so on). The Connection Status dialog also displays a connection log and an Open Consolidated Error Log button, which opens the consolidated samerror.log file in a web browser.

This button displays a green icon to indicate that all components have a connected status. The button displays a red icon to indicate that one or more components have lost connection.

Note: For the User Management Service, even if CA EEM displays without a version number in the Description column, it does not indicate a problem with the product. The service still displays as Online.

💬

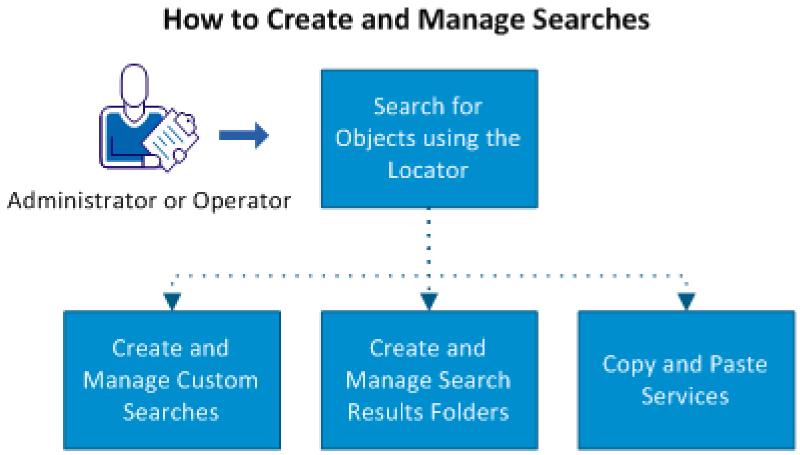
Opens the Messages dialog, which displays any new messages from the administrator.

If the SA Manager connection is lost, the Status bar also displays your user name, the login server, and an alert message.

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 87).
2. (Optional) Create custom searches (see page 89).
3. (Optional) Create search result folders (see page 90).
4. (Optional) Copy and paste services (see page 90).

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 89) 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 98).

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 90).
   - 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

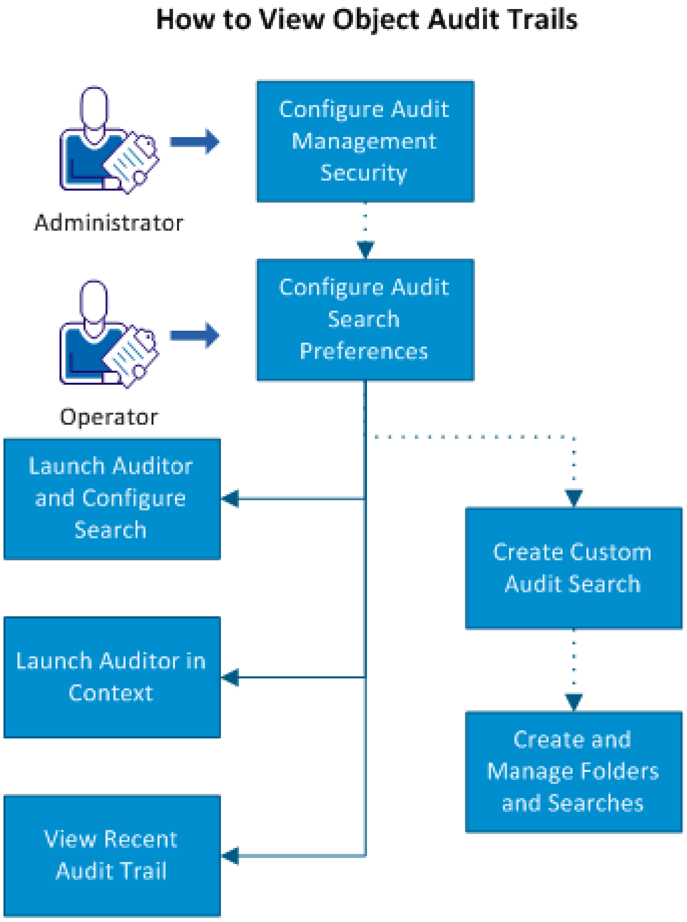
As an administrator or an operator (with access privileges), you can view the audit trail for objects (such as services, CIs, alerts, connectors, and so on). An audit trail shows updates to a selected object as tracked in the CA SOI database.

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 93).
2. (Optional) Configure your audit search preferences (see page 93).
3. Perform any of the audit trail searches:
   - Launch the Auditor and manually enter the audit trail search parameters. (see page 93)
   - Launch the Auditor in the context of an object (see page 94).
   - View the recent audit trail for an object (see page 94).
4. (Optional) Create custom audit trail searches (see page 94).
5. (Optional) Create and manage your custom audit trail search folders and searches (see page 95).

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 (see page 112) 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 86) 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 95) 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 96)
- Dock and undock panes (see page 96)
- Clone (copy) panes (see page 97)

- Set display preferences (see page 98), 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 100)
- Navigate (see page 100), collapse, or expand (see page 104) 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 87).

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 100).

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 21).

(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 5: Configuring Role-Based Security

This section describes how to create and configure users and user groups and set access privileges to services, alert queues, customers, and other various CA SOI features.

This section contains the following topics:

How to Configure Role-Based Security

As an administrator, you manage users and user access privileges to services, alert queues, customers, and CA SOI features.

CA SOI integrates with CA EEM to manage the user authentication and configure the resource access. CA SOI adds users that are defined in CA EEM to product-specific user groups with configurable privileges and access levels.

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.

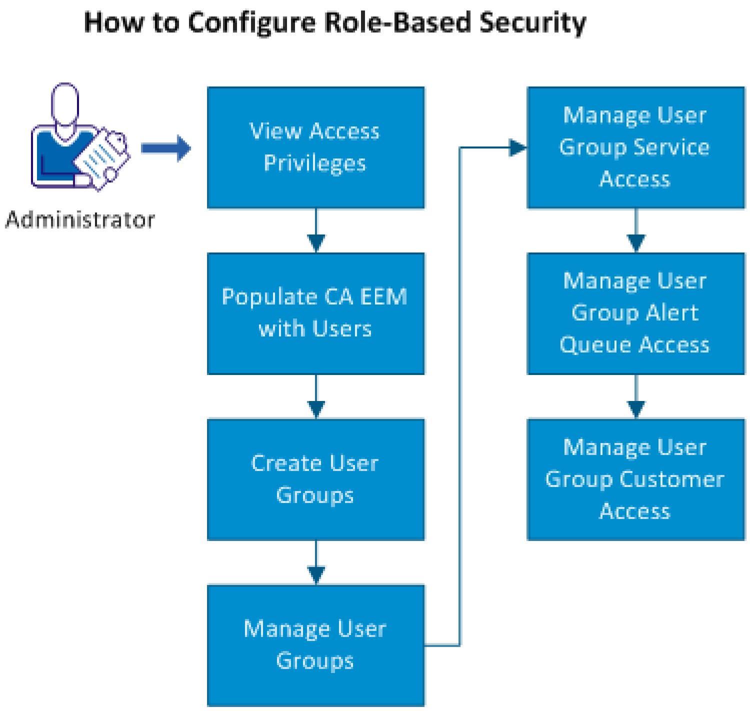
Note: For more information about installing CA EEM to integrate with CA SOI, see the *Implementation Guide*. For more information about the CA EEM functionality, see the CA EEM documentation. The documentation is provided on the CA SOI bookshelf.

You create and use different administrative users to manage the product. The only user that is defined in CA SOI before you configure the role-based security is the user that was created during the installation ("samuser" by default). The samuser is a super user with all privileges. Use samuser for the initial login and to configure user access. You can also use samuser if CA EEM connectivity is lost. Otherwise, you create and use a different administrative user for managing the product. The samuser has limitations that prevent it from being a long-term management solution, including the following limitations:

- It cannot set persistent Operations Console preferences.
- It cannot run reports.
- It cannot log in to USM Web View.

For non-administrator user groups, you manage the user group access to services, alert queues, and customers.

Use this scenario to guide you through the process:


How to Configure Role-Based Security
Administrator
View Access Privileges
Populate CA EEM with Users
Create User Groups
Manage User Groups
Manage User Group Service Access
Manage User Group Alert Queue Access
Manage User Group Customer Access

1. View the access privileges (see page 109) for the current user groups.
2. Populate the users in CA EEM (see page 110) by either creating or importing users.
3. Create the user groups (see page 112), assign privileges, add users to the user group, and define users in BusinessObjects for report access.
4. Manage the user groups in CA SOI (see page 115) to define user group privileges to give the appropriate level of access to each group role.
5. Manage the user group access to services (see page 117).
6. Manage the user group access to alert queues (see page 120).
7. Manage the user group access to customers (see page 122).

View Access Privileges

CA SOI lets you define which user groups can view services and associated data and can manage alerts, CIs, UI access, and users. The Privileges tab in the Operations Console Contents pane lists the privileges and describes each one.

Follow these steps:

1. Start the Operations Console.
2. Click the Users tab in the Navigation pane.
3. Click a user group.
4. Click the Privileges tab, Service Access tab, Alert Queues Access tab, or Customer Access tab in the Contents pane.

   The access privileges for the selected user group appear.

Predefined User Groups

CA SOI provides several default user groups with access to different CA SOI components and functionality. You can view the default access privileges (see page 109) in the Operations Console User tab.

Administrators

Identifies users that have access to all [assign the value for SOI in your book] functionality.

Operators (read-only)

Identifies users that view most CA SOI information such as alerts, customers, and services, but cannot modify information. These users cannot view the Dashboard Administration tab.

Operators (read-write)

Identifies users that can view and modify most CA SOI information such as alerts, customers, and services, but cannot modify information. These users also have access to the Dashboard Administration tab.

Super Users

Identifies the default "samuser" user that has access to all CA SOI functionality. You use the "samuser" super user until you have created other administrator users or if CA EEM problems prevent logging in as another administrator user. You cannot modify the privileges of the Super Users group.

Populate CA EEM with Users

As and administrator, you populate CA EEM with users. You can import users (see page 110) from an external directory such as Active Directory or manually create users and store them to an internal database.

Import Users

You can import users from an external directory into CA EEM for use in CA SOI.

Follow these steps:

1. Open CA EEM as follows:

   - Enter the following URL in your web browser: http://*eem_server_name*:*port_number*/spin/eiam/eiam.csp. The default port number for CA EEM is 5250. Refer to the CA EEM section on the Installation Worksheet that you filled out during installation for these values. For more information, see the *Implementation Guide*.

   - Select Start, Programs, CA, Embedded Entitlements Manager, EEM UI on the CA EEM system.

   The CA EEM login page opens.

2. Select < Global > from the Application drop-down list.

3. Enter the CA EEM Administrator user name (EiamAdmin) and password and click Log In.

4. Click the Configure tab.

5. Select the EEM Server (r8.x) or User Store (r12.x) from the submenu.

6. Click Global Users/Global Groups (r8.x) or Group Configuration (r12.x) in the left pane.

7. Select *one* of the following options in the right pane:

   - Store in internal datastore

   - Reference from an LDAP Directory (r8.x) or Reference from an external LDAP Directory (r12.x)

   - Reference from CA SiteMinder

   Note: For information about the page fields, see the CA EEM online help.

8. Click Save.

   One of the following icons appears:

   ✅

   Success icon (green circle icon with a white check mark)

   Indicates that both the External directory bind and the External directory data were loaded successfully.

   ⚠

   Warning icon (yellow triangle with red exclamation point)

   Indicates that the External directory data is still loading. Allow additional time for the process to complete.

   ❌

   Error icon (red circle with white x)

   Indicates that the External directory bind failed. Check the inputs for each of the parameters and try again.

If you selected to have CA EEM reference an external directory and the operation was successful, the CA EEM integration is complete. You can start adding users to CA SOI.

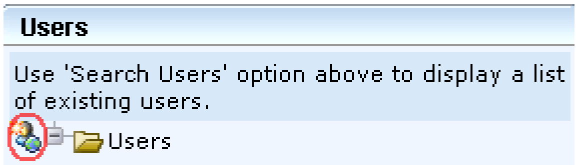
If you selected to store users in an internal datastore, you now create your users within CA EEM.

Create Users

You can create users directly in CA EEM for use in CA SOI. Later, you add these users to user groups in CA SOI

Follow these steps:

1. Select the Manage Identities tab.
2. Select Users from the submenu.
3. Click the New User icon in the Users pane (lower left):



Users

Use 'Search Users' option above to display a list of existing users.

Note: When this icon is not visible, it means that users are being imported from external sources, such as Active Directory.

4. Complete the user details in the New User pane and click Save in the New User pane on the right side. At a minimum, enter a Name (alphanumeric characters only) and a Password for the user.

   A message at the top of the User panel confirms that the user was created.

5. Repeat Steps 3 - 4 for each new user.

   The users are created.

You can now add created users to groups and configure access privileges in CA SOI.

Create User Groups

As an administrator, you create user groups to define access to [assign the value for SOI in your book] features.

Define a User Group and Group Privileges

You assign feature privileges, service access, and alert queue access at the group level. A user group defines the access level for users in the group.

You can use the predefined groups (see page 109) that are provided with CA SOI, customize the predefined groups, or you can create your own user groups to use more specialized roles. Adding privileges during group creation defines what features, services, alert queues, and so on are available to users in the group.

Note: By default, each user group has access to *all* services and alert queues, but each user group has different feature privilege sets.

Follow these steps:

1. Log in to the Operations Console:
   - If you have not defined any administrator users, log in as the default user defined during installation ("samuser" user by default). Refer to the Installation Worksheet in the *Implementation Guide* for credentials.
   - If you have defined an administrator user, log in as that administrator.
2. Click the Users tab in the left pane.
3. Click the New User Group icon 👥.
4. Enter a name for the group, and select the existing group to use as a template for assigning privileges in the Privilege Set drop-down list.

   You must select either Operator or Administrator as a starting point for assigning group privileges.

A list of privileges appears that are available for the privilege set you selected. Privileges are divided into folders corresponding to the functional areas of the product. Each privilege contains a detailed description, and all privileges are disabled by default.

Select the minimum privileges necessary for the group to manage their services, alert queues, and customers that their job function requires.

5. Expand all privileges, click the check boxes next to the privileges to enable for the group, and click OK.

   Note: Select the Enabled check box in a parent folder to enable its children automatically.

   The group is defined. The privileges appear on the Privileges tab in the right pane, where you can click Add/Remove to modify the privileges.

Add Users to a Group

You add a user created in CA EEM to a group that has the privileges appropriate for their organizational role. A user can belong to one group only.

Note: Users that are created or imported into CA EEM are not added to a default user group in CA SOI, so you must add each user manually.

Follow these steps:

1. Open the Operations Console and click the Users tab in the left pane.
2. Expand the group to which to add users, and click the New User icon 👤.
3. Click 'All users' or 'Users by filter'.

   Note: When a large number of users exists, the list shows a truncated amount. Use filters in this case to find the users that you need.

   If you clicked 'Users by filter', complete the filter criteria.
4. Click OK.

   The Select Users dialog opens with users defined in CA EEM or available through CA EEM if integrating with an external directory.
5. Select one or more users and click OK.

   The user name appears beneath its group in the left pane. Users immediately inherit all privileges, access rights, and preferences that are assigned to the group.

   Note: When you select a group in the left pane and click the Users List tab in the right pane, users in the group appear in a table in the right pane. From there you can delete, copy, and paste users and export the list in spreadsheet format.

Define Users in BusinessObjects

Before users can use the InfoView reporting functionality that is provided with CA Business Intelligence, perform the following tasks:

- You can configure CA SOI to automatically synchronize its users and report users. If you select the synchronization option, users added to CA SOI user groups in the Operations Console are automatically added to BusinessObjects and the SOI Reports group.
- You can manually define users in BusinessObjects for running reports and add them to the SOI Reports group as described in this section if you did not synchronize report users.

When creating report users, consider the following restrictions:

- Do not use the CA SOI administrator user ("samuser" user by default) to run reports.
- Do not use the BusinessObjects administrator user (Administrator by default) to run reports.
- If you configure the automatic addition of CA SOI users for reports, do not create a user in CA SOI with the same name as the BusinessObjects administrator user (Administrator by default). Identical names can cause problems with the BusinessObjects administrator user.

Follow these steps:

1. Perform one of the following tasks to open the BusinessObjects Central Management Console:
   - Enter the following URL in the Address field of your Web browser: http://*businessobjects_server_name*:*port*/CmcApp/logon.faces
   - **Note:** See the CA Business Intelligence section on the Installation Worksheet you completed during CA SOI installation for these values. See the *Implementation Guide.*
   - Click Start, Programs, BusinessObjects XI 3.1, BusinessObjects Enterprise, BusinessObjects Enterprise Central Management Console.
2. Log on using the BusinessObjects Administrator account.

   The BusinessObjects Central Management Console opens.
3. Click the Users and Groups option in the Organize area.
4. Click User List.
5. Click the New User icon .
6. Enter a user name and password for the user and click Create & Close.

   The user appears in the user list.

7. Double-click the new user entry.

   The Properties page opens.

8. Click Member of and then Join Group.

9. Select SOI Reports in the Available groups area, click the right arrow button to move it to the right side, and click OK.

   The user can now run CA SOI reports.

Manage User Groups

As an administrator, you can modify user group privileges, preferences, and export or delete user groups.

Modify Group Privileges

You can change the privileges that are assigned to user groups when group roles change.

Note: The Administrators group must have all privileges, so do not modify privileges for that group. You cannot modify the Super Users group privileges.

Follow these steps:

1. Open the Operations Console and click the Users tab in the left pane.

2. Select a group.

3. Click the Privileges tab.

4. Click Add/Remove.

5. Enable or disable privileges using the check boxes and click OK.

   The changes take effect and are reflected in the Privileges tab.

Edit User or Group Preferences

You can customize the product look and feel for an individual user or an entire user group. You can control the default settings for features such as field fonts, default alert filter, and Modeler settings. You can also set whether user groups can modify the values.

Follow these steps:

1. Right-click the user or group in the Users tab and select Set Preferences.

2. Set preferences (see page 98) for the user or group.

3. Select the check box in the Locked column to prevent users from modifying specific preferences.

   Note: Privileges that are locked at the group level are not available when setting preferences for a user in that group.

4. Click OK.

   The preferences are saved.

Export the Users in a Group

You can export user definitions in a group to a CSV file and import that file to spreadsheet software.

Follow these steps:

1. Open the Operations Console and click the Users tab in the left pane.
2. Select a user group.
3. Click Export in the right pane.
4. Enter a file name, select a path, and click Save.

Delete a User or Group

You can delete a user or user group that is no longer involved with CA SOI. CA EEM only controls user authentication. If you delete a user in CA EEM, you cannot log in to CA SOI with those user credentials. However, the user does not disappear from the Operations Console until you also delete the user from CA SOI.

Note: You cannot delete the predefined user ("samuser" user by default) or any of the predefined groups.

Follow these steps:

1. Open the Operations Console and click the Users tab in the left pane.

   A list of user groups appears.

2. Expand the tree if necessary, select a user or group, and click Delete ✕.

   The user or group is removed.

Manage User Group Access to Services

As an administrator, you grant user groups access to service models. Each user group can require access to different services based on their role. For example, considering the following users and service requirements:

- Service owners see only the services for which they are responsible.
- Customers see only the services they consume.
- IT managers see all services because they are responsible for maintaining the health and availability of all services in the data center.

Before you can grant user group access to the service models, you model services. For procedures on service modeling, see the *Service Modeling Best Practices Guide*.

Note: The Administrators group must have all privileges, so do not modify privileges for that group.

Example: User Group Access to Services

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

Services: Sales, Finance, Operations

User Groups: Group1, Group2, Group3, Admin

The following table shows sample User Groups and their access to available services that are set by the system administrator:

User Group	Service Access
Group1	Sales, Operations
Group2	Finance, Operations
Group3	Operations
Admin	All Services

The following table shows the User Groups and what each user group sees on the Services tab based on their service access:

User Group	Sees on the Services Tab
Group1	Sales, Operations
Group2	Finance, Operations
Group3	Operations

User Group	Sees on the Services Tab
Admin	All Services

Service and Sub-Service Access Situations

The following table shows various non-administrator user group permission access to services and its subservices and which services and subservices the user group sees.

The Example column uses the following service names: A, B, and C with each service having the subservice D.

User Group Service Permission	User Group Subservice Permission	Example	User Group Sees*	Notes
Not set	Not set	Access permissions are not set for services A, B, C, or subservice D	No services or subservices	
Allowed	Not set	Access permissions are set to Allowed for services A, B, C but not set for subservice D	Services A, B, C and subservice D	If service access is set to Allowed, then all subservice access is automatically set to Allowed
Allowed	Not Allowed	Access permissions are set to Allowed for services A, B, C and set to Not Allowed for subservice D	Services A, B, C	CA SOI does not support this situation. The user group sees services A, B, C and subservice D.
Not Allowed	Allowed	Access permissions are set to Allowed for services A and B and subservice D, but set to Not Allowed for service C.	Services A, B and subservice D under services A and B only	
Not Allowed for any parent	Allowed	Access permissions are set to Not Allowed for services A, B, C and set to Allowed for subservice D.	Subservice D	CA SOI does not support this situation. The user group does not see any service or subservice. However, you can create a placeholder parent service with subservice D and you can set both access permissions to Allowed.

* This column indicates what the user group expects to see. Unsupported situations are noted in the comments column and what the user group actually sees in CA SOI.

Grant User Group Access to Services

You can grant a user group access to any or all services defined in CA SOI.

Follow these steps:

1. Click the Users tab then select a user group in the Navigation Pane.
2. Click the Service Access tab in the Contents pane.
3. Perform one of the following tasks:
   - Click Allow All Access to allow users in the user group access to all services and click Yes when the confirmation dialog opens.
   - Click Add/Remove and select the services available from the Available Services pane and move them to the Services Assign to this User Group Pane, then click OK.

   The user group service access is updated and appears in the Contents pane.

Remove User Group Access to Services

You can revoke a user group access to any or all services defined in CA SOI.

Follow these steps:

1. Click the Users Tab then select a user group in the Navigation Pane.
2. Click the Service Access tab in the Contents pane.
3. Perform one of the following tasks:
   - Click Remove All Access to disallow users in the user group to access *any* services and click Yes when the confirmation dialog opens.
   - Click Add/Remove and select the services that are allowed in the Services Assigned to this User Group panel and move them to the Available Services panel, then click OK.

   The user group service access is updated and appears in the Contents pane.

Manage User Group Access to Alert Queues

As an administrator, you can permit or revoke user group privileges to all alert queues or specific alert queues.

You can think of alert access in several layers: user groups, alert queue access, and customers. In CA SOI, service access takes precedence over alert queue access. Therefore, if an alert is on a service that a user does not have access to, the alert does not appear in any alert queue that the user can see. Five users can view the same alert queue and see five different sets of alerts, depending on their user group service access privileges.

Note: The Administrators group must have all privileges, so do not modify privileges for that group.

For procedures about working with alert queues, see the *Event and Alert Management Best Practices Guide*.

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.
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.

Grant User Group Access to Alert Queues

You can grant a user group access to any or all alert queues defined in CA SOI.

Follow these steps:

1. Click the Users tab then select a user group in the Navigation Pane.
2. Click the Alert Queues Access tab in the Contents pane.
3. Perform one of the following tasks:
    - Click Allow All Access to allow users in the user group access to all alert queues and click Yes when the confirmation dialog opens.
    - Click Add/Remove and select the alert queues available from the Available Alert Queues pane and move them to the Alert Queues Assign to this User Group Pane, then click OK.

    The user group alert queue access is updated and appears in the Contents pane.

Remove User Group Access to Alert Queues

You can remove a user group access to any or all alert queues defined in CA SOI.

Follow these steps:

1. Click the Users Tab then select a user group in the Navigation Pane.
2. Click the Alert Queues Access tab in the Contents pane.
3. Perform one of the following tasks:
   - Click Remove All Access to disallow users in the user group to access any alert queues and click Yes when the confirmation dialog opens.
   - Click Add/Remove and select the alert queues that are allowed in the Alert Queues Assigned to this User Group panel and move them to the Available Alert Queues panel, then click OK.

   The user group service access is updated and appears in the Contents pane.

Manage User Group Access to Customers

As an administrator, you can permit or revoke user group privileges to all customers or specific customers.

For more information about customers, see Working with Customers.

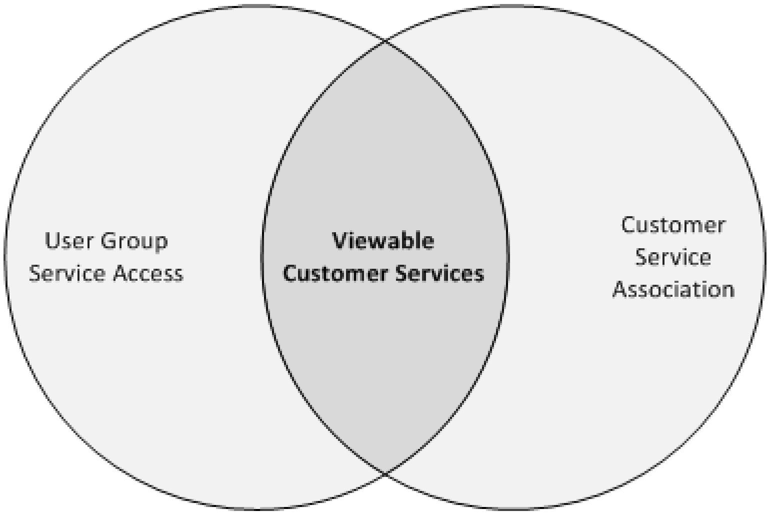
Example: User Group Access to Customers

The following example shows how both service access and customer access limit the availability of services to user groups.

For a user group to see customer services, the user group must meet the following requirements:

- The user group must have access privileges to view the services.
- The services must be associated with a customer.
- The user group must have access privileges to the customer.

The following graphic shows that the viewable customer services is the intersection between the user group service access and the customer service association. User Group Service Access includes all services that the user group has access privileges to view. Customer Service Association includes all services that are assigned to a customer.



The user group sees the Viewable Customer Services on the Operation Console Customer tab. The user group sees the User Group Service Access (all services to which they have access) on the Services tab.

For example, an administrator defined the following items in CA SOI:

User Groups: Operator1, Operator2, Operator3, Admin

Services Available: Finance, Operations, Sales

Customers: RegionUS, RegionEU

Customer Priorities: RegionUS=8, RegionEU=10

The administrator assigns the RegionEU customer a higher priority than RegionUS.

Customer Service Access: The administrator assigns the following services to the customers:

> **Region1:** Sales, Finance, Operations
>
> **Region2:** Finance, Sales

The following table shows the user groups, service access, and customer assignments that are set by the CA SOI administrator:

User Group	Service Access	Customer Assignment
Operator1	Operations, Sales	Region1
Operator2	Finance, Operations	Region2
Operator3	Operations	None
Admin	All customers	All customers

The following table shows the user groups and what each user group sees on several Operations Console tabs, based on the user group service and customer access:

User Group	In Services Tab	Services Tab: Impacted Customers Tab	In Customers Tab	Customers Tab: Services Tab
Operator1	Operations, Sales	Region1	Region1 only	Operations, Sales
Operator2	Finance, Operations	Region2	Region2 only	Finance
Operator3	Operations	None	None	None
Admin	All services	All customers	All customers	All service associations

The Operator1 user group sees only Operations and Sales in the Customers Tab. Operator1 is associated with the Region1 customer, which has service access to Finance, Operations, and Sales. However, the Operator1 user group is limited to only Operations and Sales service access; therefore, Operations and Sales are the only services Operator1 can see.

The Operator2 user group sees only Finance services in the Customers tab. The Operator2 user group has access to only Finance and Operations services and its customer association (Region2) has access to only Finance and Sales. Therefore, Operator2 is limited both by its user group access and by its customer access to view Finance only.

The Operator3 user group does not see any services. Although Operator3 has service access to Operations, the Operator3 user group is not associated with a customer (Region1 or Region2). Therefore, Operator3 cannot view any services associated with either customer.

The Admin user group can view all services and customers; therefore, the Admin user group sees all services.

Alert Queues: QueueUS, QueueEU, QueueSA

Customer and Subcustomer Access Situations

The following table shows various non-administrator user group permission access to customers and its subcustomers and what the user group sees.

The Example column uses the following customers and subcustomers:

Customers: Region1 and Region 2.

Subcustomers:

Region1: HR1

Region2: HR2

User Group Customer Permission	User Group Subcustomer Permission	Example	User Group Sees*	Notes
Not set	Not set	Access permissions are not set for customers Region1, Region2 and are not set for subcustomers HR1, HR2	No customers or subcustomers	
Allowed	Not set	Access permissions are set to Allowed for customer Region1 but not set for subcustomer HR1	Customer Region1 and subcustomer HR1	If customer access is set to Allowed, then all subcustomer access is automatically set to Allowed.

User Group Customer Permission	User Group Subcustomer Permission	Example	User Group Sees*	Notes
Allowed	Not Allowed	Access permissions are set to Allowed for customer Region1 but set to Not Allowed for HR1	Customer Region1	CA SOI does not support this situation. The user group sees customer Region1 and HR1.
Not Allowed	Allowed	Access permissions are set to Not Allowed for customer Region1 but set to Allowed for HR1	Subcustomer HR1 as top-level customer	

* This column indicates what the user group expects to see. Unsupported situations are noted in the comments column and what the user group actually sees in CA SOI.

Grant User Group Access to Customers

You can grant a user group access to any or all customers defined in CA SOI.

Follow these steps:

1. Click the Users Tab then select a user group in the Navigation Pane.
2. Click the Customer Access tab in the Contents pane.
3. Perform one of the following tasks:
   - Click Allow All Access to allow users in the user group access to all customers and click Yes when the confirmation dialog opens.
   - Click Add/Remove and select the customers available from the Available Customers pane and move them to the Customers Assigned to this User Group Pane, then click OK.

   The user group customer access is updated and appears in the Contents pane.

Remove User Group Access to Customers

You can remove a user group access to any or all customers (and sub-customers) defined in CA SOI.

Follow these steps:

1. Click the Users Tab then select a user group in the Navigation Pane.
2. Click the Customer Access tab in the Contents pane.
3. Perform one of the following tasks:
   - Click Remove All Access to disallow users in the user group to access any customers and click Yes when the confirmation dialog opens.
   - Click Add/Remove and select the customers that are allowed in the Customers Assigned to this User Group panel and move them to the Available Customers panel, then click OK.

   The user group service access is updated and appears in the Contents pane.

Enable Guest User Account

As an administrator, you can enable a guest user that lets users access the CA SOI Dashboard without login credentials. The feature is disabled by default.

Follow these steps:

1. Locate and open the following file on the UI Server:

   SOI_HOME\SamUI\webapps\sam\server-config.xml
2. Add the following entry as the second to last line (below the </manager> line):

   ```
   <guest-username>guest</guest-username>
   ```
3. Restart the UI Server service.

   The patch adds user "guest" to the "Operators (read-only)" user group. You can adjust the access privileges as necessary.

   Your users use the following URL to access the CA SOI Dashboard as the guest user:

   `http://UI_server:7070/sam/guest.jsp`

Support for Common Access Card and Smartcard Authentication Using Client Certificates

As an administrator, you can enable Common Access Card (CAC) and Smartcard authentication using client certificates. You can use your client certificates to authenticate users in CA SOI. Only authorized users can access the environment (for example, access to the web services). To enable the client certificates on the SA Manager, configure the server.xml file available at SOI_HOME\tomcat\conf. To enable the certificates on the UI Server, configure the server.xml file available at SOI_HOME\SamUI\conf.

Enable Client Certificate Authentication

To enable the client certificate authentication in CA SOI, configure the server.xml file.

Follow these steps:

1. Navigate to the SOI_HOME\tomcat\conf folder on the SA Manager.

   Note: For the UI Server, navigate to the SOI_HOME\SamUI\conf folder.

2. Open the server.xml file in a text editor.

3. Locate the clientAuth parameter in the file.

4. Change the value of the parameter to *true.*

   An example snippet is as follows:

   ```
   <Connector port="7493" maxHttpHeaderSize="8192" maxThreads="150"
   minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
   disableUploadTimeout="true"
   acceptCount="100" scheme="https" secure="true" keystoreFile="conf/ssa.jks"
   keystorePass="samuser"
   ciphers="SSL_DHE_DSS_WITH_RC4_128_SHA,SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_R
   C4_128_SHA,TLS_KRB5_WITH_RC4_128_MD5,TLS_KRB5_WITH_RC4_128_SHA,TLS_ECDH_ECDSA
   _WITH_RC4_128_SHA,TLS_ECDH_RSA_WITH_RC4_128_SHA,TLS_ECDHE_ECDSA_WITH_RC4_128_
   SHA,TLS_ECDHE_RSA_WITH_RC4_128_SHA,SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DH_RS
   A_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3D
   ES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_FIPS_WITH_3DES_EDE_CBC_S
   HA,TLS_KRB5_WITH_3DES_EDE_CBC_MD5,TLS_KRB5_WITH_3DES_EDE_CBC_SHA,TLS_ECDH_ECD
   SA_WITH_3DES_EDE_CBC_SHA,TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECDSA_W
   ITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_DSS_WITH_AES
   _128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SH
   A,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_
   AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_2
   56_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SH
   A,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,T
   LS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA"
   clientAuth="true" SSLProtocol="TLSv1"/>
   ```

5. Save the file.

Chapter 6: Understanding Service Modeling

This section provides concepts to help you understand service modeling and related features, such as: escalation policy, service discovery, and service-level agreements. For related procedures, see the *Service Modeling Best Practices Guide*.

This section contains the following topics:

Service Modeling Terminology and Concepts

The topics in this section provide service modeling terminology and concepts.

Service

The concept of a service model, or service, is central to CA SOI. A *service* typically consists of several CIs, which you can group to represent, for example, web server farms or clusters. Services can also contain *subservices*, which are subordinate service models. Subservices are previously created services that are reused as building blocks of another service. Service models typically represent high-level abstract entities like a web-based retail transaction service, an application server service, a printing service, or a routing service. You can define any type of service 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 as an infrastructure alert, impacts the business. Consider a managed resource such as a router. You can accurately, but narrowly, define it 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 that router are likely compromised also. A router can be associated with other network devices such as switches or servers, which are associated 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. These relationships help you capture how one CI 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. You can also combine it with other configuration items (CIs) 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 can itself form part of still higher-level services such as email or Blackberry.

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 working with a service owner can select configuration items that are discovered through integration with the domain managers. The operator can then create relationships among those configuration items. Similarly, if a service model 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. This ability provides a powerful mechanism to leverage your existing investment.

Service Concepts

The concepts in this section help you understand how CA SOI monitors services and calculates service impact. The following entities play a role in impact calculation:

- Alert and CI conditions from domain managers display as severity (see page 21) in the appropriate CI and alert.
- CI severity affects related CIs in service models according to propagation type and policy (see page 135) settings.
- If propagation settings cause severities to propagate, the multiplied value of severity and significance (see page 137) determines the related CI impact and, ultimately, service impact (see page 137).

Relationships

Relationships in a service model show how CIs are linked to form the service topology. A relationship between linked objects has a semantic (name or type, for example 'HasAccessTo') and a propagation type (for example, 'Custom'). CA SOI relationships correspond to instances of USM BinaryRelationship type. If you import a service from a connector, its relationships in the domain manager are mapped to USM relationships.

You can assign relationships to every link between objects in a service model. To assign relationships, you select the appropriate propagation type and then select a relationship from the list of relationships that map to that propagation type.

The available USM BinaryRelationship semantics are as follows:

Note: For details about each type or information about relationship updates, see the USM schema documentation. For information about how to access the schema documentation, see the *Connector Guide*.

Has Access To

Specifies that a CI accesses another CI's functionality. Use this relationship to indicate that a resource can access another resource, or that software communicates with or accesses a specific entity, such as a database. This relationship differs from Has Requirement For, which indicates a mandatory presence of the target CI for the source CI to function.

Has Contact

Specifies that a CI plays a specific contact role for another CI, such as an owner or assignee.

Has Detail

Specifies that a CI provides additional information for another CI. For example, an Asset CI can relate to another CI that provides more detail about the asset.

Has Member

Specifies that a child CI is a member of another CI. For example, several User CIs can be members of a user group. This relationship is the default assignment.

Has Requirement For

Specifies that a CI requires the existence of another CI, its operation, or both. For example, an Application CI can require the operation of an Application Server CI.

Is Affected By

Specifies that a CI impacts another CI and that custom policy defines the impact. Whereas the Has Requirement For relationship causes impact when the target CI is in a critical or down state, Is Affected By lets you configure the scenarios that impact the source CI. For example, a web server farm group is impacted if 40 percent of its ComputerSystem CIs are down.

Note: CIs in maintenance mode are excluded from custom policy calculations that are related to average or percentage.

Is Bound To

Specifies a symmetric relationship where two CIs are intrinsically linked, so that one cannot function without the other.

Is Cause Of

Specifies that a ChangeOrder is the cause of a Request, Incident, or Problem being opened.

Is Clone Of

Indicates that the source CI is a clone of the Target CI and that the two elements are synchronized.

Is Composed Of

Specifies a compositional relationship where a source CI is the aggregate of several target CIs.

Is Connected To

Indicates a network connection carrying data between the source and target CIs, such as between physical ports or application components.

Is Discovered By

Indicates that the specified ManagementAgent target CI discovers and manages the source CI.

Is Evolution Of

Indicates that the source CI is evolved from the target. Examples include next generations of hardware or software.

Is Hosted By

Indicates that the target CI hosts the source CI. This relationship is the inverse of Is Host For.

Is Host For

Indicates that a source CI is hosting a target CI. For example, a ComputerSystem CI can host a VirtualSystem or RunningSoftware CI.

Is Impacted By

Indicates that another CI impacts or affects the source CI. For example, a Memory child CI or Port child CIs affect the parent ComputerSystem CI.

Is Instance Of

Specifies that a source CI is an occurrence of a target CI. For example, a ProvisionedSoftware CI can run an instance of a RunningSoftware CI.

Is Location For

Specifies that a source CI defines the target CI location.

Is Manager For

Specifies that a source CI controls or manages a target CI. For example, a DatabaseInstance CI can manage a Database CI.

Is Request For

Specifies that a source CI has been created to create, provision, or otherwise handle the target CI.

Is Resolved By

Specifies that the specified ChangeOrder target CI resolves or corrects a Request, Incident, or Problem source CI.

Is Result Of

> Specifies that a source CI is created as a result of an automated workflow or manual processing of a target CI.

Relationships display as color-coded arrows between two objects in the Topology view. The Topology view is available on the Operations Console and the Service Modeler. Propagation types of relationships define CA SOI derives CI and service impact.

More Information:

Propagation Types (see page 135)

Propagation Types

Propagation type defines how CA SOI derives the impact when conditions change in related objects. Every relationship in a service model has a propagation type, and each USM relationship type maps to a specific propagation type in CA SOI. The propagation types are as follows:

- Aggregate
- Bound
- Custom
- Operative

Relationships are depicted as arrows between two CIs in the Topology view. The color of the arrow reflects the propagation type of the underlying relationship. The Topology view is available on the Operations Console and the Service Modeler. The first letter of the propagation type is a label on the arrows (A, B, C, or O for Aggregate, Bound, Custom, and Operative, respectively).

Note: Sometimes the arrows are animated red dashes to indicate the root cause of a situation.

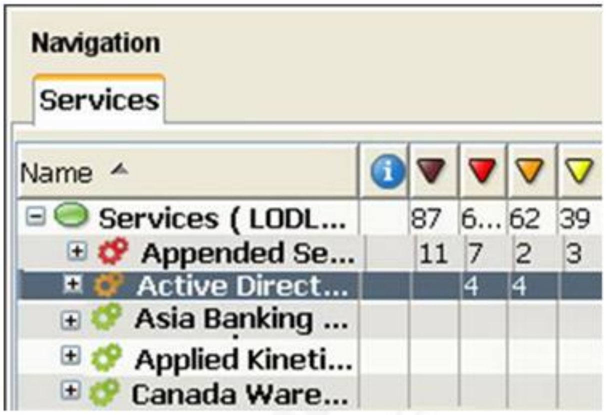
Severity

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
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 ▲	i	▼	▼	▼	▼
⊟ 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.

Significance

Significance indicates the importance of a CI. In a service, many CIs can affect another CI or service. Although each CI affects the health of the service, some CIs can be more important than others. For example, it is important that a print server is available for an online order service. However, the print server does not affect order processing as much as the inventory database does. In this case, the print server has a lower significance than the inventory database.

Significance is a property of a CI in the context of a service. Each CI type has a default significance, but the actual significance is stored in the relationship, thus providing significance with a service scope. When you change significance for an individual CI in a service, the CI's significance value only changes within that service. If the CI belongs to other services, it retains its previous significance value in those services. This behavior ensures that you can maintain different significance values for the same CI if it is more or less important to other services.

CIs can be in as many services as needed and can affect each service differently, based on the significance setting. Suppose that the Payroll department also uses the print server to print checks. Therefore, the print server has much higher significance.

Significance is a value from 1 through 10, where 1 is the least significant and 10 is the most significant. The numeric value denotes how important a child object (antecedent) is to the functioning of its parent object (dependent). Each CI is assigned a significance when it is imported from a domain manager.

CA SOI assigns a default global significance value to every CI type available in the product. For instance, all servers of a Computer System type added to a service model have a significance of 5, while switches and routers have a value of 9. The types Service, Network, and Operating System are considered to be the most important and have a significance of 10.

You can set significance globally or for individual CIs and relationships.

Impact

Impact indicates how much a CI affects a service and related CIs. The following factors determine impact:

- CI severity
- CI significance
- Propagation type and policy

Impact provides IT personnel with a good understanding of what fault conditions really mean to the services that CIs support.

CA SOI calculates the impact by multiplying severity (see page 21) by significance (see page 137). Significance is a number from 1 (lowest) to 10 (highest), and severity ranges from 0 (Normal) to 4 (Down). Therefore, the highest possible impact is 40. Consider an application with a severity of 4 and a significance of 4. The resulting impact is 16.

Note: When a custom propagation policy connects CIs, you can define complex rules for changing the severity value. For more information, see the *Service Modeling Best Practices Guide*.

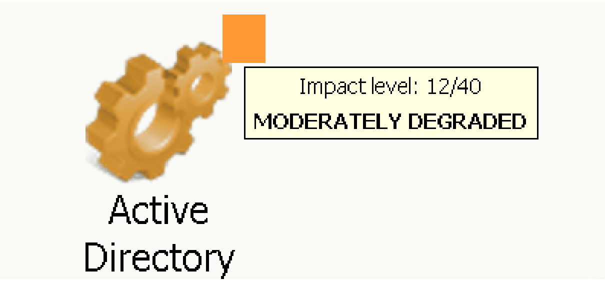
Consider the following items:

- If you change the significance of an item, the impact changes after a new alert is received.
- Priority is used in the calculation of impact instead of significance in the following situations:
  - The service is a top-level service
  - The significance of the parent relationship is zero

The following table defines the impact ranges:

Impact	Color	Description
0	Green	Operational
1-10	Yellow	Slightly Degraded
11-20	Orange	Moderately Degraded
21-30	Red	Severely Degraded
31-40	Burgundy	Down

The Topology tab of the Contents pane shows the impact color as a small box above and to the right of a service, CI, or group. Mouse over the box to display the impact value.



Impact level: 12/40
MODERATELY DEGRADED

The impact number shows on the small box when you click Chart Display Complexity Level ✷ and switch to the Advanced view.

The color of the service icons in the Operations Console indicates the quality impact of the service. *Quality impact* is the inverse value of service health (see page 162), which displays on the Dashboard and the Component Detail pane of the Operations Console.

Granularity

CA SOI supports granularity at two levels: Normal and Low. Normal granularity mode represents an explicit modeling principle where alerts are presented in CA SOI only if all the impacted CIs are included in the model. For example, a computer system CI that is running many service-supporting resources. When the service granularity is Normal, you include all the resources in the model to show their alerts as impacting the service.

Low granularity mode represents a mixed modeling principle where you manage the service granularity as follows:

- You include only the parent CIs and no associated child CIs in the service. In this case, parent CIs act as aggregators for all alerts that affect them directly or indirectly through their commonly related resources. For example, consider the same scenario of a computer system running various service-supporting resources. In this case, you only include the computer system, and any alerts affecting any of the resources hosted on the computer system are aggregated to the computer system.
- You include the parent CIs and specific child CIs (not all child CIs) in your service. In this case, any alerts that are directly associated with the included child CIs are aggregated to those CIs. The alerts that are associated with the nonmodeled child CIs are aggregated to the corresponding parent CIs. For example, you include a computer system CI and its child CPU CI in your service model. If any CPU-related alert comes in, it is associated directly to the CPU. Any other alert not directly associated with the CPU gets attached to the parent computer system CI. Therefore, including granular child CIs does not change the low granularity of the service model for excluded child CIs, enabling mixed-mode low granularity modeling.

Service Models

Service Models are the basis of all administrative and management functions in CA SOI. Service models represent high-level abstract entities; for example, a web-based retail transaction service, a printing service, and a routing service. Service models help you manage your enterprise from the perspective of business services, providing consolidated, holistic, and realistic views of all IT resources.

Each service model consists of the following entities:

- A CI that represents the service itself.
- Child CIs that represent IT elements that support the service or measure and manage some aspect of its behavior.
- Relationships that determine how CIs interact and depend on one another.

Set of propagation policies that determine how impact from a CI fault condition propagates to related CIs.

For service model building procedures, see the *Service Modeling Best Practices Guide*.

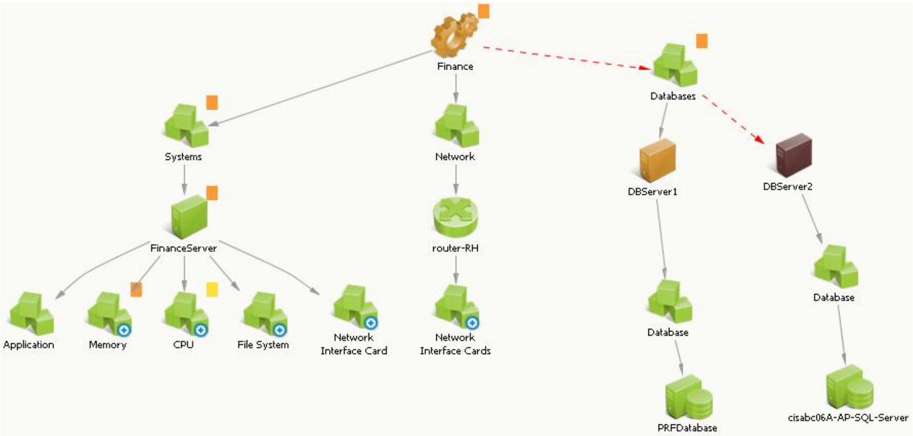
Service Model Types

The most common types of service models are as follows:

Bottom-Up

Bottom-up service models are constructed from a domain-oriented perspective (network, systems, applications, and so on). These models take less time to define and are easier to understand. They focus on impact analysis, not root cause, and are the most common starting point. Most service models that are imported from domain managers are bottom-up, because they define a service from the perspective of their managed domain.

The following graphic shows an example of a bottom-up service model:

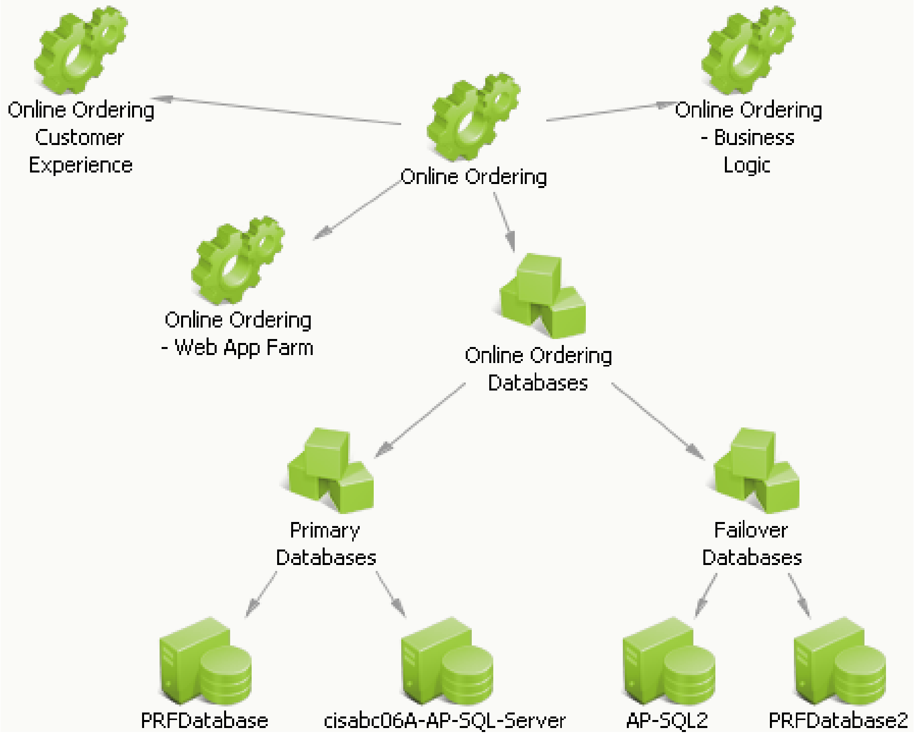


Notice that this bottom-up example is modeled based on groups that define distinct domains: Databases, Network, and Systems. Separate products can manage these domains, and the model combines the intelligence of these domain managers to create a service representation for a Finance department. The model uses groups to aggregate domains and specific objects within those domains (such as the network cards in a router). Note how the model is able to pinpoint the root cause of Finance service degradation as the database server DBServer2.

Note: For a detailed scenario that builds on this example, see the *Service Modeling Best Practices Guide*.

Top-Down

Top-down service models are organized based on a logical business service topology, not by domain. These models are more advanced. They require a better understanding of the logical structure of your enterprise and of the capabilities of service modeling in CA SOI. They ultimately provide better root cause information than bottom-up models.


Online Ordering Customer Experience
Online Ordering
Online Ordering - Business Logic
Online Ordering - Web App Farm
Online Ordering Databases
Primary Databases
Failover Databases
PRFDatabase
cisabc06A-AP-SQL-Server
AP-SQL2
PRFDatabase2

This example uses subservices to provide a solid representation of the business-oriented topology of the service. The items in the specific subservices may or may not be specific to domains. Impact still propagates from subservices to the top-level service.

Federated Modeling

A f*ederated modeling* approach indicates that intelligence is distributed across integrated products. The network management tool has intelligence around the network model, the application management tool has intelligence around applications and transaction models, and so on. CA SOI combines the collective intelligence of all integrated products to derive the overall impact of any CI condition on modeled services.

The benefits of federated modeling are as follows:

- Distributed models are scalable.
- Models in each environment are optimized to suit their role within that environment.
- Leveraging existing models lowers the cost and effort of implementation.
- Models are flexible and extensible to meet the specific detail level that each service requires.

Consider the following example of federated modeling in practice:

- A service in CA SOI models an application and its dependency to a host.
- CA Spectrum models the same host and its dependency to the network and systems infrastructure.
- When a change to the operational state of the infrastructure impacts the host, CA SOI is notified through its CA Spectrum connector. CA SOI can identify the root cause of the problem using the intelligence that CA Spectrum provides without having to model the underlying infrastructure and topology in the service.

Service Discovery

Service Discovery is a CA SOI connector that publishes its data to CA SOI as an ordinary connector running in CA SOI Integration Services. You can use a wizard to define policies that automatically create and maintain services and relationships between source and target CIs according to specified criteria. Service Discovery searches the Persistent Store of all the data that is collected from connectors for CIs that match the policy criteria you define. Service Discovery then creates services and relationships using those CIs.

Service Discovery runs as a part of Integration Services as a connector. The Service Discovery connector appears on the Administration Pages panel among other connectors and the connector can be started or stopped from here.

You can install the Service Discovery connector on the same computer as CA SOI Integration Services and the SA Manager or on a different computer. It is possible to have only one Service Discovery connector in the whole CA SOI solution.

Service Discovery is useful when:

- You want to maintain a collection of CIs that share common qualities.
- Some areas of your enterprise are constantly changing, and you want to maintain a service dynamically without having constantly to add CIs manually.
- Certain relationships occur repeatedly in your enterprise, and manually establishing those relationships would take a significant amount of time.

The following policy types are available:

Note: Service Discovery policies support USM-Core CIs.

Dynamic service policy

Automatically discovers CIs matching specified USM types and attribute criteria and places them under a specified service.

Relationship policy

Automatically creates relationships that are based on source and target CI types and match criteria.

Unmanaged relationship policy

Discovers unmanaged relationships and creates managed relationships (with the same source and target CIs) based on the specified filtering criteria match and whether the source CI is part of the service.

Note: A subservice does not automatically inherit the scope of the parent service. If you want to scope an Automatic Relationship or Unmanaged Relationship policy to a parent service and any of the parent's child services, you must explicitly add the child services to the scope list in the policy.

For Service Discovery procedures, see the *Service Modeling Best Practices Guide*.

Service-Level Agreements

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.

An SLA can, for example, help ensure that an online shopping site is available and delivering the level of service that internet shoppers expect. If performance is poor, some transactions can be lost, thus reducing profits and discouraging repeat customers.

You can define SLAs when you define or edit service models using the SLA tab. CA SOI uses the measurable provisions that you specify in the SLA to monitor the real-time health of each associated service, and records outage time when the service is down. The recorded time is compared to the SLA thresholds to determine the status of the SLA for a given time period.

SLAs let you track service metrics over a specified interval based on specific thresholds. They can help ensure adherence to any quality or availability requirements that an organization must maintain.

SLAs in CA SOI are based on the following attributes:

- Health, Quality, Risk, or Availability metric
- Violation threshold
- SLA time period
- Business hours

Each SLA is based on one of the core CA SOI metrics. An SLA calculates violations that are based on a threshold, spans a defined time period, and is optionally only monitored during defined business hours.

CA SOI uses the measurable provisions that you specify in the SLA to monitor the real-time health of each associated service, and records outage time when the service is down. The recorded time is compared to the SLA thresholds to determine the status of the SLA for a given time period.

For example, you can define an SLA that tracks the quality of a customer-facing website. If the quality drops below the threshold level, an outage is recorded. If the quality stays below the threshold level past the defined threshold time, a violation is recorded. You can track the SLA status through the Operations Console, Dashboard, and reports to ensure that the website meets the customer quality expectation level.

For service-level agreement procedures, see the *Service Modeling Best Practices Guide*.

Chapter 7: Understanding Event and Alert Management

This section provides concepts to help you understand both event and alert management. For related procedures, see the *Event and Alert Management Best Practices Guide*.

This section contains the following topics:

Event and Alert Management Overview

Managing the large stream of messages and fault conditions that the multitudes of data sources generate is a unique and difficult challenge in the modern IT infrastructure. Distributing the management of these conditions across multiple domain managers increases overhead, the potential for error or duplication of work, and time to resolution.

CA Service Operations Insight (CA SOI) collects and displays data from all domain managers in your enterprise. Therefore, CA SOI is the ideal product to use as a unified alert management tool across all managed domains. Operations personnel can use the unified alert view to manage all fault conditions in one place, drilling into the source product when necessary to resolve problems.

You can manage alerts in CA SOI from multiple perspectives:

Service-oriented

> Alerts that are associated with managed services appear when viewing that service, and you can manage alerts from this perspective to ensure service health.

Queue-oriented

> CA SOI also introduces the concept of alert queues to enable unified alert management with no reliance on existence in a managed service. CA SOI displays all collected alerts, including alerts that are not associated with any services. You can group alerts that share common characteristics into queues so that you can manage them together.

These distinct perspectives let you manage alerts in the manner that best suits your needs. If your enterprise is in the early stages of transitioning to a service-oriented paradigm, you can use alert queues to ease the transition to services.

Due to its unique position in the product hierarchy, CA SOI can also serve as the single escalation point for all alerts enterprise-wide. Notification emails, help desk tickets, and other escalations can all originate from CA SOI to consolidate and simplify the escalation and remediation process.

CA SOI also includes an event management layer that lets you define rules for processing raw and normalized event messages. You can define policies that influence how and when raw events appear as alerts, so that operators are presented with a quality set of actionable alert conditions.

The combined features of event and alert management let you effectively manage alert data throughout its lifecycle, from processing to assignment to management to escalation to resolution.

Concepts

This section introduces the core concepts and terms that are associated with event and alert management.

Alerts

An *alert* is a message on the Operations Console that reports a fault condition that is associated with a resource or service. Alerts affect CI severity and, when associated with a service, overall service health. Alerts let you monitor the health of your enterprise and take corrective action when required.

Alerts can come from the following sources:

- CA Catalyst connectors send alerts from their integrated domain managers to CA SOI. Connectors are the primary source of alert data.

  Note: Domain managers have varying terms for the fault conditions they report, such as alarm, notification or event. Connectors convert these conditions so that they all display as alerts in CA SOI and adhere to the USM schema properties for the alert type.

- CA SOI generates alerts on services that indicate service health degradation.
- The Event Management component lets you generate new alerts that are based on correlated event data.
- CA SOI plugins such as the Universal connector let you manually establish custom integrations that produce alert data.

Alert management includes the following features:

- Displaying all alerts in a single console view.
- Launching the source domain manager that generated the alert for more information.
- Alert assignment, annotation, and acknowledgement to track that status of an alert until it is cleared.
- Alert queues to group alerts that share common characteristics for consolidated management.
- Escalation policy to automate the actions to take in response to alert conditions.
- Full help desk integration so that CA SOI can serve as the single point of escalation to CA Service Desk or other help desk products.

Infrastructure Alerts

A domain manager reports an *infrastructure alert*, which is a fault condition on a CI in CA SOI. All infrastructure alerts begin their CA SOI lifecycle (see page 152) as events (see page 23). Events that have a severity greater than normal and come out of Event Management event policy filtering become infrastructure alerts.

CA SOI automatically associates infrastructure alerts with their corresponding CI and assigns to each alert condition a severity that 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 CI 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 belong to one of the following categories:

Quality

Indicates the level of excellence that consumers of a resource experience. For example, performance degradation detected by CA APM takes the form of a quality alert.

Risk

Indicates the likelihood of delivering the service quality that is required to support business objectives. For example, an alert specifying that a computer system has low disk space is a risk alert. If no category is defined, risk is the default category.

These categorizations help determine the quality, risk, and health value for any associated service.

Note: For more information about how alert quality and risk affect the service impact and health, see the *Service Modeling Best Practices Guide*.

Depending on their service association, infrastructure alerts can appear as the following types:

Service impacting

Infrastructure alerts are service impacting when they affect a CI that is part of a managed service. You can view these alerts when viewing the service in the Operations Console or other interfaces.

Non-service impacting

Infrastructure alerts are non-service impacting when they affect CIs that are not part of a managed service. These alerts appear under associated alert queues on the Alert Queues tab of the Operations Console. If the alert does not meet the criteria of any defined alert queues, it appears as a part of the Default queue. You can perform the same operations on non-service impacting alerts (assignment, escalation, and so on) as you can on service impacting alerts.

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.

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.

Alert Escalation Policy

Escalation policy specifies the automated actions to take in response to fault conditions. Escalation policy consists of the following items:

Policy type and assignment

Defines the alerts that the policy evaluates. Escalation policy can be global, or you can assign the policy to evaluate only alerts in specified services or alert queues.

Policy criteria

Defines criteria that an alert must match for the specified action to occur. Criteria can be type-based, time-based, and attribute-based, and the policy can also have an associated schedule.

Escalation action

Defines the action to perform when an alert meets the policy criteria.

Use escalation policies to automate the response to common alert conditions and therefore decrease the time that is required to resolve problems.

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.

Event Types

As an administrator, Event Management lets you interact with the following event types:

Normalized events

Normalized events are events that have been processed to use the alert properties defined in the USM schema. These events become CA SOI alerts unless you create a policy to manipulate or filter them.

Raw events

Raw events are records of normalized events that still use the properties of their event source. Normalization always occurs by default but is often too generic to be useful for raw event sources. Events from raw event sources such as SNMP traps or CA NSM Event Management require a user action to normalize them appropriately to USM alert properties. You can create normalization policy for raw events that map to USM properties to facilitate faster resolution when they become alerts.

Event Policies

An *event policy* is a combination of event search patterns and an action to perform when the patterns match. You can perform the following event policy actions:

- Save them for an on demand view of events that match the search patterns.
- Deploy them to evaluate incoming events that are dynamically based on the search criteria and perform the specified action in response to matches.

Event policies let you manage when and how events become alerts in CA SOI. CA SOI provides the following action types:

- Correlation to associate related events that are based on any criteria
- Filtering to eliminate extraneous events and subsequently lower alert volume
- Creating new events as a result of event policies to consolidate multiple conditions into one actionable condition
- Enriching events to add vital information from outside sources
- Normalization to map raw events to USM alert properties

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

Event Policies with a Normalization Action

You can create and deploy an event policy that manually normalizes raw events with custom mappings from raw event properties to USM alert properties. Normalizing raw events is useful when the default policy for a connector is only generic in nature. The default policy does not perform a mapping that is specific enough to manage the incoming events effectively as alerts. The following connectors are examples of connectors that have generic policy:

- Event connector (some sources)
- SNMP trap connector
- IBM Tivoli Netcool/OMNibus connector
- Oracle Enterprise Manager Grid Control connector
- IBM Tivoli Enterprise Console connector

You can also deploy a normalization action on event sources that have detailed connector policy to refine how required event properties are normalized. The mappings in the event policy overwrite any default mappings in the default policy file. If you want to add information to optional properties or the user attribute properties, use an enrichment action instead, unless that information exists in raw event properties.

The following situations are common normalization action use cases:

- Raw events contain an important property value that is not mapped to any USM alert property by the default connector policy.
- SNMP traps contain important information in their variable bindings that require mapping to individual properties.
- Large-scale event management sources (like IBM Tivoli Netcool/OMNibus) aggregate events from multiple disparate sources. You want to create specific normalization rules for events from each source.

Normalization actions require a raw event search that is available. Deploy a normalization action on only one source connector (which cannot be the Mid-tier connector).

Alert Lifecycle

All alert data that is collected from connectors initially become events, but the lifecycle of an alert can vary. The following process summarizes the typical lifecycle of a message that is retrieved from a connector data source:

1. Connectors convert all types of messages (informational events, error messages, high-level alarms, and so on) from their domain manager to use USM alert properties.
2. Connectors store each USM alert entity as an event in the Event Store on the connector system.

   Note: A record of each raw event with pre-normalized properties is also retained in the Event Store.
3. Event Management evaluates each event against defined policies. If the event matches policy criteria before the event becomes an alert, one of the following actions could happen:
   - The event could be discarded as part of a filter policy and prevented from becoming an alert.
   - The event could be enriched with additional information as part of an enrichment policy.
   - The event could be manually normalized to USM alert properties as part of a normalization policy.
4. Events with a severity greater than Normal that pass through Event Management processing without being discarded become alerts in the Operations Console that are associated with the affected CI.

   Note: Events with a severity of Informational or Normal are automatically prevented from becoming alerts.
5. Alerts that are associated with a service are evaluated for the service impact. If the alert directly affects the service health, it becomes a root cause alert.
6. Alerts are evaluated against alert queue and escalation policies. If a match occurs, one of the following actions could happen:
   - The alert becomes a part of any alert queue with matching criteria.
   - If the alert matches escalation policy criteria, the associated escalation action occurs.
7. Alerts update based on user actions such as assignment, annotations, acknowledgment, and manual escalation.

8. An alert is cleared when one of the following actions occurs:
    - An operator manually clears the alert in the Operations Console.
    - A corresponding Normal alert occurs on the CI.
9. The alert disappears from the main Operations Console views and remains stored as a cleared alert for historical analysis.

Introduction to Alert Management

Alert conditions that impact CIs in integrated domain managers appear in CA SOI as infrastructure alerts. CA SOI provides a powerful and unified alert console that provides operations personnel a view of the following items:

- All managed alerts with their associated services
- All unmanaged alerts with their associated alert queues
- All alerts that identify a degraded service quality or risk from infrastructure alert conditions.

  These service alerts originate from CA SOI based on analysis of the service model, impact policy, and active infrastructure alerts.

CA SOI alerts include details like the alert severity (see page 21) that the domain manager assigns, the number of services the alert impacts, and the impact of the alert condition on those services. In CA SOI, you can acknowledge, assign, annotate, escalate, and clear alerts.

You can work with alerts as follows:

- From a comprehensive alert management perspective using alert queues. The Alert Queues tab lets you define queues to create logical alert categories and manage all collected infrastructure alerts, not only those alerts that are associated with managed services.
- From a service-oriented perspective on the Services tab. The Services tab displays managed services and the alerts that are associated with those services.

You can use alert queues or a combination of both management methods as your infrastructure matures and you move toward a service-oriented management paradigm.

Operations personnel are responsible for the day-to-day tasks involved in monitoring the health of services and resources. This section explains the properties of an alert and contains basic alert management procedures.

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 21) 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.

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 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.

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

Alert Escalation

Alert escalation is the process of performing some action that facilitates the resolution of the alert condition. Alert escalation policy automates alert escalation according to user-defined criteria. When the policy criteria is met, a specified escalation action runs.

Escalation policy is based on any or all of the following criteria:

Alert type

Specifies to act on all alerts of a specific type that meet the defined criteria. For example, an escalation policy can apply to service alerts only, or a subset of infrastructure alerts, such as root cause alerts.

Each escalation policy must specify the alert types to include. You can create escalation policy with only alert types and no criteria to escalate all alerts that meet the type requirement (for example, to escalate all root cause alerts).

Time-based criteria

Specifies to act on alerts according to time-based thresholds, such as the alert age or time in an alert queue. For example, you can specify to act on any alert that has not been assigned within 10 minutes.

Attribute-based criteria

Specifies to act on alerts with attributes that meet specified criteria.

The following types of escalation policies are available:

Non-Global (service or alert queue specific)

Escalates alerts in one or more specified services or alert queues that meet the policy criteria. When an alert is being considered for escalation, it is evaluated in the following policy order: non-global (service then alert queue) then global. For example, you can create service-specific escalation policy for a payroll service owner who wants a notification when CA SOI raises an alert against the payroll service. You can also create a policy that sends an email when critical alerts have not been cleared in an alert queue for a specified time period.

Global

Escalates all alerts that meet the policy criteria. For example, you create a global escalation policy for an IT manager who wants notification when CA SOI raises *any* service alert.

Escalation policy results in one of the following actions:

- Run a command
- Send a notification by email to a technician or operator

- Open a help desk ticket
- Open a help desk announcement
- Execute a CA Process Automation process
- Clear an alert

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

Introduction to Event Management

An event is a message that indicates an occurrence or change in your enterprise. Events can indicate a negative occurrence or object state change. Event management is crucial to understanding the dynamic state of an enterprise across the network, security, system, application, service, and other domains. As the number of resources grows exponentially, so do the challenges of understanding and administering diverse management events from those resources.

CA SOI provides a scalable event management collection and distribution solution (Event Management) with remote visualization and administration capabilities. Entities that connectors report with the USM type of alert are collected into the Event Store on each connector system and are available for Event Management operations. After Event Management processing is complete, the processed events become alerts that you can escalate, add to alert queues, and include in service impact analysis. Typically, with no deployed event policies, all events become alerts. Event Management lets you control the event stream so that a consolidated, high quality, and actionable set of alert conditions appear in the Operations Console as alerts.

Implementing Event Management in a complex distributed environment helps organizations create a unified event management system for their enterprise, providing a holistic view of the entire IT infrastructure. The solution lets organizations collect, transform, correlate, filter, enrich, and manage events from various sources (such as network devices, applications, and enterprise servers) across the enterprise. You can track the events and can create policies to have a manageable set of actionable conditions and convert those conditions for escalation and inclusion in alert queues.

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

Chapter 8: 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 163) and as a mobile device interface (see page 187).

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 29) 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 166) (▼) 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 166) (▼) 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 166) (▼) 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 166) (▼) 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 166) (▼) 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 166) (▼) 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 166) (▼) 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 166) (▼) 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 166) (▼) 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 176).

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 176).

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 (see page 57), 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.

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 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 (see page 288), 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 (see page 288).
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 163) 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 188)

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 189)

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

Customers (see page 190)

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 187).
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 192) 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 189) to display the available alert queues.
   - Tap Customers (see page 190) 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 187).
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 187).
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 188) tab to view services.
   - Tap the Customers (see page 190) 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 195) 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 187).
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 188) tab to view services.
   - Tap the Alert Queues (see page 189) 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 187).
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 191) to display the USM properties for the service.
   - Tap Alerts (see page 192) to display active alerts for the service.
   - Tap Hierarchy (see page 192) 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 187).
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 190) to display the health, quality, risk, and availability for the selected service.
   - Tap Alerts (see page 192) to display active alerts for the service.
   - Tap Hierarchy (see page 192) 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 187).
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 191) to display the USM properties for the service.
   - Tap Alerts (see page 192) to display active alerts for the service.
   - Tap Metrics (see page 190) 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 189).

Follow these steps:

1. Access the Mobile Dashboard (see page 187).
2. Tap the Status Indicator to the right of a given service.

   Each alert displays a colored icon that indicates the severity (see page 21) 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 190) to display the health, quality, risk, and availability for the selected service.
   - Tap Details (see page 193) to display the USM properties for the service.
   - Tap Hierarchy (see page 192) 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 195).

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 187).
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 195) to perform available actions on the alert.
   - Tap Affected CIs (see page 193) 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 187).
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 193) to display the USM properties for the selected alert.
   - Tap Actions (see page 195) to perform available actions on the alert.
   - Tap a service to display the Alerts page (see page 192) for the selected service.
   - Tap a CI to display the USM properties for the CI (see page 194).

View CI USM Properties

You can view the USM properties for a selected CI.

Follow these steps:

1. Access the Mobile Dashboard (see page 187).
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 192) to display alerts impacting the CI.
   - Tap Hierarchy (see page 195) 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 187).
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 192) to display alerts impacting the CI.
   - Tap Details (see page 194) to view the CI USM properties.
   - Tap a service to display the metrics (see page 190) for that service.

View CI Alerts

You can view the alerts impacting a CI.

Follow these steps:

1. Access the Mobile Dashboard (see page 187).
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 194) to view the CI USM properties.
   - Tap Hierarchy (see page 195) to display the CI hierarchy.
   - Tap an alert to see the Actions page (see page 195) 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 189).

Follow these steps:

1. Access the Mobile Dashboard (see page 187).
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 196).
   - Tap Acknowledge Alert or Unacknowledge Alert to acknowledge/unacknowledge an alert (see page 198).
   - Tap Exempt Alert or Unexempt Alert to exempt/unexempt an alert (see page 198).
   - Tap Clear Alert to clear an alert (see page 199).

     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 193) to display the USM properties for the selected alert.
   - Tap Affected CIs (see page 193) 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 187).
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 187).
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 187).
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 195) 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 187).
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 187).
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 187).
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.

Mobile Dashboard Customization

As an administrator or an operator, you can customize the Mobile Dashboard to tailoring its appearance and contents to fit your needs. This section describes all Mobile Dashboard customizations that you can perform.

Change the Icon on the Mobile Dashboard

You can replace the icon that is shown on the Mobile Dashboard with a custom graphic, which applies for all user groups.

To change the icon on the Mobile Dashboard, place a PNG file named mobile_logo.png into the SOI_HOME\SamUI\webapps directory.

The new file appears on the Mobile Dashboard in place of the CA Technologies logo.

Note: You can change the display and positioning of the icon if necessary by customizing the Mobile Dashboard display (see page 201).

Change the Metric Icons on the Mobile Dashboard

You can change the metric icons that show the status of services and SLAs on the Mobile Dashboard. For example, you can change the icons if you prefer a vertical graph representation or an icon that is accompanied by text.

Follow these steps:

1. Stop the CA SOI User Interface service on the UI Server.
2. Delete the SOI_HOME\SamUI\webapps\mobile directory.
3. Rename the SOI_HOME\SamUI\webapps\mobile.war file to mobile.zip.
4. Unzip the mobile.zip file to any empty temporary directory.

   The compressed files are extracted.
5. Replace the icons in the \images\gauge directory with a new version.

   The new icons must have the same names as the old ones and must be PNG files. The following sets of files exist:

   - X-out-of-5.png files show the Quality, Risk, Availability, and Health values.
   - X-out-of-3.png files show the SLA status.

   You cannot add different icons for each metric (for example, separate icons for Health and Quality).
6. Add the modified contents of the temporary directory back to mobile.zip.

   Important! Verify that you compress the contents of the temporary directory only and not the directory itself; otherwise, the Mobile Dashboard will not work.
7. Rename the file to mobile.war.
8. Replace the old SOI_HOME\SamUI\webapps\mobile.war file with the new one.
9. Start the CA SAM User Interface service.

   The new icons appear on the Mobile Dashboard.

Customize Mobile Dashboard Display

If certain objects or pages do not appear correctly on new or unsupported devices, you can customize the Mobile Dashboard display.

Follow these steps:

1. Create a file named mobile_extra_style.css in the SOI_HOME\SamUI\webapps\mobile\styles directory on the UI Server.
2. Write the modifications to the default style sheet and save the file.

   The customizations display on the Mobile Dashboard. You can tweak the style sheet as many times as necessary to achieve the optimal display settings.

For example, if you change the Mobile Dashboard icon (see page 199), you can modify the width and height as follows in mobile_extra_style.css:

```
.logo {
  width: 40px;
  height: 40px;
  left: 2px;
  top: 2px;
}
```

This example sets the icon to be a square of 40x40 pixels and moves it five pixels near the top of the page.

Chapter 9: 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 204).
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 209) 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 204).
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 209) 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 204).
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.

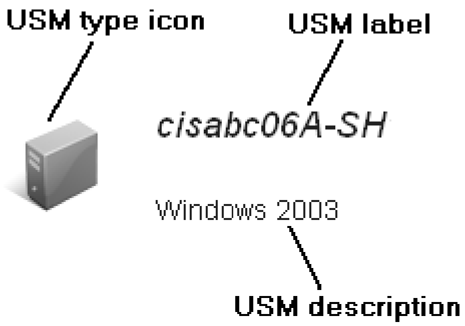
   The search results (see page 209) display.
5. (Optional) Click Start Again to return to the Starting page.
6. (Optional) Click Back to the list of attributes to return to the Browse by CI Attribute page.

Results and USM Properties

As an administrator or an operator, after you search (see page 204) or browse (see page 207) the database, you can view the search results and USM properties.

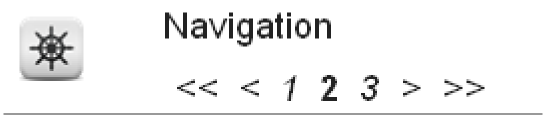
Work with Results in USM Web View

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:



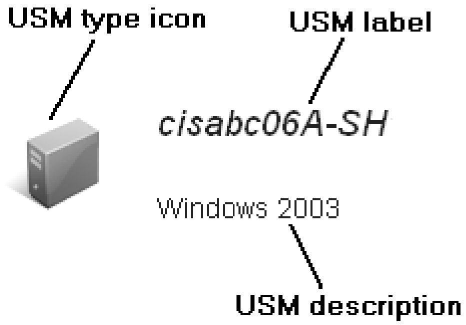
You can do the following on the results page:

- Click an object to display the USM properties (see page 211) 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 217) for the current results.
  - Click Add/Remove to favorite views to add/remove the current search to your favorites (see page 216).
- 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 211) 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 217) for the current results.
  - Click Add/Remove to favorite views to add/remove the current search to your favorites (see page 216).
- 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 204).
- 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 209).

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 214).
- Click Delete entity to delete a manually created CI (see page 215).
- Click Delete manual overrides to delete any manually-entered USM properties (see page 216) 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 217) for updates performed on the current CI.
- Click a property to display search results (see page 209) 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 212), 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 207) 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 204) or browse (see page 207) to locate the relationship object.
2. View the USM properties (see page 211) 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 204).
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 204).

Follow these steps:

1. Search (see page 204) or browse (see page 207) 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 207) objects and navigate to the USM Properties page (see page 211).
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 207) objects and navigate to the USM Properties page (see page 211).
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 211) 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 204) or browse (see page 207) to locate the CI.
2. View the USM properties (see page 211) 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 204) or browse (see page 207) 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 204).

Follow these steps:

1. Search or browse (see page 207) 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 204) 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 10: 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 219).
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 205).
3. (Optional) Click Expand ▲ and select a domain manager from the drop-down list.
4. Click Start searching ➪.

   The search results (see page 222) 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 219).
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 209).

Browse by CI Attribute

You can browse for objects by attribute.

Follow these steps:

1. Access the Starting page (see page 219).

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 209).

Results and USM Properties in USM Web View Mobile

As an administrator or an operator, after you search (see page 220) or browse (see page 220) 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 217).
- 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 217).
- 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 223).
- Click Go ➡ to the right of Delete relationship to delete the relationship (see page 225).
- Click Go ➡ to the right of Delete entity to delete the CI (see page 226).
- Click Go ➡ to the right of Delete manual overrides to delete any manually-entered USM properties (see page 227) 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 220) or browse (see page 220) 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 220) or browse (see page 220) to locate the relationship object.
2. View the USM properties (see page 222) 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 204).
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 204).

Follow these steps:

1. Search (see page 220) or browse (see page 220) to locate the CI.
2. View the USM properties (see page 222) 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 220) or browse (see page 220) to locate the CI.
2. View the USM properties (see page 222) 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 11: Scheduling Maintenance for Services and Resources

This section describes how to enable and schedule maintenance for services and CIs.

This section contains the following topics:

How to Schedule Maintenance for Services and Resources

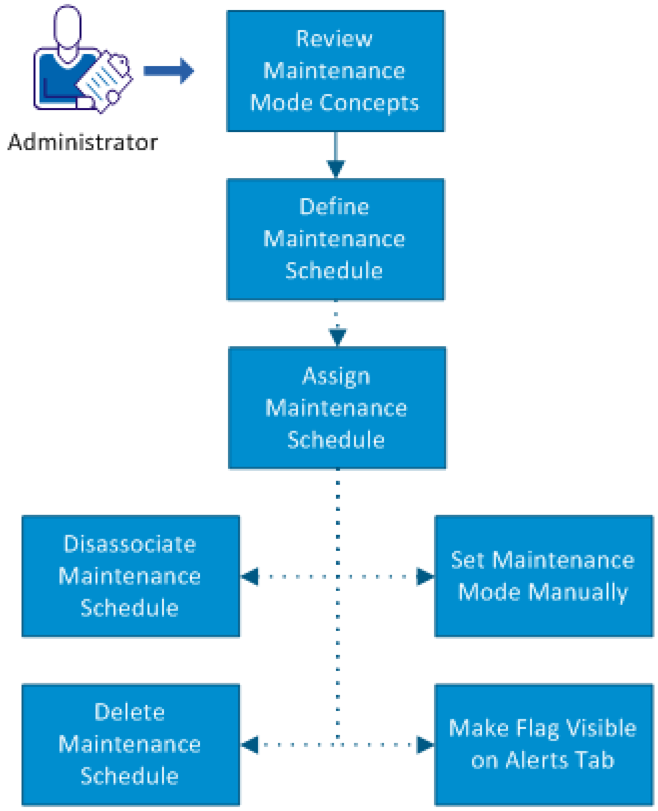
As an administrator, you schedule service and CI maintenance to help ensure peak performance. A *maintenance schedule* defines a time in the future (which can recur at defined intervals) on which to put a service or CI in maintenance. Because CIs can be in multiple services, they can also have multiple schedules.

Before you schedule maintenance, determine the hours when services and resources could be taken offline without affecting the business. If a server is part of a server farm, for example, it could be maintained during business hours without adversely affecting a service because of the redundancy with the other servers.

Note: CIs in maintenance mode are excluded from custom policy calculations that are related to average or percentage.

Use this scenario to guide you through the process:

How to Schedule Maintenance for Services and Resources


Administrator
Review Maintenance Mode Concepts
Define Maintenance Schedule
Assign Maintenance Schedule
Disassociate Maintenance Schedule
Set Maintenance Mode Manually
Delete Maintenance Schedule
Make Flag Visible on Alerts Tab

1. Review maintenance schedule concepts:
   - Maintenance schedule features and behaviors (see page 231)
   - Maintenance mode and impact analysis (see page 232)
   - Maintenance mode and alert escalation (see page 233)
   - Domain manager maintenance propagation (see page 233)
2. Define the maintenance schedule (see page 234).
3. Assign the maintenance schedule to services and CIs (see page 235).
4. (Optional) Perform any of the following actions:
   - Disassociate the maintenance schedule (see page 236).
   - Delete a maintenance schedule (see page 236).
   - Set the maintenance mode manually (see page 237).
   - Make the maintenance mode flag visible on the Alerts tab (see page 237).

Maintenance Schedule Concepts

Become familiar with the following maintenance schedule concepts.

Maintenance Schedule Features and Behaviors

The following features and behaviors are related to maintenance for services and CIs:

Operational mode

Specifies whether services and CIs are in production or in maintenance. The following interfaces shows the operational mode:

- Operations Console, Component Detail pane, Information tab

  If you must maintain an object off the regular schedule, you can set the mode on this tab manually (see page 237). Otherwise, the schedule sets the mode automatically.

- Dashboard, Services table

Maintenance schedule

Specifies when to perform regular maintenance on a service or CI. The schedules are shown on the Information tab of the Component Detail pane.

Icon in Topology view

Shows when an object is in maintenance mode because its icon is dimmed in the Topology view. Also, a small decal (similar to a picture of a wrench) appears at the upper left of the icon. No change happens to the icon in the Navigation pane.

Maintenance flag

Shows which CIs are in maintenance mode. By default, the flag is not visible on the Alerts tab of the Contents pane. You can make it visible (see page 237) by setting preferences. Flags are applied to existing alerts and any new alerts that are generated.

When a service is in maintenance, the services and CIs under it are not.

Impact and escalation

Configures the effect that maintenance has on alert impact and escalation. You can control the following behaviors:

- Whether alerts for CIs in maintenance mode affect the impact of a parent object. By default, the impact of CIs is propagated to the parent service based on propagation and propagation policy.

  For more information about how maintenance mode affects impact, see Maintenance Mode and Impact Propagation (see page 232).

- Whether alerts are escalated when CIs are in maintenance. By default, alerts are escalated when the CIs return to production mode.

  For more information about how maintenance mode affects escalation, see Maintenance Mode and Alert Escalation (see page 233).

Alert creation

Specifies whether alerts are shown for items in maintenance. By default, alerts are shown after the items return to production mode. You can control this setting using a check box on the Alert Filter dialog.

When the filter is enabled, the Alerts tab in the Contents pane displays "Filtered By Maintenance."

Maintenance Mode and Impact Propagation

A global setting on the Administration tab (see page 66) lets you specify how maintenance mode affects the CI and service impact (see page 137). You can select whether to propagate the impact to a parent CI or service.

Note: CIs in maintenance mode are excluded from custom policy calculations that are related to average or percentage.

CA SOI does not automatically place CIs for a service in maintenance mode because the CIs may belong to another service that is not in maintenance mode. Consequentially, Operators could receive alerts for a service that is in maintenance mode. The Operators then mistakenly open tickets against the alerts. You can configure CA SOI to hide alerts on CIs in which that parent service is in maintenance mode. For more information, see the *Event and Alert Management Best Practices Guide.*

Impact propagation on

Specifies that a parent service receives impact values from child services or CIs no matter whether it is in maintenance or production mode.

Impact propagation off

(Default) Specifies that a parent service in maintenance mode is not affected by the impact of child services or CIs. If a CI is propagating impact, either from a child CI or from alerts on the CI itself, impact propagation stops when the service enters maintenance.

When the parent enters maintenance, any propagated impact the service received during production mode is set to zero and the status is returned to normal. The only exception is for impact from an alert on the service itself, as opposed to from child objects.

For information about how to configure impact propagation for maintenance mode, see Configure Global Settings (see page 66).

Maintenance Mode and Alert Escalation

Alert escalation behavior of items in maintenance mode is specific to each escalation policy.

When you define escalation policy, you can specify whether alerts are escalated for CIs that are in maintenance mode. For CIs that are in multiple services, escalation occurs if only one parent is in maintenance.

If the parent service is in maintenance, you can also define whether to escalate any type of infrastructure alert. If you disable this escalation, the policy is only applied after the service is out of maintenance mode. If you enable this escalation, policy is assigned to multiple services, and one of the services is not in maintenance mode, the policy is still triggered.

For more information about how to configure alert escalation for maintenance mode, see the *Event and Alert Management Best Practices Guide*.

Domain Manager Maintenance Propagation

You can configure a global setting (see page 66) to propagate the maintenance mode setting from domain managers that are integrated through connectors for managed CIs and services in CA SOI.

If you enable this feature, a change to the maintenance mode in any domain manager that is integrated through a connector causes the CA SOI maintenance mode for that resource to change accordingly.

Multiple domain managers can have different maintenance settings for the same CI. Reconciliation formulas in the CA Catalyst Logic Server determine which maintenance setting is propagated to CA SOI. For more information about reconciliation, see Working with CA Catalyst Reconciliation (see page 239).

Note: By default, the last update to the maintenance mode is always propagated to CA SOI.

You can also configure maintenance settings in CA SOI to propagate to the source domain managers. For more information about configuring CI synchronization, see Working with CA Catalyst Synchronization (see page 253).

Define a Maintenance Schedule

CA SOI lets you schedule maintenance to occur on specific days and times.

Follow these steps:

1. Open the Operations Console and select Tools, Schedule Editor.
2. Click ⊕ Add.
3. Select or enter the following information:

   Schedule Type

   Specifies the type of schedule to create. Select "Maintenance Schedule" from the drop-down list. The other two schedule types (SLA Period and Business Hours) are used for SLAs and escalation policy.

   Start Date

   Specifies the day of the week and the date when the schedule begins. The date cannot be more than one year in the future.

   Time

   Specifies the start time, end time, and duration (in hours) of the maintenance. The duration is calculated automatically based on the start and end times.

   Recurrence

   Specifies how often to apply maintenance. Select from the following options:

   None

   Specifies that the maintenance schedule occurs only once.

   Daily

   Specifies that the schedule recurs every week day, every weekend, or after a specified number of days. For example, you can create a schedule that renews every three days. A daily schedule starts for the first time on the specified start date.

   Weekly

   Specifies that the schedule recurs after a specified number of weeks and begins on a specific day. For example, you can create a schedule that starts on the first Monday after the specified start date and renews every two weeks.

Monthly

Specifies that the schedule recurs after a specified number of months and begins on a specific day of the month. For example, you can create a schedule that starts on the fifth day of the month after the specified start date and renews every three months.

Yearly

Specifies that the schedule recurs after a specified number of years and begins on a specific day of a specific month. For example, you can create a schedule that starts on January 5 (the first occurrence of this day after the start date) and renews every two years.

For all recurrence options, select either No Expiration for the schedule to recur indefinitely or enter a Schedule End Date when the schedule stops.

Description

Specifies a name for the schedule. Spaces and punctuation are allowed.

Limits: 256 characters

4. Click OK.

   The Schedule Editor reopens, with the new schedule listed on the Schedules tab.

Assign a Maintenance Schedule to Services and CIs

After you define a maintenance schedule, you assign it to services and CIs. Assigned schedules are listed on the Information tab of the Component Detail pane.

When maintenance for an object occurs based on the schedule, the following changes take place:

- The Operational Mode is changed automatically to Maintenance. The modes are shown on the Information tab in the Component Detail pane. When maintenance is finished, the mode is changed back to Production.
- The icon is dimmed in the Topology view. Also, a small decal (similar to a picture of a wrench) appears at the upper left of the icon. No change happens to the icon in the Navigation pane. An 'M' appears in the Information column next to the CI.

Follow these steps:

1. Perform one of the following actions:
   - Right-click a service or CI on the Services tab of the Navigation pane and select Assign Maintenance Schedules.
   - Click a service or CI on the Services tab, and select Tools, Assign Maintenance Schedules.

2. Click a schedule in the Available Schedules pane on the left side of the dialog, and then click the right arrow button.

   Note: If you do not see a schedule that you want to use, click the Create button to define a maintenance schedule (see page 234).

3. Click OK.

Disassociate a Maintenance Schedule

If you want to remove a service or CI schedule, you can disassociate the schedule. The assigned schedules are listed on the Information tab of the Component Detail pane.

Note: Before you delete an unwanted schedule, disassociate all the associated items from the schedule.

Follow these steps:

1. Perform one of the following actions:
   - Right-click a service or CI on the Services tab of the Navigation pane and select Assign Maintenance Schedules.
   - Click a service or CI on the Services tab and select Tools, Assign Maintenance Schedules.
2. Click a schedule in the Current Schedules pane and click the left arrow button.
3. Click OK.

Delete an Unused Schedule

You can delete a schedule (that is, a maintenance schedule, SLA period, or business hours) that no service or CI uses.

Follow these steps:

1. Open the Operations Console and select Tools, Schedule Editor.
2. Select the schedule to delete in the Schedules tab.
3. (Optional) Disassociate the schedule from any items in the Associated Items tab them before deleting.
4. Click Delete then confirm the deletion.

Set Maintenance Mode Manually

When scheduled maintenance occurs, CA SOI automatically changes the operational mode of services and resources to Maintenance. When the scheduled maintenance is finished, the mode automatically changes back to Production.

If you must perform unscheduled maintenance, you can also change the maintenance mode manually.

Follow these steps:

1. Right-click a service or CI in the Navigation or Contents pane and select Set Maintenance Mode. You can select multiple services or CIs using Ctrl+click and then right-click to set the maintenance mode for multiple resources at the same time.
2. Perform one of the following actions:
   - Click Set in the New Mode column for the appropriate resource, select the maintenance mode to apply, and click OK.

     The maintenance mode changes for the selected CI or service.
   - Click Maintenance or Production next to "Reset 'New Mode' column value for all selected items" and click OK.

     The maintenance mode changes to the appropriate setting for all selected services or CIs.

You can also manually set the operational mode from the Information tab for a CI or service in the Component Detail pane. Click set next to Operational Mode to change the mode.

Make the Maintenance Flag Visible on the Alerts Tab

An alert maintenance flag indicates that CIs are in maintenance mode. The flag appears for existing alerts and any new alerts that are generated. By default, the flag is not visible on the Alerts tab in the Contents pane. You can make it visible, however, by setting preferences.

Follow these steps:

1. Open the Operations Console and select View, Preferences.
2. Expand Alerts Tab and Alerts Table and click Columns.
3. Click Maintenance, and click OK.
4. Restart the Operations Console.

Appendix A: Working with CA Catalyst Reconciliation

This section describes how to customize reconciliation policies through the CA Catalyst Registry.

This section contains the following topics:

How to Perform CA Catalyst Reconciliation

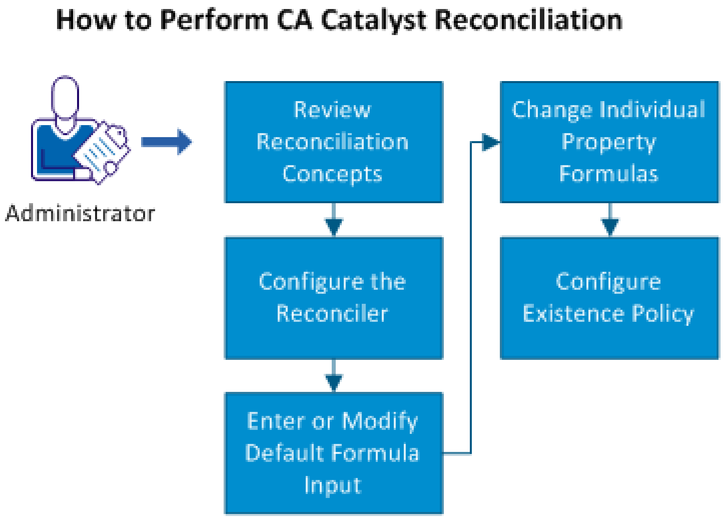
As an administrator, you can configure CA SOI to perform CI reconciliation.

The Correlator and Reconciler components interact as follows to create a reconciled set of CIs:

1. The Correlator receives notification when the correlation keys match for two or more collected CIs.
2. The Correlator gathers the projection sheets from the matching CIs into a notebook and sends an event indicating a new or updated notebook to the Reconciler.
3. The Reconciler retrieves the notebook indicated in the event from the Persistence Service. The Reconciler then creates a reconciled sheet from the notebook. The reconciled sheet is a single set of properties that are derived from the projection sheets using reconciliation formulas.

CA SOI displays the reconciled sheet from each notebook as a CI in the USM Web View. You can view USM properties for each CI to see the reconciled set of properties. You can also view the USM notebook for each CI to see the reconciled sheet compared with the projection sheets listing the properties retrieved from each source domain manager.

Use this scenario to guide you through the process:


How to Perform CA Catalyst Reconciliation
Administrator
Review Reconciliation Concepts
Configure the Reconciler
Enter or Modify Default Formula Input
Change Individual Property Formulas
Configure Existence Policy

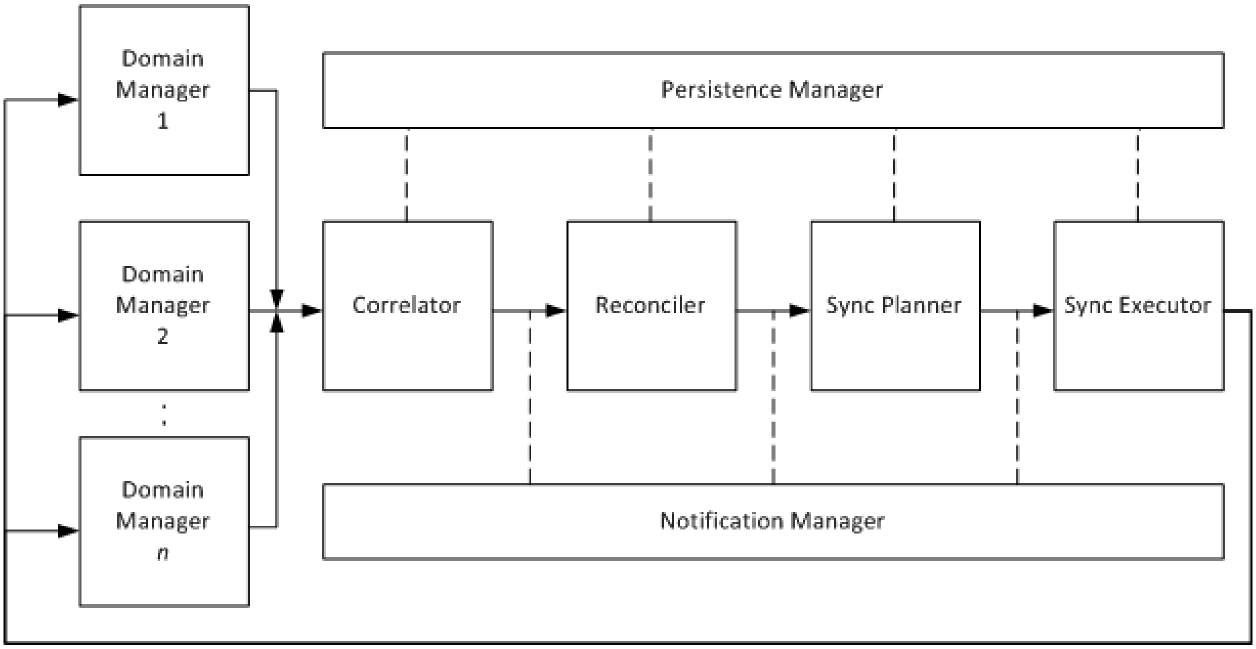
1. Review reconciliation concepts (see page 240).
2. Configure the Reconciler (see page 244).
3. Enter or modify the default formula input (see page 246).
4. Change individual property formulas (see page 247).
5. Configure existence policy (see page 248).

Reconciliation Concepts

Become familiar with the following reconciliation concepts and how to access the CA Catalyst Registry.

Logic Server Overview

The Logic Server uses the USM schema and the Persistence Service interface to enact operations that create a unified, Persistent Store of USM data from the domain manager data retrieved by connectors. The following illustration shows the flow of data from connectors through the Logic Server:



Correlator

Matches USM entities coming from multiple domain managers that represent the same managed object (for example, a database server managed by CA NSM, CA Spectrum, and CA eHealth). This SA Manager component evaluates data against common properties named *correlation keys*. Each CI enters the SA Manager as a *projection sheet*. If correlation keys match, the Correlator creates a *notebook* with all projection sheets that the Correlator determined refers to the same CI. Correlation occurs in the SA Manager and notebooks are transmitted to the Reconciler in the Logic Server.

Reconciler

Creates a *reconciled sheet* of common properties for correlated projection sheets, so that objects managed by multiple domains appear as one reconciled CI in CA SOI that uses the unified set of properties in the reconciled sheet.

Note: For more information about how reconciliation works and how to customize reconciliation policies and formulas, see How Reconciliation Works. (see page 239)

Persistence Manager

Transmits data to and from the Persistence Service for creating, updating, and deleting CI sheets and notebooks and running named queries on objects.

Notification Manager

Manages the subscription and buffering of events from the Persistence Service. This component notifies the Logic Server modules when USM data requires modification.

Sync Planner

Determines when to synchronize data from the Persistent Store with source domain managers based on synchronization plans.

Sync Executor

Performs the synchronization operations indicated by the Sync Planner. The Executor pushes synchronization changes to the connector framework, after which the connector carries out the necessary inbound operations on its domain manager to change the domain manager data so that it matches the records in the Persistent Store.

Note: For more information about how synchronization works, see Synchronization (see page 253).

Important! The functionality enabled by the Sync Planner and Sync Executor components is only supported for specific synchronization use cases (see page 253).

Reconciliation Formulas

The Reconciler reconciles notebook CI properties that are based on reconciliation rules and formulas. The Reconciler contains a Formula Processor that determines the appropriate value of each property in a reconciled sheet that is based on the following provided formulas:

NullFormula

Sets a property value to Null in the reconciled sheet.

NoOpFormula

Ignores the calculation of any property value in the reconciled sheet. The old property value is preserved if it was set previously.

FirstNonNullValueWinsFormula

Uses the first not null value found in the projection sheets for the property in the reconciled sheet.

MajorityWinsFormula

Uses the property value that is reported by the most projection sheets as the value in the reconciled sheet.

SingleSourceOfTruthFormula

Populates the reconciled sheet based on a CI projection sheet from a specific domain manager as a source of truth. This formula requires an input to define the source of truth (see page 246).

BinaryRelationshipFormula

Calculates the source MdrID and target MdrID in BinaryRelationship reconciled CIs. This formula uses only the following properties in the defaultsheet.xml file:

- SourceMdrProduct
- SourceMdrProdInstance
- SourceMdrElementID
- TargetMdrProduct
- TargetMdrProdInstance
- TargetMdrElementID

LastUpdatedWinsFormula

Uses property values from the last updated projection sheet to calculate the reconciled sheet.

Access the CA Catalyst Registry

You can access the CA Catalyst Registry to configure Logic Server functionality such as reconciliation rules, synchronization policies, and so on.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA Service Operations Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Catalyst Registry.
5. Enter the CA SOI administrator user credentials in the Username and Password fields and click Sign-in.

More Information:

Working with CA Catalyst Reconciliation (see page 239)

Configure the Reconciler

The Reconciler configuration is stored in the Registry. You can change the properties of several elements to influence how reconciliation occurs.

Follow these steps:

1. Access the CA Catalyst Registry.
2. Navigate to the following location: /topology/physical/node0/sor/ssaserver.xml

   A page opens for viewing or editing the contents.
3. Click Edit as text.

   The contents of the ssaserver.xml file display. The Reconciler configuration properties are located in the <tns:reconciler> section.
4. Make changes to any of the following key elements and click Save Content:

   numberOfCorrelationObservers

   Defines the number of observers that can read the correlation queue for correlated events and process them. Increasing this number uses more memory and CPU to process events.

   Default: 1

   numberOfInstructionObservers

   Defines the number of observers that can read the instruction queue for new instruction events and process them. Increasing this number uses more memory and CPU to process events.

   Default: 3

   mdrName

   Defines the value of the MDR Name property in the reconciled sheet. The default is CA:00030, which is the registered MdrProduct property value for CA Catalyst.

   mdrInstanceName

   Defines the value of the MDR Instance Name property in the reconciled sheet.

   Default: tenant0

DefaultFormula

Defines the default formula used by the Reconciler to reconcile correlated CI projection sheets. You can set any available reconciliation formula (see page 242) as the default. The default formula is the global formula used by the Formula Processor to perform all reconciliations.

Default: com.ca.ssa.sor.formula.LastUpdatedWinsFormula

To change the default, set the ini:javaImpl property value next to "Default Formula" to the formula name prefixed by the implementation, which is com.ca.ssa.sor.formula for all provided formulas.

For example, to set the default formula to NoOpFormula, modify the "Default Formula" line as follows:

```
<tns:formula name="Default Formula"
ini:javaImpl="com.ca.ssa.sor.formula.NoOpFormula"
```

If the formula that you set as the default requires an input, you provide that input in the defaultsheet.xml file (see page 246).

defaultSheetURL

Defines the location of the file used to calculate the property values in the reconciled sheet.

Default: /topology/physical/node0/sor/defaultsheet.xml

You can manipulate the file listed in this location to specify different formulas for calculating the value of each property (see page 247). Do not change this property unless you have changed the location of the defaultsheet.xml file.

configurationURL

Defines the location of the file used to define existence policy, which declares the domain managers that should be the source of truth for determining CI existence in the Persistent Store.

Default: /topology/physical/node0/sor/sourceoftruthmdr.xml

The Reconciler uses existence policy to detect if a CI managed by multiple domains should be deleted. You can manipulate this file to change the primary, secondary, and non-source of truth domain managers (see page 248). Do not change this property unless you have changed the location of the sourceoftruthmdr.xml file.

Enter or Modify Default Formula Input

You specify the default reconciliation formula (see page 244) in the Registry.

MdrProduct

Defines the MdrProduct USM property value for the connector whose domain manager you want to be the single source of truth. All connectors have a registered MdrProduct value that is a five-digit number with a prefix of 'CA:'. The *Connector Guide* contains a table of all registered MdrProduct values.

MdrProductInstance

Defines the MdrProductInstance USM property value for the domain manager system to use as the single source of truth. This value is typically the server name associated with a specific instance of the domain manager.

Important! The input string for this property is case sensitive.

true|false

Specifies how the formula handles a null property value in the single source of truth CI projection sheet. Set this value to true to populate the reconciled sheet property with the null value. Set this value to false to use the FirstNonNullValueWinsFormula to populate the reconciled sheet property.

For the SingleSourceOfTruth formula, which is the only formula requiring an input, you must specify the domain manager in the defaultsheet.xml file and adhere to the following convention:

input="*MdrProduct*::*MdrProductInstance*,true|false"

As no other formulas require an input value, the default entry in the defaultsheet.xml file has the appropriate value of *.

Follow these steps:

1. Access the CA Catalyst Registry (see page 243).
2. Navigate to the following location: /topology/physical/node0/sor/defaultsheet.xml.
3. Click Edit as text.
4. Change the input property in the line beginning with '<defaultFormula' to the appropriate value and click Save Content.

Example: Set default input for CA Spectrum single source of truth formula

The following example sets a CA Spectrum instance as the single source of truth for the default reconciliation formula (which this example assumes is SingleSourceOfTruthFormula):

```
<defaultFormula name="DefaultFormula" input="CA:00002::cadev2,true" />
```

CA:00002

Sets data retrieved from the CA Spectrum connector as the single source of truth.

cadev2

Sets the specific CA Spectrum instance cadev2 as the single source of truth.

true

Populates any null property value from the single source of truth projection sheet with the null value in the reconciled sheet.

Change Individual Property Formulas

You specify the default reconciliation formula (see page 244) in the ssaserver.xml file. The defaultsheet.xml file lets you set different reconciliation formulas for specific properties. Property-specific formulas override the default for that property.

For example, consider a situation where CA Spectrum is the preferred domain manager for maintenance information. If the default formula is FirstNonNullValueWinsFormula, you may want to set the formula for the IsInMaintenance property to always use the property retrieved from CA Spectrum.

Follow these steps:

1. Access the CA Catalyst Registry (see page 243).
2. Navigate to the following location:
   /topology/physical/node0/reconciler/defaultsheet.xml.
3. Click Edit as text.

   Notice that several properties already have specific formulas applied, such as MdrProduct and MdrElementID. Do not change the formulas for these properties.
4. Use the following line to define a property-specific formula and click Save Content:

   ```
   <formulaRecord input="" name="" cellName=""/>
   ```

cellName

Defines the name of the USM property to which to apply the specific reconciliation formula.

name

Defines the name of the reconciliation formula to apply when reconciling the specified property. This attribute requires only the formula name, such as NoOpFormula.

input

Defines input parameters for any formula that requires them. Currently, only SingleSourceOfTruthFormula requires input. For all other formulas, enter an asterisk (*) for the input.

Example: Set cell-specific formula for IpAddress

This example sets the reconciliation formula for the IpAddress property to NoOpFormula, so that the Reconciler does not perform any calculations on this property:

```
<formulaRecord input="*" name="NoOpFormula" cellName="IpAddress"/>
```

Configure Existence Policy

Existence policy controls the domain managers that the Reconciler uses as a source of truth to detect whether to delete a CI from the Persistent Store that has been deleted from a source domain manager. By default, CA Catalyst never deletes a reconciled CI from the Persistent Store. You can edit existence policy in the sourceoftruthmdr.xml file to specify a primary and secondary source of truth and a non-source of truth to use for this calculation.

For example, consider a CI that is managed in CA NSM, CA Spectrum, and CA CMDB. If CA CMDB is set as the primary source of truth in existence policy and the CI is deleted from CA CMDB, the Reconciler deletes the CI from the Persistent Store, despite its continued existence in CA NSM and CA Spectrum.

Follow these steps:

1. Access the CA Catalyst Registry (see page 243).
2. Navigate to the following location:
   /topology/physical/node0/sor/sourceoftruthmdr.xml.
3. Click Edit as text.
4. Enter entries for the following sections as necessary and click Save Content:

   <tns:PrimaryST>

   Defines the primary source of truth for CI existence. If a CI managed by this connector is deleted in the source domain manager, CA Catalyst deletes it from the Persistent Store.

   <tns:SecondaryST>

   Defines the secondary source of truth for CI existence. If a CI managed by this connector is deleted in the source domain manager, CA Catalyst deletes it from the Persistent Store unless it still exists in any primary source of truth.

   <tns:NonST>

   Defines the non-source of truth for CI existence. If a CI managed by this connector is deleted in the source domain manager, CA Catalyst deletes it from the Persistent Store only if it does not exist in any domain managers listed as primary or secondary sources of truth.

   You can define multiple sources of truth in each section, as long as specific instances appear in only one of the sections. When sections contain multiple sources of truth, a connector needs to match only one source of truth to trigger the appropriate action.

   Use the following format to define a source of truth:

   ```
   <tns:MdrProduct>MdrProduct</tns:MdrProduct>
   <tns:MdrProductInstance>MdrProductInstance</tns:MdrProductInstance>
   ```

   MdrProduct

   Defines the MdrProduct USM property value for the connector whose domain manager to use as a source of truth. All connectors have a registered MdrProduct value that is a five-digit number with a prefix of 'CA:'. The *Connector Guide* contains a table of all registered MdrProduct values.

   MdrProductInstance

   Defines the MdrProductInstance USM property value for the domain manager system to use as a source of truth. This value is typically the server name associated with a specific instance of the domain manager defined in the MdrProduct property.

   Important! The input string for this property is case sensitive.

5. Restart the CA SAM Application Server service.

Example: Multi-domain existence policy

The following example illustrates an existence policy with multiple domains and instances defined in each section:

```
<tns:SourceOfTruthMdr
xmlns:tns="http://ns.ca.com/catalyst/2010/02/sourceoftruthmdr"
xmlns:usm-core="http://ns.ca.com/2009/07/usm-core">
       <tns:PrimaryST>
              <tns:MdrID>
                     <tns:MdrProduct>CA:00020</tns:MdrProduct>
                     <tns:MdrProdInstance>cmdbserver</tns:MdrProdInstance>
              </tns:MdrID>
              <tns:MdrID>
                     <tns:MdrProduct>CA:00020</tns:MdrProduct>
                     <tns:MdrProdInstance>cmdbserver2</tns:MdrProdInstance>
              </tns:MdrID>
       </tns:PrimaryST>
       <tns:SecondaryST>
              <tns:MdrID>
                     <tns:MdrProduct>CA:00003</tns:MdrProduct>
                     <tns:MdrProdInstance>nsmserver</tns:MdrProdInstance>
              </tns:MdrID>
              <tns:MdrID>
                     <tns:MdrProduct>CA:00004</tns:MdrProduct>
                     <tns:MdrProdInstance>specserver</tns:MdrProdInstance>
              </tns:MdrID>
       </tns:SecondaryST>
       <tns:NonST>
              <tns:MdrID>
                     <tns:MdrProduct>CA:00031</tns:MdrProduct>
                     <tns:MdrProdInstance>scomserver</tns:MdrProdInstance>
              </tns:MdrID>
              <tns:MdrID>
                     <tns:MdrProduct>CA:00002</tns:MdrProduct>
                     <tns:MdrProdInstance>5ehserver/tns:MdrProdInstance>
              </tns:MdrID>
       </tns:NonST>
</tns:SourceOfTruthMdr>
```

Based on this example, the Reconciler determines reconciled CI existence in the Persistence Store as follows:

- Deletes the reconciled CI when the projection CI is deleted in the CA CMDB servers cmdbserver and cmdbserver2.
- Deletes the reconciled CI when the projection CI is deleted in the nsmserver CA NSM instance or the specserver CA Spectrum instance if the CI is not reported from either of the CA CMDB servers listed in the primary source of truth section.
- Deletes the reconciled CI when the projection CI is deleted from the scomserver Microsoft SCOM instance or ehserver CA eHealth instance if the CI is not reported from any of the instances listed as primary and secondary sources of truth.

Appendix B: Working with CA Catalyst Synchronization

This section describes how to interact with the CA Catalyst Logic Server synchronization functionality.

This section contains the following topics:

Synchronization

Synchronization is the CA Catalyst capability of updating source domain manager data due to CI changes. Changes are a result of reconciliation or other changes to data in the Persistent Store, including CI creation and deletion. Synchronization can occur only for connectors that have bidirectional functionality and can perform inbound to connector operations on their source domain manager.

The following process indicates how the Logic Server performs CI synchronization on source domain managers:

1. The Reconciler publishes an event indicating a new or updated notebook with a reconciled CI.
2. The SyncPlanner collects the event and creates a synchronization plan for the notebook by doing the following:
   - Compares the difference between the reconciled sheet and the projection sheets
   - Verifies the list of connectors currently integrated with source domain managers that support synchronization
   - Runs the plan through the plan control file, which provides specialized filtering so that only specific operations appear in the final plan
3. The SyncPlanner passes the synchronization plan to the SyncExecutor through the Notification Manager as an event.
4. The SyncExecutor runs the synchronization plan by passing necessary synchronization changes to the UCF Broker.

5. The UCF Broker tells the connectors with domain managers that require synchronization changes to make the appropriate changes in the source domain managers.

Consider a scenario where the Reconciler creates a reconciled sheet for a CI managed by CA CMDB, CA eHealth, and CA NSM based on a formula that defines the CA CMDB CI as the single source of truth. If enabled, synchronization determines that the reconciled sheet contains different properties than the projection sheets for CA eHealth and CA NSM CIs, creates a plan to synchronize the CA eHealth and CA NSM CIs with the reconciled properties, and runs the plan so that CA eHealth and CA NSM are synchronized with the reconciled CI in the Persistent Store.

Important! Synchronization functionality is not enabled by default for this release and is only supported for specific use cases. This section only includes information about enabling those specific use cases.

Synchronization Use Cases

The CA Catalyst framework and bidirectional connectors provide the functionality to invoke inbound create, update, and delete operations to synchronize the data in integrated domain managers. This functionality is only supported when used as part of a certified use case.

CA SOI supports synchronization for the following use cases:

Alert Synchronization (see page 256)

CA SOI supports synchronization of Cleared and Acknowledged alert properties for CA NSM, CA Spectrum, and Microsoft SCOM.

CA SOI Service Synchronization (see page 262)

CA SOI supports synchronization of all CI types and relationships for BMC Atrium or CA CMDB.

Maintenance Mode Synchronization (see page 268)

CA SOI supports synchronization of maintenance mode status with connectors that support inbound to connector update operations on the IsInMaintenance USM property.

Important! Patches to Registry files may require you to re-enable previously enabled synchronization use cases after patch application. See the notes included with each patch for more information.

Configure Registry Email Settings

As an administrator, you configure the Registry to send an email with error details if the Synchronizer fails to synchronize a property after a specified number of retries. By default, the Registry does not send error emails, so you define the settings for these emails in the CA SOI Administration UI.

Follow these steps:

1. Access the CA SOI web user interface.
2. Click the Administration tab.
3. Click the plus sign (+) next to CA Service Operations Insight Manager Configuration.
4. Click the plus sign (+) next to the server you want to configure.
5. Click the Email Configuration option.
6. Complete the following fields and click Save:

   SMTP Server Host

   Specifies the email server host name.

   SMTP Server Port

   Specifies the email server port number.

   SMTP Server Domain

   Specifies the email server domain.

   SMTP Server Password

   Specifies the SMTP server password, if any. Leave this field blank if there is no password.

   SMTP Mail From

   Defines the sender of synchronization error emails.

   SMTP Mail To

   Defines the recipient of synchronization error emails.

   The email server configuration settings are updated in the ssaserver.xml file in the Registry.

7. Restart the CA SAM Application Server service.

How to Enable Alert Synchronization

As an administrator, you can synchronize the Cleared and Acknowledged alert properties from CA SOI to the following products and releases:

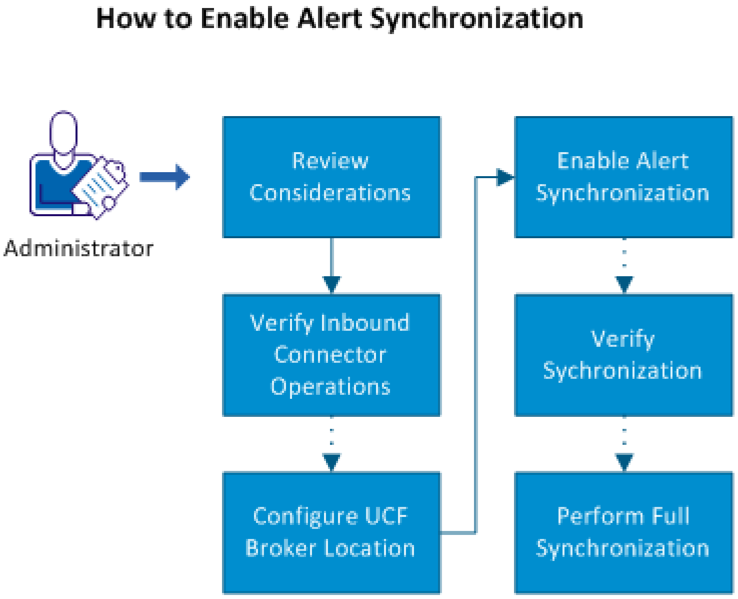
- CA Spectrum r9.2.0 H03 (Acknowledged and Cleared properties)
- CA NSM r11.2 SP2 (Acknowledged property only)
- Microsoft SCOM 2007 R2 (Cleared and Acknowledged properties)

The domain manager sends an alert to CA SOI; once a user clears or acknowledges the alert in CA SOI, the update propagates to the domain manager.

Unlike other synchronizations where CIs are correlated across all domain managers, CA SOI alerts are correlated in pairs with the domain manager that initiated the alert (CA SOI and CA Spectrum, CA SOI and Microsoft SCOM, or CA SOI and CA NSM).

All reconciliation formulas are supported, but only SingleSourceOfTruth and LastUpdateWinsFormula (the default formula) are certified.

Use this scenario to guide you through the process:


How to Enable Alert Synchronization
Administrator
Review Considerations
Verify Inbound Connector Operations
Configure UCF Broker Location
Enable Alert Synchronization
Verify Sychronization
Perform Full Synchronization

1. Review the considerations (see page 257).
2. Verify that inbound to connector operations are enabled on all connectors that you want to participate in the use case (see page 258).
3. (Optional) Configure the UCF Broker location if it uses a different server or port number than the default (see page 258).

4. Enable alert synchronization and configure reconciliation formulas (see page 259).
5. (Optional) Verify the synchronization (see page 259).
6. (Optional) Perform a full synchronization (see page 260).

Considerations

When using CA SOI alert synchronization, consider the following:

- CA Spectrum supports alert synchronization for Cleared and Acknowledged properties.
- CA NSM supports alert synchronization for the Acknowledged property only. This applies to the CA NSM DSM connector, not the CA NSM WorldView connector.
- Microsoft SCOM supports alert synchronization for Cleared and Acknowledged properties.
- Alert synchronization is performed in pairs between CA SOI and the domain manager that initiated the alert (CA SOI and CA Spectrum, CA SOI and CA NSM, and so on), but not across all domain managers.
- Some connectors may set the USM IsAcknowledgable and IsClearable properties to false for certain alerts, meaning that these alerts cannot be cleared or acknowledged in the source domain manager. However, CA SOI allows clearing and acknowledging of all alerts in the Operations Console regardless of these property values, which could cause minor inconsistencies in alert status between CA SOI and the source domain manager.

Enable Inbound to Connector Operations in the Connector

By default, inbound to connector operations are enabled in all connectors. Verify that operations are enabled only in the connectors for which you want to make changes in their domain managers.

Note: If you are performing maintenance mode synchronization, verify that each connector supports update operations on the IsInMaintenance property. Then you can verify inbound to connector operations. See the *Connector Guide* for each connector for a list of supported operations.

Follow these steps:

1. Access the CA SOI Dashboard.
2. Click the Administration tab.
3. Expand Connector Configuration and the connector server name and select a connector entry.

   Settings for that connector display.
4. Verify that IsRemotable is selected in the Connector Controls table, select the check box if it is not, and click Save.
5. Repeat Steps 3-4 for all connectors that you want to participate in a supported use case. You can also disable inbound to connector operations for connectors that you do not want to participate in a supported use case.

Configure UCF Broker Location

The Synchronizer uses the UCF Broker to communicate synchronization changes to connectors, so it must have the correct UCF Broker URI. By default, the UCF Broker URI is set to localhost listening on port 8020. If either condition is true, you configure the UCF Broker location:

- You installed the UCF Broker on a separate system from the SA Manager.
- You set the UCF Broker to listen on a nondefault port.

Follow these steps:

1. Access the CA Catalyst Registry.
2. Navigate to the following location: /topology/physical/node0/sor/ucf-broker.properties.

   A page opens for viewing or editing the file contents.
3. Click Edit as text.

4. Change the following line to use the correct UCF Broker system and listener port and click Save Content:

   ```
   broker.1.ws.uri=http://localhost:8020/ucf/BrokerService
   ```

5. Restart the CA SAM Application Server service.

Enable Alert Synchronization

The CA SOI Dashboard provides an Administration page that lets you enable alert synchronization that the use case supports.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Synchronization Configuration.
5. Select the Enable option for Alerts.
6. Click Save.

   This control enables alert synchronization in all domain managers that the use case supports with connectors that have the IsRemotable control enabled.

7. (Optional) To change the reconciliation formula, see Working with CA Catalyst Reconciliation (see page 239).

   The default reconciliation formula is LastUpdateWinsFormula. You can change the formula to define a single source of truth or define rules for specific CI properties.

8. Click Submit.
9. Restart the CA SAM Application Server service.

Verify Alert Synchronization

After you have enabled the alert synchronization use case, clear or acknowledge an alert in the Operations Console. Then verify that the change occurs in the reconciled sheet and the supported domain manager that contains the alert.

Perform Full Synchronization

Enabling synchronization use cases only synchronizes changes from the time they are enabled forward. CA SOI provides a synchronization priming utility that fully synchronizes CA SOI to the real-time environment.

This utility is useful in the following situations:

- You just enabled synchronization, and you want to synchronize changes already in place.
- You experienced a product failure (CA SOI, a connector, the Synchronizer, and so on) and you want to synchronize any changes that occurred during the downtime.
- You added a product to your solution and you want to completely synchronize with the products already installed.

Due to the possible increased load on your network that was generated during a full synchronization, we recommend performing the synchronization during non-business hours.

Important! Enable synchronization use cases before you run the priming utility, or full synchronization does not occur. Run the priming utility for use cases you have enabled only. You can enable any or all of the supported use cases simultaneously.

Follow these steps:

1. Locate the sync_primer.properties file at SOI_HOME\Tools\PrimingUtility, and open with a text editor.
2. Update the following values as necessary:

   sleep_time_secs

   Defines the sleep time in seconds between sets of CI notebooks that are sent to the reconciler.

   Default: 5

   notebook_chunk_size

   Defines the maximum number of notebooks to send to the Reconciler in a single set.

   Default: 100

   Limit: 1000

Alert_Synch

Defines if alert synchronization is enabled (true) or disabled (false).

Alert_Synch_Type

Defines the CI types to synchronize.

Note: Currently only the Alert type is supported.

InMaintenance

Defines if maintenance mode synchronization is enabled (true) or disabled (false).

InMaintenance_Types

Defines the CI types to synchronize separated by commas. By default, the full list of CI types is provided, so you can remove CI types you do not want to synchronize if necessary.

SOI_Service_Synchronization

Defines if the CA SOI service synchronization is enabled (true) or disabled (false).

SOI_Service_Synchronization_Types

Defines the list of supported CI types separated by commas, or enter All_Types to synchronize all CI types, depending on the policies on the machine.

start_date=*yyyy-mm-dd hh*:*mm*:*ss*

Defines the date in the past to begin the CI synchronization. If left blank, all CIs (regardless of date) are retrieved and synchronized. The format is *yyyy-mm-dd hh*:*mm*:*ss* where hour (*hh*) is based on a 24-hour clock; for example, *hh* for 3 PM is 15.

Example: Enter 2010-11-12 14:21:00 to synchronize all CIs since November 12, 2010 at 2:21:00 PM.

SOI_MDR_PRODUCT_ID=CA:00047

For future use. Do not change the value of this property.

3. Save the file.
4. Run PrimerUtility.bat in the SOI_HOME\Tools\PrimingUtility directory on the server where the SA Manager is installed.

   The utility indicates the number of notebook IDs retrieved. The utility provides its progress by displaying the current number of CIs remaining to be reconciled and when it is sleeping (based on the value you entered for sleep_time_secs).

How to Enable CA SOI Service Synchronization

As an administrator, you can synchronization all CI types and relationships from CA SOI to the following products and releases:

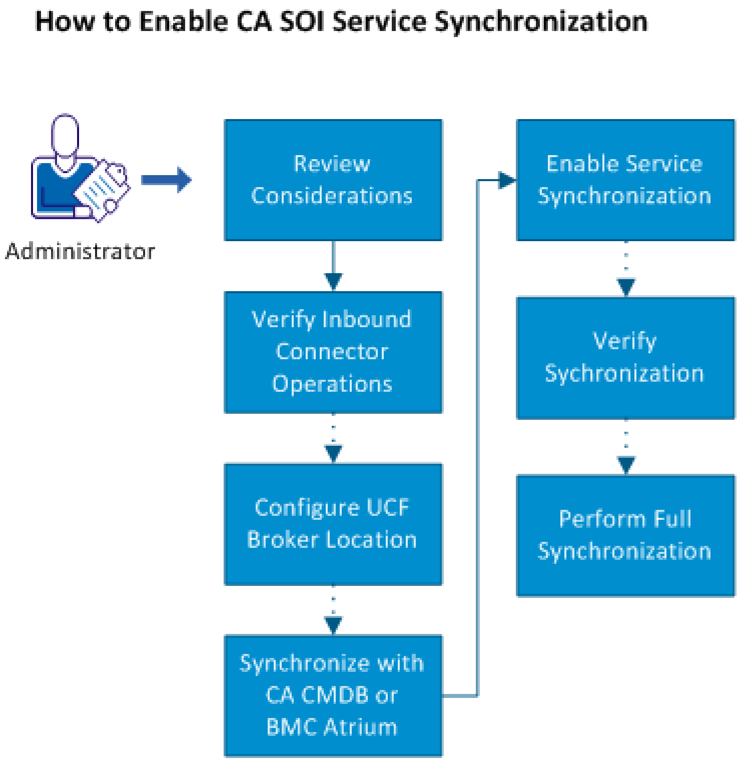
- CA CMDB r12.5
- BMC Atrium r7.6.00

When a change to a service model (including adding or updating a CI) occurs, connectors supporting the use case invoke the change in their domain manager. Therefore, the services are synchronized across your enterprise.

Note: When enabling service synchronization, only relationships can be deleted.

The default reconciliation formula is LastUpdateWinsFormula.

Use this scenario to guide you through the process:


How to Enable CA SOI Service Synchronization
Administrator
Review Considerations
Verify Inbound Connector Operations
Configure UCF Broker Location
Synchronize with CA CMDB or BMC Atrium
Enable Service Synchronization
Verify Sychronization
Perform Full Synchronization

1. Review the considerations (see page 263).
2. Verify that inbound to connector operations are enabled on all connectors that you want to participate in the use case (see page 264).
3. (Optional) Configure the UCF Broker location if it uses a different server or port number than the default (see page 264).

4. (Optional) Synchronize CA SOI with all service models in CA CMDB or BMC Atrium (see page 265).
5. Enable CA SOI service synchronization and configure reconciliation formulas (see page 265).
6. (Optional) Verify the synchronization (see page 266).
7. (Optional) Perform a full synchronization (see page 266).

Considerations

When using CA SOI service synchronization, consider the following items:

- Due to processing requirements, perform an initial synchronization during non-business hours.
- All CI types and relationships are supported, but CA SOI must manage the CIs and therefore part of the managed service.
- You can synchronize either CA CMDB or BMC Atrium, but not both.
- Only one instance of either product is supported; for example, you cannot have three instances of CA CMDB.
- Relationships are correlated when CA SOI manages them.
- The use case supports all CI types and relationships. However, the CA CMDB and BMC Atrium connectors support inbound to connector operations on only a subset of CI types. For a list of supported types for each connector, see the CA CMDB and BMC Atrium connector documentation. Also, see the InboundToConnectorTypes list on the connector's page in the Administration UI.

  Note: BinaryRelationship is not included in the InboundToConnectorTypes list for BMC Atrium, but the connector does support inbound to connector operations on the BinaryRelationship type.
- To correctly synchronize relationship deletions in CA SOI with CA CMDB or BMC Atrium, import all synchronized services from CA CMDB or BMC Atrium back into CA SOI. The import includes services managed in other products that are integrated with CA SOI and created in CA CMDB or BMC Atrium as a result of enabling synchronization. If you want to synchronize all services managed in CA CMDB or BMC Atrium, including those created when synchronization occurs, enable automatic service import from the appropriate connector before enabling the synchronization. However, if you want to synchronize only a subset of managed services in CA CMDB or BMC Atrium, manually import that subset of services back into CA SOI after enabling synchronization.

Enable Inbound to Connector Operations in the Connector

By default, inbound to connector operations are enabled in all connectors. Verify that operations are enabled only in the connectors for which you want to make changes in their domain managers.

Note: If you are performing maintenance mode synchronization, verify that each connector supports update operations on the IsInMaintenance property. Then you can verify inbound to connector operations. See the *Connector Guide* for each connector for a list of supported operations.

Follow these steps:

1. Access the CA SOI Dashboard.
2. Click the Administration tab.
3. Expand Connector Configuration and the connector server name and select a connector entry.

   Settings for that connector display.
4. Verify that IsRemotable is selected in the Connector Controls table, select the check box if it is not, and click Save.
5. Repeat Steps 3-4 for all connectors that you want to participate in a supported use case. You can also disable inbound to connector operations for connectors that you do not want to participate in a supported use case.

Configure UCF Broker Location

The Synchronizer uses the UCF Broker to communicate synchronization changes to connectors, so it must have the correct UCF Broker URI. By default, the UCF Broker URI is set to localhost listening on port 8020. If either condition is true, you configure the UCF Broker location:

- You installed the UCF Broker on a separate system from the SA Manager.
- You set the UCF Broker to listen on a nondefault port.

Follow these steps:

1. Access the CA Catalyst Registry.
2. Navigate to the following location: /topology/physical/node0/sor/ucf-broker.properties.

   A page opens for viewing or editing the file contents.
3. Click Edit as text.

4. Change the following line to use the correct UCF Broker system and listener port and click Save Content:

   ```
   broker.1.ws.uri=http://localhost:8020/ucf/BrokerService
   ```

5. Restart the CA SAM Application Server service.

Synchronize with CA CMDB or BMC Atrium

You can synchronize CA SOI with all service models in CA CMDB or BMC Atrium, including service models that are created during a synchronization.

Follow these steps:

1. Select the appropriate connector on the Configure Data Sources dialog in the Operations Console.
2. Click Auto to enable the automatic service import for that connector. If you select this option, then do *not* perform a full synchronization (see page 266).

   Note: If you want to synchronize only a certain subset of services in CA CMDB or BMC Atrium with CA SOI, then manually import those services from CA CMDB or BMC Atrium back into CA SOI. Do not click Auto for the import.

Enable CA SOI Service Synchronization

The CA SOI Dashboard provides an Administration page that lets you enable service synchronization that the use case supports.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Synchronization Configuration.
5. Select the Enable option for Services.
6. Click Save.

   The changes are applied. This control enables service synchronization in all domain managers that the use case supports with connectors that have the isRemotable control enabled.

7. (Optional) To change the reconciliation formula, see the Working with CA Catalyst Reconciliation (see page 239).

   The default reconciliation formula is LastUpdateWinsFormula. You can change the formula to define a single source of truth or define rules for specific CI properties.

8. Click Submit.

9. Restart the CA SAM Application Server service.

Verify CA SOI Service Synchronization

After you have enabled the service synchronization use case, perform one of the following actions to verify the functionality:

- (LastUpdatedWinsFormula) Import a service into CA SOI from any source (like CA eHealth or CA Spectrum), and verify that the service is created in BMC Atrium or CA CMDB.
- (LastUpdatedWinsFormula) Add CIs to a service in CA CMDB and BMC Atrium and verify that the CIs are created in the CA SOI service.
- (SingleSourceOfTruthFormula) Change a CI property in a synchronized service in the single source of truth domain manager. Also, verify that the change occurs in all participating products.

Perform Full Synchronization

Enabling synchronization use cases only synchronizes changes from the time they are enabled forward. CA SOI provides a synchronization priming utility that fully synchronizes CA SOI to the real-time environment.

This utility is useful in the following situations:

- You just enabled synchronization, and you want to synchronize changes already in place.
- You experienced a product failure (CA SOI, a connector, the Synchronizer, and so on) and you want to synchronize any changes that occurred during the downtime.
- You added a product to your solution and you want to completely synchronize with the products already installed.

Due to the possible increased load on your network that was generated during a full synchronization, we recommend performing the synchronization during non-business hours.

Important! Enable synchronization use cases before you run the priming utility, or full synchronization does not occur. Run the priming utility for use cases you have enabled only. You can enable any or all of the supported use cases simultaneously.

Follow these steps:

1. Locate the sync_primer.properties file at SOI_HOME\Tools\PrimingUtility, and open with a text editor.

2. Update the following values as necessary:

   sleep_time_secs

   Defines the sleep time in seconds between sets of CI notebooks that are sent to the reconciler.

   Default: 5

   notebook_chunk_size

   Defines the maximum number of notebooks to send to the Reconciler in a single set.

   Default: 100

   Limit: 1000

   Alert_Synch

   Defines if alert synchronization is enabled (true) or disabled (false).

   Alert_Synch_Type

   Defines the CI types to synchronize.

   Note: Currently only the Alert type is supported.

   InMaintenance

   Defines if maintenance mode synchronization is enabled (true) or disabled (false).

   InMaintenance_Types

   Defines the CI types to synchronize separated by commas. By default, the full list of CI types is provided, so you can remove CI types you do not want to synchronize if necessary.

   SOI_Service_Synchronization

   Defines if the CA SOI service synchronization is enabled (true) or disabled (false).

   SOI_Service_Synchronization_Types

   Defines the list of supported CI types separated by commas, or enter All_Types to synchronize all CI types, depending on the policies on the machine.

start_date=*yyyy-mm-dd hh*:*mm*:*ss*

Defines the date in the past to begin the CI synchronization. If left blank, all CIs (regardless of date) are retrieved and synchronized. The format is *yyyy-mm-dd hh*:*mm*:*ss* where hour (*hh*) is based on a 24-hour clock; for example, *hh* for 3 PM is 15.

Example: Enter 2010-11-12 14:21:00 to synchronize all CIs since November 12, 2010 at 2:21:00 PM.

SOI_MDR_PRODUCT_ID=CA:00047

For future use. Do not change the value of this property.

3. Save the file.
4. Run PrimerUtility.bat in the SOI_HOME\Tools\PrimingUtility directory on the server where the SA Manager is installed.

   The utility indicates the number of notebook IDs retrieved. The utility provides its progress by displaying the current number of CIs remaining to be reconciled and when it is sleeping (based on the value you entered for sleep_time_secs).

How to Enable Maintenance Mode Synchronization

As an administrator, you can synchronize the maintenance mode status with connectors that support inbound to connector update operations on the IsInMaintenance USM property. The following connectors support this use case:

- Microsoft SCOM
- CA Spectrum
- CA CMDB
- CA NSM
- CA SOI

Note: See the *CA Catalyst Connector Guide* for each connector to verify other connectors that support the use case.

A maintenance mode update for a CI in a domain manager changes the CA Catalyst CI reconciled sheet according to the reconciliation formula. After this change occurs, connectors supporting the use case invoke the change in their domain managers, so that maintenance status is synchronized across your enterprise.

The use case also affects the maintenance mode in CA SOI. You can configure CA SOI so that IsInMaintenance property updates in the source domain manager change the CA SOI maintenance mode setting for the CI. For more information about maintenance mode in CA SOI, see the *CA SOI Administration Guide*.

Although most reconciliation formulas (see page 242) work with the maintenance mode synchronization use case, the most common formulas to apply to the use case are as follows:

SingleSourceOfTruthFormula

Updates the CA SOI maintenance mode status and the IsInMaintenance property in the CA Catalyst reconciled sheet and other domain managers. Updates are based on the setting in one source of truth domain manager. For example, if you define CA CMDB as the single source of truth, and a CI managed in CA CMDB goes into maintenance, the update occurs in CA SOI and all other domain managers with connectors that support the use case. An update to the maintenance status in other domain managers is ignored and reverted to the single source of truth value.

LastUpdatedWinsFormula

Updates the CA SOI maintenance mode status and the IsInMaintenance property in the reconciled sheet and other domain managers. Updates are based on the last domain manager that updated the property. For example, if you put a CI into maintenance in CA NSM, the update occurs in CA SOI and all other domain managers with connectors that support the use case. Also, if you put a CI into maintenance in CA SOI, the update occurs across domains. This formula synchronizes every maintenance mode update.

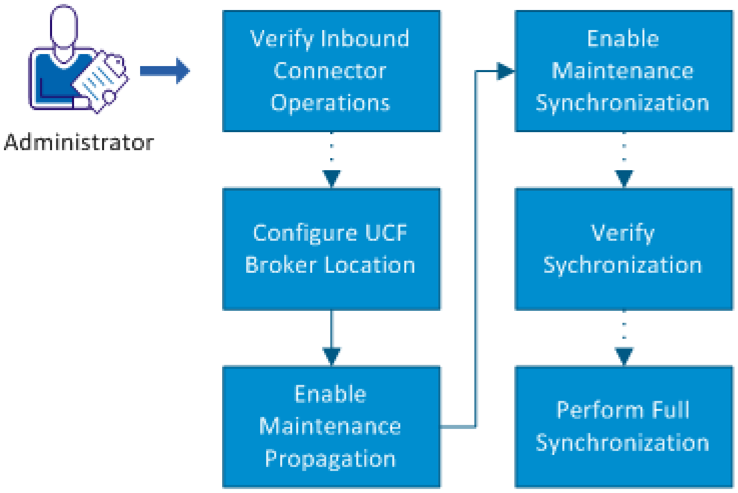
The use case supports only updating the property, not creating or deleting. The specific USM property for which updates are synchronized is IsInMaintenance. The following USM types include this property:

- Application
- ApplicationServer
- ApplicationSystem
- BackgroundProcess
- Cluster
- ComputerSystem
- Database
- DatabaseInstance
- DirectoryServer
- File
- GenericIPDevice
- Group
- HypervisorManager
- InterfaceCard
- MailServer
- ManagementAgent
- Memory
- Network
- OperatingSystem
- OrganizationalEntity
- Port
- Printer
- Processor
- Router
- Service
- Switch
- Tablespace
- VirtualSystem

Note: The list includes types that at least one participating connector supports. Not all participating connectors support all of these types.

Use this scenario to guide you through the process:

How to Enable Maintenance Mode Synchronization


Administrator
Verify Inbound Connector Operations
Configure UCF Broker Location
Enable Maintenance Propagation
Enable Maintenance Synchronization
Verify Sychronization
Perform Full Synchronization

Important! This release supports only the synchronization customizations described in Step 4. Do not perform additional customization to synchronization settings or the synchronization plan.

1. Verify that inbound to connector operations are enabled on all connectors that you want to participate in the use case (see page 271).

   Note: See the *CA Catalyst Connector Guide* for each connector to verify whether it supports updating IsInMaintenance in its domain manager.

2. (Optional) Configure the UCF Broker location if it uses a different server or port number than the default (see page 271).
3. Enable CA SOI maintenance propagation (see page 272).
4. Enable maintenance synchronization and configure reconciliation formulas (see page 272).
5. (Optional) Verify the synchronization (see page 274).
6. (Optional) Perform a full synchronization (see page 274).

Enable Inbound to Connector Operations in the Connector

By default, inbound to connector operations are enabled in all connectors. Verify that operations are enabled only in the connectors for which you want to make changes in their domain managers.

Note: If you are performing maintenance mode synchronization, verify that each connector supports update operations on the IsInMaintenance property. Then you can verify inbound to connector operations. See the *Connector Guide* for each connector for a list of supported operations.

Follow these steps:

1. Access the CA SOI Dashboard.
2. Click the Administration tab.
3. Expand Connector Configuration and the connector server name and select a connector entry.

   Settings for that connector display.
4. Verify that IsRemotable is selected in the Connector Controls table, select the check box if it is not, and click Save.
5. Repeat Steps 3-4 for all connectors that you want to participate in a supported use case. You can also disable inbound to connector operations for connectors that you do not want to participate in a supported use case.

Configure UCF Broker Location

The Synchronizer uses the UCF Broker to communicate synchronization changes to connectors, so it must have the correct UCF Broker URI. By default, the UCF Broker URI is set to localhost listening on port 8020. If either condition is true, you configure the UCF Broker location:

- You installed the UCF Broker on a separate system from the SA Manager.
- You set the UCF Broker to listen on a nondefault port.

Follow these steps:

1. Access the CA Catalyst Registry.
2. Navigate to the following location: /topology/physical/node0/sor/ucf-broker.properties.

   A page opens for viewing or editing the file contents.
3. Click Edit as text.

4. Change the following line to use the correct UCF Broker system and listener port and click Save Content:

   ```
   broker.1.ws.uri=http://localhost:8020/ucf/BrokerService
   ```

5. Restart the CA SAM Application Server service.

Enable Maintenance Propagation

You can configure a CA SOI setting so that the maintenance mode status can participate in maintenance synchronization. When enabled, the CA SOI maintenance status can play any role in the synchronization use case. The status can be the single source of truth, or it can implement a maintenance status change from other domains. If you do not enable CA SOI to participate in maintenance synchronization, any maintenance status that you define in CA SOI CIs is unaffected by maintenance synchronization in other connectors and their domain managers.

Follow these steps:

1. Access the CA SOI Dashboard
2. Click the Administration tab.
3. Expand CA Service Operations Insight Manager Configuration and the server that you want to configure.
4. Click Global Settings.

   Select Yes from the Propagate Domain Manager Maintenance Settings drop-down list and click Save.

Enable Maintenance Synchronization

The CA SOI Dashboard provides an Administration page that lets you enable maintenance mode synchronization that a use case supports.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Synchronization Configuration.
5. Select enabled in the IsInMaintenance Property Synchronization pane.

   This control enables maintenance mode synchronization in all domain managers that a use case supports. The connectors must have the IsRemotable control enabled.

6. Click Add Formula in the IsInMaintenance Property Reconciliation Formula Record pane.

   A drop-down list appears for selecting the reconciliation formula for the IsInMaintenance property. Note that this formula only affects reconciliation on the IsInMaintenance property, not other properties.

7. Select the appropriate reconciliation formula.

   If you select Single Source of Truth, the MDR drop-down list appears.

8. (Single Source of Truth formula only) Do the following:

   - Select the domain manager to use as the single source of truth in the MDR drop-down list. If you do not see an entry that should appear in the MDR drop-down list, verify that the UCF Broker is running and that all connectors are running with the IsRemotable control enabled. You can define multiple sources of truth by adding another formula. The first single source of truth takes precedence over other selections.

   - Select the Accept null value check box to accept any IsInMaintenance value provided by the single source of truth, even a null value, as the reconciled property value to synchronize in all participating domains. If you leave this check box cleared, a null value in the single source of truth causes the Synchronizer to evaluate the next formula for the reconciled IsInMaintenance value.

9. (Optional) Complete Steps 6-8 to add as many reconciliation formulas as necessary.

   The Synchronizer evaluates the formulas in the order they appear on the page, with the first formula taking precedence. You can have multiple sources of truth or multiple formulas to calculate the reconciled value if the first formula does not apply (the source of truth returns a null value, for example).

10. Click Submit.

11. Restart the CA SAM Application Server service.

Verify Maintenance Synchronization

After you have enabled the maintenance synchronization use case, perform one of the following actions to verify the functionality:

(SingleSourceOfTruthFormula) Change the maintenance mode for a CI in the single source of truth domain manager, and verify that the change occurs in the reconciled sheet and other domain managers with connectors that the use case supports.

- (LastUpdatedWinsFormula) Change the maintenance mode for a CI in CA SOI, and verify that the change occurs in all domain managers with connectors that the use case supports.
- (LastUpdatedWinsFormula) Change the maintenance mode for a CI in any domain manager, and verify that the change occurs in CA SOI and other domain managers with connectors that the use case supports.

Perform Full Synchronization

Enabling synchronization use cases only synchronizes changes from the time they are enabled forward. CA SOI provides a synchronization priming utility that fully synchronizes CA SOI to the real-time environment.

This utility is useful in the following situations:

- You just enabled synchronization, and you want to synchronize changes already in place.
- You experienced a product failure (CA SOI, a connector, the Synchronizer, and so on) and you want to synchronize any changes that occurred during the downtime.
- You added a product to your solution and you want to completely synchronize with the products already installed.

Due to the possible increased load on your network that was generated during a full synchronization, we recommend performing the synchronization during non-business hours.

Important! Enable synchronization use cases before you run the priming utility, or full synchronization does not occur. Run the priming utility for use cases you have enabled only. You can enable any or all of the supported use cases simultaneously.

Follow these steps:

1. Locate the sync_primer.properties file at SOI_HOME\Tools\PrimingUtility, and open with a text editor.
2. Update the following values as necessary:

   sleep_time_secs

   Defines the sleep time in seconds between sets of CI notebooks that are sent to the reconciler.

   Default: 5

   notebook_chunk_size

   Defines the maximum number of notebooks to send to the Reconciler in a single set.

   Default: 100

   Limit: 1000

   Alert_Synch

   Defines if alert synchronization is enabled (true) or disabled (false).

   Alert_Synch_Type

   Defines the CI types to synchronize.

   Note: Currently only the Alert type is supported.

   InMaintenance

   Defines if maintenance mode synchronization is enabled (true) or disabled (false).

   InMaintenance_Types

   Defines the CI types to synchronize separated by commas. By default, the full list of CI types is provided, so you can remove CI types you do not want to synchronize if necessary.

   SOI_Service_Synchronization

   Defines if the CA SOI service synchronization is enabled (true) or disabled (false).

   SOI_Service_Synchronization_Types

   Defines the list of supported CI types separated by commas, or enter All_Types to synchronize all CI types, depending on the policies on the machine.

start_date=*yyyy-mm-dd hh*:*mm*:*ss*

Defines the date in the past to begin the CI synchronization. If left blank, all CIs (regardless of date) are retrieved and synchronized. The format is *yyyy-mm-dd hh*:*mm*:*ss* where hour (*hh*) is based on a 24-hour clock; for example, *hh* for 3 PM is 15.

Example: Enter 2010-11-12 14:21:00 to synchronize all CIs since November 12, 2010 at 2:21:00 PM.

SOI_MDR_PRODUCT_ID=CA:00047

For future use. Do not change the value of this property.

3. Save the file.

4. Run PrimerUtility.bat in the SOI_HOME\Tools\PrimingUtility directory on the server where the SA Manager is installed.

   The utility indicates the number of notebook IDs retrieved. The utility provides its progress by displaying the current number of CIs remaining to be reconciled and when it is sleeping (based on the value you entered for sleep_time_secs).

Appendix C: Understanding REST Web Services

Representational State Transfer (REST) is a client-server architectural style of building applications that leverages the fundamental properties of HTTP to manage objects accessible at a URL. REST architecture and applications are stateless, which means that no client context information is stored between requests. Each request contains all the information necessary to service the request. REST web services are lightweight, HTTP-based, easy to create and use, and have the desirable property of relating the classes of data to each other using hyperlinks. REST web services provide a simple yet powerful mechanism to interact with data. Using these web services, integration developers can configure the product and can make it communicate through the REST interface. They can use REST web services directly to send HTTP requests to the server for the resources they want to manipulate.

CA SOI lets you expose CA SOI data over REST web services. Because of the inherent standards in the REST architecture, CA SOI REST web services make the CA SOI data accessible to many different development environments. Several resources such as CA SOI user interfaces and third-party interfaces can then consume the exposed data. This ability helps integration developers extend the CA SOI solution by integrating its data with other products through REST web services. These interfaces provide an HTTP-based integration point to the CA SOI data, allowing read or write access. Using these web services, you can access the CA SOI data directly from a browser or can integrate it into your own applications. You can use these web services with any language that understands how to manage HTTP integration.

This section provides an overview of available CA SOI REST web services, supported REST HTTP methods, and requirements common to all REST web services. For complete REST web services information, see the *Web Services Reference Guide*.

This section contains the following topics:

Available CA SOI REST Web Services

As an integration developer, you use the following REST web services that CA SOI provides:

- Alert Queue (see page 278)
- Alert (see page 279)
- CI (see page 279)
- Configuration (see page 280)
- Customer (see page 280)
- Email (see page 281)
- Escalation Policy Action (see page 281)
- Escalation Policy (see page 282)
- Group (see page 282)
- Meta (see page 283)
- Schedule (see page 284)
- Service (see page 284)
- User (see page 285)

Note: The complete documentation for CA SOI REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/

Alert Queue REST Web Services

You can perform the following operations using the Alert Queue REST web services:

- The Alert Queue REST web services let you perform the following tasks:
- Create an alert queue
- Get a list of alert queues
- Get a list of alerts in an alert queue
- Get the alert queue definition
- Get hyperlink entries associated with an alert queue

- Get the status information for an alert queue
- Update an alert queue
- Delete an alert queue

Note: The complete documentation for the CA SOI Alert Queue REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_AlertQueueResource.html

Alert REST Web Services

You can perform the following operations using the Alert REST web services:

- Get a list of alerts
- Get hyperlink entries associated with an alert
- Get the alert definition
- Get the status information for an alert
- Get a list of escalation policy actions associated with an alert
- Perform an escalation policy action on a specific alert
- Update an alert
- Delete an alert

Note: The complete documentation for the CA SOI Alert REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_AlertResource.html

CI REST Web Services

You can perform the following operations using the CI REST web services:

- Get hyperlink entries associated with a CI
- Get the status information for a CI
- Get the CI USM information
- Get a list of alerts impacting a specific CI

- Get a list of direct children for a specific CI
- Get a list of direct parents for a specific CI
- Get a list of services for a CI

Note: The complete documentation for the CA SOI CI REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_CIResource.html

Configuration REST Web Services

You can perform the following operations using the Configuration REST web services:

- Get a list of configuration nodes
- Get a list of configuration sections for a configuration node
- Get the configuration section definition
- Get hyperlink entries associated with a configuration section
- Update a configuration section

Note: The complete documentation for the CA SOI Configuration REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_ConfigurationResource.html

Customer REST Web Services

You can perform the following operations using the Customer REST web services:

- Get a list of customers
- Get hyperlink entries associated with a customer
- Get the status information for a specific customer
- Get a list of services associated with a customer
- Get a list of alerts on all services associated with a customer
- Get a list of subcustomers
- Get information about the parent customer
- Get information about the selected customers
- Get information about services of a specific customer
- Get the customer definition
- Get a list of services associated with a customer (as XML)

- Create a top-level customer
- Create a subcustomer
- Set customer services
- Update a customer
- Delete a customer

Note: The complete documentation for the CA SOI Customer REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_CustomerResource.html

Email REST Web Services

The CA SOI Email REST web services give you the option to create and send emails using the REST programming interface. You can perform the following operation using the Email REST web services:

- Send an email

Note: The complete documentation for the CA SOI Email REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_EmailResource.html

Escalation Policy Action REST Web Services

Using the Escalation Policy Action REST web services, you can perform escalation policy action-related operations in CA SOI. You can perform the following operations using the Escalation Policy Action REST web services:

- Get a list of escalation policy actions
- Get hyperlink entries associated with an escalation policy action
- Get the escalation policy action definition

Note: The complete documentation for the CA SOI Escalation Policy Action REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_EscalationPolicyActionResource.html

Escalation Policy REST Web Services

You can perform the following operations using the Escalation Policy REST web services:

- Get a list of escalation policies
- Get hyperlink entries associated with an escalation policy
- Get the escalation policy definition
- Create an escalation policy
- Update an escalation policy
- Delete an escalation policy
- Get a list of assigned service IDs for an escalation policy
- Get a list of assigned alert queue IDs for an escalation policy
- Get a list of assigned escalation policy action IDs for an escalation policy
- Get a list of assigned schedule IDs for an escalation policy
- Set a list of escalation policy services
- Set a list of escalation policy alert queues
- Set a list of escalation policy actions
- Set a list of escalation policy schedules

Note: The complete documentation for the CA SOI Escalation Policy REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_EscalationPolicyResource.html

User Group REST Web Services

You can perform the following operations using the User Group REST web services:

- Get a list of groups
- Get hyperlink entries associated with a group
- Get the status information for a group
- Create a group
- Update a group
- Delete a group
- Get a list of users assigned to a group
- Assign users to a group

- Remove a user from a group
- Get the user definition in the assigned group
- Get the user group access status for all alert queues
- Set the user group access status for all alert queues
- Get a list of specific privileged alert queues for a group
- Set a list of specific privileged alert queues for a group
- Get the user group access status for all services
- Set the user group access status for all services
- Get a list of specific privileged customers for a group
- Set a list of specific privileged customers for a group
- Get a list of all the privileges for the Administrator role
- Get a list of all the privileges for the Operator role

Note: The complete documentation for the CA SOI Group REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_GroupResource.html

Meta REST Web Services

Using the Meta REST web services, you can retrieve administrator and operator group privileges:

- Get a definition of the Administrator group
- Get a definition of the Operator group

The GET method is used to perform these tasks.

Note: The complete documentation for the CA SOI Meta REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_MetaResource.html

Schedule REST Web Services

Using Schedule REST web services, you can manage, create, or delete escalation schedules:

- Get a list of schedules
- Create a schedule
- Get schedule details
- Delete a schedule
- Get hyperlink entries associated with a schedule

The GET, POST, and DELETE methods are used to perform these tasks.

Note: The complete documentation for CA SOI Schedule REST web service is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_ScheduleResource.html

Service REST Web Services

You can perform the following operations using the Service REST web services:

- Get a list of services
- Get hyperlink entries associated with a service
- Get the status information for a service
- Get the service USM information
- Get the service metric history information
- Get a list of service alerts
- Get a list of direct children for a service
- Get a list of direct parents for a service
- Get a list of services based on service IDs
- Get a list of subservices
- Create a service
- Update a service
- Delete a service

Note: The complete documentation for the CA SOI Service REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_ServiceResource.html

User REST Web Services

You can perform the following operations using the User REST web services:

- Create a user
- Get a list of users
- Get hyperlink entries associated with a user
- Get the user definition
- Get a list of groups associated with a user
- Update a user

Note: The complete documentation for the CA SOI User REST web services is available at:

https://<ui-server>:<ssl port>/rest/docs/rest/resource_UserResource.html

Supported REST HTTP Methods

As an integration developer, you use REST HTTP methods with the REST web service URLs to manage information in your environment. REST HTTP methods help you achieve the following objectives:

- Access and modify associated resources
- Send an HTTP request to the server for the resource that you want to manipulate
- Control the attributes that you want to retrieve using HTTP headers

CA SOI REST web services support the following REST HTTP methods:

POST (Create)

Creates a resource. The web service can respond with data or status indicating a success or failure.

GET (Read)

Performs a query on a resource and retrieves data. The data that is returned from the web service is a representation of the requested resource.

PUT (Update)

Updates an existing resource.

DELETE (Delete)

Removes an existing resource.

Appendix D: Customizing the Operations Console Menu

For more information about the Operations Console, see Operations Console Basics (see page 79).

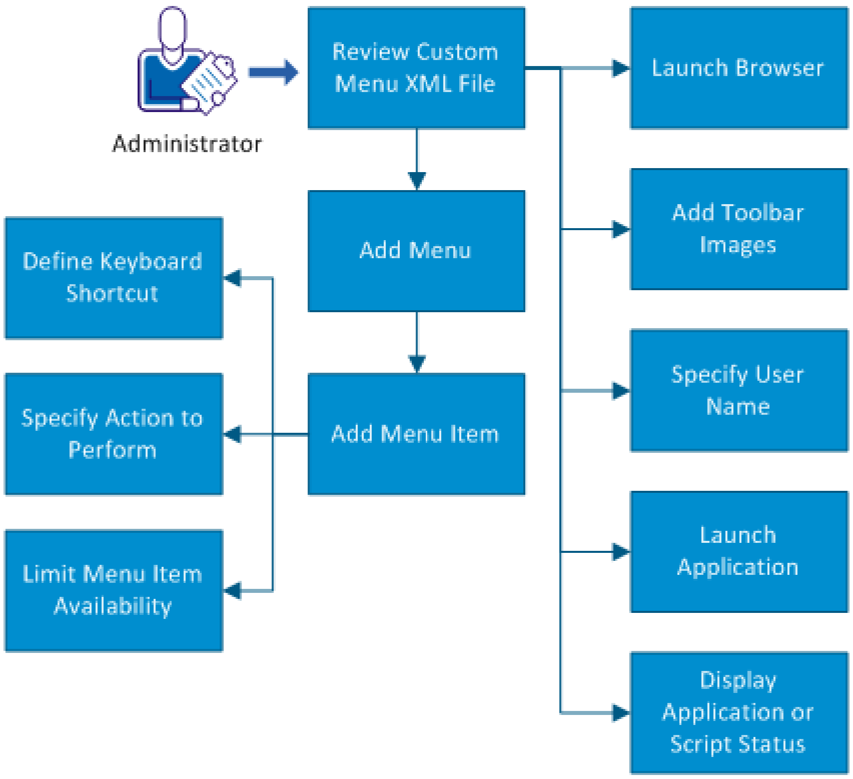
This section contains the following topics:

How to Customize the Operations Console Menu

As an administrator, you can add new menus and new menu items to the Operations Console interface. You can use new menu items to launch URLs, third-party applications, and scripts, and to pass parameters to them.

Use this scenario to guide you through the process:

How to Customize the Operations Console Menu



1. Review the custom-menu-config.xml file (see page 288).
2. Add a menu (see page 289).
3. Add a menu item (see page 290), then perform any of the following actions:
   - Define a keyboard shortcut (see page 291).
   - Specify an action to perform (see page 292).
   - Limit the availability of a menu item (see page 294).
4. Launch a browser (see page 296).
5. Add toolbar images (see page 299).
6. Specify a user name (see page 300).
7. Launch an application. (see page 300)
8. Display the status of a launched application or script (see page 303).

custom-menu-config.xml File

The custom-menu-config.xml file in either of the following folders contains examples of how to add custom menus and custom menu items to the Operations Console:

- SOI_HOME\tomcat\webapps\sam\WEB-INF\console\config
- SOI_HOME\SamUI\webapps\sam\WEB-INF\console\config

Use the <menu> and <item> XML elements to create menus and menu items. The <menu> element can enclose one or more <item> elements that define the commands on the menu. The <item> element can enclose several other elements that define how the menu item appears and behaves. The following table describes each element:

Element	Parent Element	Description
<menu>	<root>	Defines the menu. The name attribute defines the name of the menu.
<separator>	<menu>	Defines a separator line. Use it before an <item> element.
<item>	<menu>	Defines an item on a menu. Use the name attribute to define the item name.
<privilege>	<item>	Associates a privilege to the menu item. A user who does not have this privilege cannot access the menu item.

<toolbar-image>	<item>	Specifies the image to display for the menu item and its associated toolbar button.
<toolbar-image-rollover>	<item>	Specifies the toolbar image displayed when a user places the cursor hovers over the toolbar button.
<toolbar-image-disabled>	<item>	Specifies the toolbar image displayed when the functionality is disabled (not available to the user). A typical representation for this state is an image that is 80% dimmed.
<accelerator>	<item>	Defines a keyboard sequence that completes the action that the menu item defines.
<action>	<item>	Defines the action that the menu item performs.
<hot-key>	<item>	Underlines the first instance of the indicated letter as a keyboard shortcut, and performs the action when that letter is pressed.

Add a Menu

The <menu> element is used to create an Operations Console menu.

Follow these steps:

1. Open the custom-menu-config.xml file (see page 288).

   Note: The <root> element is the first element for this file. You must define all new menus inside the <root> element.

2. Add a new menu using the <menu> element. This element has one attribute, name, which defines the menu name.

   Note: Some examples in the custom-menu-config.xml file show a fully qualified menu name that references a Java class. For example, com.aprisma.spectrum.app.swing.window.menu.Tool is the name attribute in the <menu> element for the Tools menu. You do not have to use a fully qualified name; simply use the exact text that you would like for the menu name.

3. Add items to the new menu using the <item> element and its child elements.

   Note: For more information, see Add a Menu Item (see page 290). If you do not specify menu items, the menu is not visible in the Operations Console.

4. Save the changes you have made to custom-menu-config.xml.

5. Restart the Operations Console to view and test the new menus.

Example: Add a New Menu

This example shows a new Connections menu.

```
<menu name="Connections">
    <item name="Ping Local">
        .
        .
        .
    </item>
    <item name="Launch Diagnostics">
        .
        .
        .
    </item>
</menu>
```

Add a Menu Item

To add an item to an existing menu, create an <item> element inside a <menu> element.

Note: The item is also added to the context menu.

Follow these steps:

1. Open the custom-menu-config.xml file (see page 288).

2. Find the <menu> element to which you want to add items.

3. Create new menu items using the <item> element. This element has one attribute, name, which defines the name of the menu item.

4. Add toolbar images (see page 299).

5. Specify an action to perform (see page 292)

6. (Optional) Define a keyboard shortcut (see page 291).

   Note: The <item> element has several child elements that define how the item behaves. For more information, see custom-menu-config.xml File (see page 288) and subsequent procedures.

7. Save the changes you have made to custom-menu-config.xml.

8. Restart the Operations Console to view and test the new menu items.

Example: Add a New Menu Item

This example adds a menu item named Ping Local to a menu named Connections.

```
<menu name="Connections">
    <item name="Ping Local">
      <accelerator modifiers="2">VK_I</accelerator>
      <action>
        <filter>
           <has-attribute>AttributeID.NETWORK_ADDRESS</has-attribute>
        </filter>
        <context>com.aprisma.spectrum.app.topo.client.render.ModelContext
        </context>
        <context>com.aprisma.spectrum.app.alarm.client.group.AlarmContext
        </context>
        <launch-application>
           <platform>
              <os-name>Windows 9x</os-name>
              <command>command.com /c start "Local ping {0}" cmd.exe /c
              "ping.exe {0} &amp;&amp; pause"</command>
           </platform>
           <platform>
              <os-name>Windows</os-name>
              <command>cmd.exe /c start "Local ping {0}" cmd.exe /c "ping.exe
              {0} &amp;&amp; pause"</command>
           </platform>
           <platform>
              <command>/usr/dt/bin/dtterm -e ping -s {0}</command>
           </platform>
           <param>
              <attribute>AttributeID.NETWORK_ADDRESS</attribute>
           </param>
        </launch-application>
      </action>
    </item>
</menu>
```

Define a Keyboard Shortcut

The optional child attribute <accelerator> of a menu item lets you specify a keyboard shortcut that completes a menu action. It consists of the following items:

- The *modifiers* attribute is an integer that indicates the key or keys to use with a text character:

  1 = Shift

  2 = Ctrl

  3 = Ctrl+Shift

8 = Alt

9 = Alt+Shift

10 = Ctrl+Alt

- The code *VK_X* where *VK_* is fixed code and *X* is the capital letter of the text character.

Example: Define a Keyboard Shortcut

This example specifies that the menu action is performed by pressing Ctrl+L.

```
<accelerator modifiers="2">VK_L</accelerator>
```

Specify an Action to Perform

The <action> element specifies the action that the menu item performs. You can use the child elements shown in the following table to specify a particular action.

The <context> element specifies when the menu item is active so that the action can be run. This applies to both the standard and the shortcut menus. You can specify a ModelContext, which indicates that the action is available when you select a CI. You can also specify an AlarmContext, which indicates that the action is available when you select an alert.

```
<context>com.aprisma.spectrum.app.topo.client.render.ModelContext
</context>
<context>com.aprisma.spectrum.app.alarm.client.group.AlarmContext
</context>
```

You can specify one or both contexts. If no specified context matches the current window context, the menu item is disabled. If no contexts are specified, the menu item is displayed in all contexts.

The following table describes the elements used to implement an action.

Element	Parent Element	Description
<context>	<action>	Specifies when the menu item is active so that you can perform the action.
<filter>	<action>	Limits the display of menu items.
<has-attribute>	<filter>	Specifies the attribute on which to filter.
<and>, <or>, <value>, <equals>	<filter>	Creates an expression for use with a filter.

Element	Parent Element	Description
<launch-browser>	<action>	Opens a browser. See Launch a Browser for more information.
<launch-sso-browser>	<action>	Opens a browser and includes in the URL a single sign-on token associated with the current session. You can use this token to reauthenticate the session across integrated web applications instead of prompting repeatedly for a user name and password. See Launch a Browser for more information.
<url>	<launch-browser>	Specifies the URL to launch in the browser.
<launch-application>	<action>	Opens an application. See Launch an Application for more information.
<launch-web-server-script>	<action>	Launches a script available on the web server. See Launch a Web Server Script for more information.
<display-output>	<launch-application>, <launch-web-server-script>	Displays the output from the script you ran. For more information, see Display the Status of a Launched Application or Script.
<display-exit-status>	<launch-application>, <launch-web-server-script>	Displays the exit status of a launched script.
<command>	<launch-application>, <launch-web-server-script>, <platform>	Specifies the application or script that the menu item launches.
<platform>	<launch-application>	Used with <os-name> to specify the application to launch based on the client operating system.

Element	Parent Element	Description
<os-name>	<platform>	Used with <platform> to specify the application to launch for the client operating system.
<param>	<url>, <command>	Specifies a parameter that is passed to a browser, program, or script.
<attribute>	<param>	Specifies an attribute used as a parameter.

Limit the Availability of Menu Items

The <filter> element specifies a filter that further restricts the enabled state of the menu item. You can filter on any attribute of the selected context. For example, the following code shows that the action needs the IP address of the alerted CI. Therefore, it is enabled only if the CI has the IP address attribute populated.

```
<filter>
   <has-attribute>AttributeID.NETWORK_ADDRESS</has-attribute>
</filter>
```

You can specify complex attribute filters with any combination of nested, and, and or filters.

For more information, see Attribute Filter Syntax (see page 295).

Example: Nested Filters

The following example enables the item if the selected model has the Network_Address attribute and the Condition (ID 0x1000a) attribute is RED.

```
<filter>
   <and>
      <has-attribute>AttributeID.NETWORK_ADDRESS</has-attribute>
    <equals>
      <attribute id="AttributeID.CONDITION">
         <value>43</value> <!--red-->
      </attribute>
    </equals>
   </and>
</filter>
```

Attribute Filter Syntax

The file SOI_HOME\SamUI\webapps\sam\WEB-INF\common\schema\attribute-filter.xsd contains the complete syntax for attribute filters.

Notes:

- For examples of how to filter menu items, see Limit the Availability of Menu Items (see page 294).
- If you use an attribute other than the attributes listed in the following tables, specify the attribute using its hexadecimal attribute ID.

The following table defines commonly used attributes where an attribute ID is expected.

Constant	Attribute
AttributeID.NETWORK_ADDRESS	Network Address
AttributeID.MTYPE_NAME	CI Class name
AttributeID.MODEL_OBJECT	CI Handle
AttributeID.MODEL_NAME	CI Name
AttributeID.MODEL_CLASS	CI Class
AttributeID.CONDITION	Condition
AttributeID.DOMAIN_ID	SA Manager ID
AttributeID.DOMAIN_NAME	SA Manager name

You can use the constants in the following table for the indicated alert attributes:

Constant	Attribute
AlarmAttrID.ACKNOWLEDGED	Acknowledged
AlarmAttrID.ALARM_ID	Alert ID
AlarmAttrID.ALERTDETAIL	Alert Detail
AlarmAttrID.ASSIGNED	Assignment
AlarmAttrID.CONNECTOR_NAME	Connector Name
AlarmAttrID.DESCRIPTION	Description
AlarmAttrID.CREATION_DATE	Creation Date
AlarmAttrID.EVENT_SOURCE	Source Name
AlarmAttrID.EVENT_SOURCE_ID	Source Alarm ID

Constant	Attribute
AlarmAttrID.EVENT_OCCURRED	Source Creation Date
AlarmAttrID.PRIORITY	Service Impact
AlarmAttrID.SEVERITY	Severity
AlarmAttrID.SITUATION_TYPE	Category
AlarmAttrID.TICKET_ID	Ticket ID
AlarmAttrID.USER_CLEARABLE	User Clearable

Launch a Browser

The <launch-browser> element lets you launch a specified URL in a browser and pass parameters to the URL. These parameters can be hard-coded values or values from model attributes.

Note: For more information about parameters, see the definition of <param-type> in the file SOI_HOME\SamUI\webapps\sam\WEB-INF\common\schema\basic-config.xsd.

Example: <launch-browser> Code

This example launches the default browser on the client computer. The <url> element specifies the URL pattern. You can specify parameters to substitute in the URL pattern by enclosing the parameter number (starting at 0) in curly braces {}. You then specify <param> elements for each parameter.

```
<launch-browser>
   <url>http://{0}</url>
   <param>
      <attribute>AttributeID.NETWORK_ADDRESS</attribute>
   </param>
</launch-browser>
```

CA SOI processes the <param> elements in order so that the first one corresponds to the 0th parameter in the URL pattern. A <param> element has a specific syntax. The most common element is <attribute>, which substitutes the value of the specified attribute for the selected context. In this example, the value of the Network Address attribute is substituted in the URL pattern.

Important! See Characters in URLs (see page 297) for information about the characters to use and not to use in URLs.

Characters in URLs

This section discusses the characters to use or avoid in URLs.

Standard Characters

The URL formatting must adhere to the standards published in the Internet Engineering Task Force (IETF) RFC 1738. Use of non-standard characters in URLs results in unreliable browser performance including the browser not locating the specified web page.

Spaces and Commas

If you use spaces or commas, convert them to their ASCII equivalent. URL encoding consists of a percent (%) symbol followed by the two-digit hexadecimal representation (case-insensitive) of the ISO-Latin code point for the character.

- For spaces, use %20
- For commas, use %2C

Note: Some browsers encounter problems processing URLs even with this encoding.

Ampersands

If you use ampersands, convert them to &amp.

CDATA

You can put URLs inside a CDATA section so that they are not parsed, which avoids possible problems with URLs and the XML parser.

Comply with the CDATA requirements, including the following:

- A CDATA section cannot contain the string "]]>"; therefore, nested CDATA sections are not allowed.
- Use no spaces or line breaks inside the "]]>" string.

Unsafe Characters

The following table lists characters that are easily misinterpreted in URLs. Always substitute these characters with % followed by the hexadecimal code points listed in the table. For example, use %20 to represent a space in a URL.

Character	Code Points (Hex)
Space	20
Quotation marks (")	22
Less Than symbol (<)	3C
Greater Than symbol (>)	3E
Pound character (#)	23
Percent symbol (%)	25
Left Curly Brace ({)	7B
Right Curly Brace (})	7D
Vertical Bar/Pipe (|)	7C
Backslash (\)	5C
Caret (^)	5E
Tilde (~)	7E
Left Square Bracket ([)	5B
Right Square Bracket (])	5D
Grave Accent (`)	60

Reserved Characters

The following table lists characters that have special uses in URLs. Substitute such characters with % followed by the hexadecimal code points listed in the table when they are used as regular text and not in their special role. For example, use %24 to represent a plain-text dollar sign ($) in a URL.

Character	Code Points (Hex)
Dollar ($)	24
Ampersand (&)	26 (or "&amp" as explained earlier)
Plus (+)	2B
Comma (,)	2C

Character	Code Points (Hex)
Forward slash/Virgule (/)	2F
Colon (:)	3A
Semi-colon (;)	3B
Equals (=)	3D
Question mark (?)	3F
At symbol (@)	40

Add Toolbar Images

Toolbar images have the following states, which you specify in your menu item definition. The elements for toolbar states are as follows:

- <toolbar-image>
- <toolbar-image-rollover>
- <toolbar-image-disabled>

For more information, see custom-menu-config.xml File (see page 288).

You can use the following formats for toolbar images: .png, .gif, .jpg, and .jpeg. We recommend the size 24 x 24 pixels.

Create the images directory at the following location: SOI_HOME\ui\tomcat\custom\images directory. Store your custom images at this location. When you reference an image in this directory, specify the path from the images directory, for example, images\myimage.png.

Example: Specify a Toolbar Image

This example points to the hints.gif file:

```
<toolbar-image>images/hints.gif</toolbar-image>
```

Specify a User Name

You can pass a user name to an application, web browser, or script. Use the following expression to specify the name of the logged-in user:

```
<param>
   <expression>
      com.aprisma.spectrum.app.util.context.DefaultApplicationContext.

getGlobalParameter(com.aprisma.spectrum.app.util.context.ApplicationContext.
      USER_PARAMETER_NAME)
   </expression>
</param>
```

Example: Pass User Name to Browser

This example opens a browser and passes a user name to it.

```
<launch-browser>
   <url> http://acme.com?user={0}</url>
   <param>
   <expression>
      com.aprisma.spectrum.app.util.context.DefaultApplicationContext.

getGlobalParameter(com.aprisma.spectrum.app.util.context.ApplicationContext.
      USER_PARAMETER_NAME)
   </expression>
   </param>
</launch-browser>
```

Launch an Application

The <launch-application> element lets you start a command or program.

<command> Element

The <command> element specifies the command or program to run. You can provide the path to the command or program in one of the following ways:

Environment variable

In a Solaris environment use the PATH variable. To create an environment variable on Windows, right-click My Computer, select Properties and Advanced, and click the Environment Variables button.

Absolute path

The path must be the same on each CA SOI client. Path statements on Windows should have a double backslash instead of a single backslash, for example:

```
C:\\Windows\\system32\\cmd.exe
```

The following syntax rules apply to the <command> element:

- Spaces delimit command arguments.
- Spaces in an argument are surrounded by quotation marks or preceded by the backslash escape character (\).
- Quotation marks in an argument are preceded by the backslash escape character (\).
- CA SOI automatically surrounds command arguments that contain commas with quotation marks, which is important to know if you parse a numeric argument that contains commas.
- CA SOI replaces arguments that return null or have a string length of zero with empty quotation marks (“ ”).

<validate> Element

The <validate> element verifies that the command or program exists on the client and has run permissions. If either of these conditions is not met during startup, the associated menu item is not added to the menu.

If the <validate> element is not used, the menu item is always added to the menu, but its state is determined by the value of other elements.

The <validate> element requires an absolute path in the <command> element, as shown in the following example:

```
<launch-application>
   command>c:\\windows\\system32\\notepad.exe</command>
   <validate/>
</launch-application>
```

Examples: Launch an Application

The following are two examples for launching an application:

- This example launches an application called myapp on the client machine and passes the IP address of the selected model. As with the <launch-browser> action, you can substitute any number of parameters.

  ```
  <launch-application>
     <command>myapp {0}</command>
     <param>
        <attribute>AttributeID.NETWORK_ADDRESS</attribute>
     </param>
  </launch-application>
  ```

- This example uses the <platform> element to specify commands for different platforms. The <os-name> element specifies the operating system name and the <command> element specifies the command to run on that operating system. The <os-name> element is optional. If you do not specify <os-name>, the associated command is the default such that if no other platforms match, the default command runs.

```
<launch-application>
   <platform>
      <os-name>Windows</os-name>
      <command>cmd.exe /c start "ping {0}" cmd /c "ping.exe {0}
      &amp;&amp;pause"</command>
   </platform>
   <platform>
      <os-name>SunOS</os-name>
      <command>>/usr/dt/bin/dtterm -e ping {0}</command>
   </platform>
   <param>
      <attribute>AttributeID.NETWORK_ADDRESS</attribute>
   </param>
</launch-application>
```

At runtime, the specified OS names are compared to the OS name returned by the *os.name* Java property. A best-match algorithm lets you specify only a prefix of the OS name. The following are valid OS names:

- SunOS for the Solaris platform
- Windows for all Windows platforms
- Windows 9x for Windows 95/98
- Windows 2000 for Windows 2000
- Windows 2003 for Windows 2003
- Windows XP for Windows XP
- Windows Vista for Windows Vista and Windows Server 2008
- Linux for the Linux platform
- Mac for the Macintosh platform

If no specified platforms match, the associated menu item is disabled.

Display the Status of a Launched Application or Script

Use the <display-exit-status> and <display-output> elements with <launch-web-server-script> and <launch-application> to display the exit status and the output from the script or application.

By default <display-exit-status> displays “Success” if the exit code is 0 and “Failed with error code #” otherwise. You can change the default behavior by specifying <status> child tags that map an exit code to a custom message to display.

Example: <display-exit-status> Code

This example maps status codes 1, 2, and 3 to specific message strings. The last status code specifies default=“true”, mapping all other error codes except 0, which by default maps to “Success.” If exit code 0 does not indicate success, you can override it with a <status> tag. The {0} in the message string substitutes the exit code.

```
<display-exit-status>
   <status code="1">Could not open file</status>
   <status code="2">Bad parameter</status>
   <status code="3">Could not connect to the server</status>
   <status default="true">Unknown error code {0}</status>
</display-exit-status>
```

By default, <display-output> displays both the standard output and standard error output from the process. You can display only the standard output by specifying:

```
<display-output stdout="t"/>
```

or only the standard error output by specifying:

```
<display-output stderr="t"/>
```

Note: The <display-exit-status> and <display-output> elements can be used only for command line applications or scripts and not GUI applications. The interface waits for the script to finish before being available to the user again.

Appendix E: Database Maintenance

This section describes the database maintenance requirements for the SA Store.

This section contains the following topics:

CA SOI Toolbox Utility

As an administrator, you use the CA SOI toolbox application to manage the maintenance of data in your CA SOI SA Store database. The toolbox is a command line utility which allows you to start and stop specific connectors and services, enabling efficient cleanups of your CA SOI instance.

The toolbox lets you clear unwanted data from your database. You can clear history data, imported data from connectors, and security data, individually or all at once.

The CA SOI toolbox is on the SA Manager in the SOI_HOME\Tools folder. Navigate to this location on a command prompt and run the following command with the options/parameters described in the ensuing sections:

```
soitoolbox
```

Note: The command help also contains information about the functions of the options and commands at are described in this section. For practical examples of using the utility, see How to Clean Up Data with the CA SOI Toolbox (see page 310).

Configuration Options

This section describes the different commands for the CA SOI toolbox that you can use to configure a CA SOI instance. In all commands, include the necessary options to establish a valid connection with the SA Store database. If you do not, the utility prompts you for the necessary information.

-m, --machine

Specifies the system to connect to which runs the SA Store database.

Default: localhost

-n, --mUsername

Specifies the name of the user who has access to the database system.

Note: This command is not valid and has no effect when using the localhost system.

Default: Administrator

-w, --mPassword

Specifies the password of the Windows users in plain text.

Note: This command is not valid and has no effect when using the localhost system.

-d, --dbName

Specifies the name of the CA SOI database.

Default: SAMStore

--dbArchiveName

Allows you to specify a new name for the archive database.

-u, --dbUsername

Specifies the user with privileges to access the CA SOI database.

Default: sa

-p, --dbPassword

Specifies the password for the database user in plain text.

Note: If the password is not specified, the utility requests it during runtime.

--credentials

Specifies the location of the file containing the user names and passwords for all systems that run CA SOI components. This command is required when you operate a distributed CA SOI instance.

-x

Creates a configuration file template if the file does not exist.

Note: This command is the equivalent of *--credentials=soitoolbox.cfg*.

-q, --quiet

Specifies that the user is not asked to confirm the running of a destructive operation.

-t, --timeout

Specifies the generic timeout in seconds.

Default: 30

-b, --dbConnectionTimeout

Specifies the timeout in seconds for the initial wait time for the opening of the database connection.

Default: 30

-c, --connector

Specifies the connectors to be used in action commands.

Default: *

Note: * in this case means all connectors in a CA SOI instance. The following examples show how the * symbol can be used:

```
--connector=CA:09998_soimachine.ca.com, CA:00005_soimachine.ca.com
--connector=CA:09998_*
--connector=CA:*_soimachine.ca.com
--connector=*
```

-s, --beSmart

Activates a special method for stopping connectors. In beSmart mode, the utility only stops components (services and connectors) which affect or can be affected by an action command.

Note: This option requires that you include --*credentials.*

Service Related Action Commands

You can use the following action commands to stop, start, and restart the services in a CA SOI instance. You can also use the utility to get information about the status of your services. The cleanup actions require the services to stop before the cleanup and restart after the cleanup. If you do not stop and restart the services, the utility performs the tasks automatically at the appropriate times.

These commands are:

--stopAllServices

Stops all the Windows services in a CA SOI instance.

--startAllServices

Starts all the Windows services in a CA SOI instance.

--restartAllServices

Restarts all the Windows services in a CA SOI instance by stopping and starting them.

--getServiceStatus

Displays the status of all the Windows services in a CA SOI instance.

Connector and Database Related Action Commands

Use the following action commands to manage and view the connector status. If you are cleaning up connector data, stop the connector before doing so.

--startConnector

Starts the connectors which you specify in the --*connector* parameter.

Note: Provide the --*credentials* parameter to use this command.

Important! If the CA SOI UI Server is not running, the command fails.

--stopConnector

Stops the connectors which you specify in the --*connector* parameter.

Note: Provide the --credentials parameter to use this command.

Important! If the CA SOI UI Server is not running, the command fails.

--getConnectorStatus

Provides the status of all the connectors in a CA SOI instance, including system connectors.

--getAvailableConnectors

Lists the names of all the connectors present in a CA SOI instance, excluding system connectors.

--getStatisticalData

Displays statistical data from the CA SOI database. This data includes information on the number of CIs, Alerts, and Services.

Note: The *--connector* option influences the output of this command.

Database Cleanup Commands

You can use the following commands to clean up the data in a CA SOI database.

--archiveHistoryData

Moves all historical data older than a specified number of days to an archive database.

Note: You specify the number of days by adding a number to the end of the command, for example --archiveHistoryData=10.

Note: The default name for the archive database is SOIArchiveDB. You can change the name of the archive database with the *--dbArchiveName* command.

--cleanHistoryData

Deletes all the historical data from the CA SOI database that is older than a specified number of days.

Note: You specify the number of days by adding a number to the end of the command which specifies the number of days.

--cleanImportedData

Deletes all the data that came from connectors that you specify in the *--connector* parameter.

Note: This command does not delete data that users create manually.

--cleanSecurityData

Deletes all service access rights that are set for specific users and groups within the CA SOI instance.

--cleanData

Deletes all history data, imported data, and security data for all the connectors in a CA SOI instance.

--purgeClearedAlerts

Deletes cleared alerts from the database that are older than a specified number of days. You can specify two different purge types, :*full* or :*strict*, by adding *full* or *strict* to the end of the command:

:full

Deletes all alerts that are cleared in at least one system.

:strict

Deletes only those alerts which are cleared in all systems.

--rebuildIndexes

Rebuilds database indexes.

--reinitializeDB

Clears the whole CA SOI database, deleting the data from all the tables.

Note: You can use this command to start with a clean state similar to that of a new installation.

--restoreHistoryData

Restores from the archive database all archived historical data that are not older than the specified number of days.

Note: You specify the number of days by adding a number to the end of the command, for example --restoreHistoryData=10.

How to Clean Up Data with the CA SOI Toolbox

As an administrator, you maintain the CA SOI database. You ensure that your database runs efficiently and that the data it maintains is the data you need. Using the CA SOI Toolbox command utility, you can clean up the following data types:

- Imported data from a specific connector
- History and security data
- All the data that is maintained in a CA SOI instance

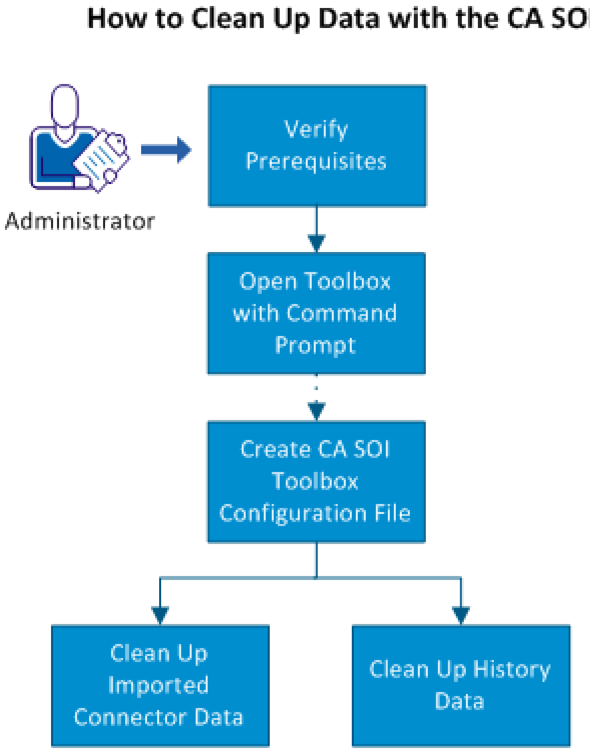
You may want to clean up data for the following reasons:

- You want to clean up data from a connector in your CA SOI instance that was not written correctly. Thus, the connector provides flawed data (for example, CIs using incorrect naming conventions) that does not correlate with data provided from other connectors.
- You want to maintain a more efficient CA SOI instance that does not maintain history that you do not need and consumes needed disk space. Thus, you clean up the history data that is no longer of use.

- Clear all security data for all users and user groups in a CA SOI instance.
- You want to restart a CA SOI instance from a clean state and clear all its data. This option is useful during the product implementation phase when incorrect connector configurations can cause database *pollution*.

Note: This scenario provides examples of commands for removing connector and history data. For detailed definitions of every parameter available, see the command help that comes with the toolbox.

Use this scenario to guide you through the process:


How to Clean Up Data with the CA SOI Toolbox
Administrator
Verify Prerequisites
Open Toolbox with Command Prompt
Create CA SOI Toolbox Configuration File
Clean Up Imported Connector Data
Clean Up History Data

1. Verify the prerequisites.
2. Determine the database sizing (see page 312).
3. Open the toolbox with a command prompt (see page 315).
4. (Optional) Create a CA SOI Toolbox configuration file (see page 316).
5. Do any of the following:
   - Clean up the history data (see page 317).
   - Clean up imported connector data (see page 318).

CA SOI Toolbox Prerequisites

To use the CA SOI toolbox, you must have the following information:

- The server credentials for the CA SOI instance
- The database location and credentials for the CA SOI instance if the database location is on a remote system

  Note: If you run an instance all on one server locally, you do not need credentials for the database.
- The name of the connector, If you want to perform a connector-specific cleanup

System Requirement:

- The CA SOI Toolbox requires that your system has the Microsoft Visual C++ 2008 Redistributable Package (x86) installed.

Determine Database Sizing

Maintaining the SA Store database is required to sustain consistent performance and maintain product function. Use the data provided in this section that is measured against the disk space and performance capabilities of your database server. You can then determine how often to perform maintenance.

The following tables display estimates of how you can expect the database to grow over time. They project growth over a three-year period for several implementation sizes.

Note: All tables assume that you have defined an SLA for every managed service.

Small (100 services, 1000 alerts per day)

Item	Amount	Average Row Size (KB)	Number of Rows	Disk Space Requirement (MB)
Managed CIs	20,000	.85	60,000	51
Staged CIs	100,000	1.345	300,000	403.5
Alerts	1,095,000	.6	3,285,000	1,971
Alert History		1.062	2,190,000	2,325.78
SLA	100	.3	109,500	32.85
History tables		.65	5,256,000	3,416

Item	Amount	Average Row Size (KB)	Number of Rows	Disk Space Requirement (MB)
Total table size				8,201
Database log file				4,920
Total size				13,121

Mid-sized (500 services, 5000 alerts per day)

Item	Amount	Average Row Size (KB)	Number of Rows	Disk Space Requirement (MB)
Managed CIs	50,000	.85	150,000	127.5
Staged CIs	500,000	1.345	1,500,000	2,018
Alerts	5,475,000	.6	16,425,000	9,855
Alert History		1.062	10,950,000	11,629
SLA	500	.3	547,500	164.25
History tables		.65	26,280,000	17,082
Total table size				40,875
Database log file				24,525
Total size				65,400

Large (1,000 services, 10,000 alerts per day)

Item	Amount	Average Row Size (KB)	Number of Rows	Disk Space Requirement (MB)
Managed CIs	100,000	.85	300,000	255
Staged CIs	1,000,000	1.345	3,000,000	4,035
Alerts	10,950,000	.6	32,850,000	19,710
Alert History		1.062	21,900,000	23,258

Item	Amount	Average Row Size (KB)	Number of Rows	Disk Space Requirement (MB)
SLA	1,000	.3	1,095,000	328.5
History tables		.65	52,560,000	34,164
Total table size				81,750
Database log file				49,050
Total size				130,800

Review the following considerations when interpreting these estimates:

- The Amount column lists the actual amount of each entity in CA SOI at the end of the three-year period. The Number of Rows column is larger than the actual amount in most cases.
- The SA Store tables not represented in this table are small enough that they have a negligible impact on database size.
- The History table row calculation is based on the fact that the three history tables (DBAvailHistory, DBQualityHistory, and DBRiskHistory) create a row every thirty minutes per service. Therefore, the history tables generate 48 rows per day per service.
- Plug your numbers into the table (total number of managed and staged CIs, average alerts received per day, and number of SLAs defined) that most closely approximates your implementation size to calculate the projected database growth rate for your implementation.
- The database log file is approximately 60 percent of the total database size.

Based on this data, you can make the following assumptions:

- At the end of a three-year period, the total disk space consumed by the SA Store database would be between 10,000-100,000 MB or 10-100 GB depending on the number of managed services, CIs, and alerts.
- You can expect a growth rate of roughly 2.7 GB per 1000 services per month, or 1.35 GB per 500 services per month, or 270 MB per 100 services per month.
- Consider these estimates when planning the frequency of maintenance to help ensure that the SA Store does not grow to an unmanageable size. As a best practice, the row count for all tables should be limited so that SQL queries on any table can complete within a few seconds. For example, if you find that this limit is around 10,000,000 rows per table on your database server, you would have to at least archive and purge the history tables periodically depending on implementation size to keep them from growing beyond this threshold.

Open the Toolbox with a Command Prompt

To use the toolbox to run its commands, open the toolbox with a command prompt.

Follow these steps:

1. Navigate to the CA SOI toolbox on the SA Manager in the <SOI_Home>\Tools folder.
2. Run the following command from the command prompt:

   ```
   soitoolbox
   ```

   The toolbox file opens in the command window and lists all the commands of the toolbox in the command help.

   Note: The following steps of this scenario provide two examples of different ways you can use the toolbox to clean up data.

Create a CA SOI Toolbox Configuration File

For CA SOI instances that do not run entirely in one local location, create a CA SOI toolbox configuration file. This configuration file allows you to run commands, using the *-x* option. The *-x* option allows you to provide all the credentials of a complex CA SOI instance which is not run in one location locally. To allow the running of commands using the *-x* option for a complex CA SOI instance, create a CA SOI toolbox configuration file.

Follow these steps:

1. Open the toolbox with a command prompt (see page 315).
2. Run the *-x* command from the toolbox.

   The toolbox creates an empty configuration file.

   Important! Before the toolbox creates the empty configuration file, an *ERROR: bad content - File not found* message appears. Disregard this message.
3. Open the empty configuration file *soitoolbox.cfg* in a text editor.

   The empty configuration file, which is a template, opens displaying instructions with placeholders.
4. Specify all the information for your CA SOI instance in the configuration file placeholders.

   Note: The file contains instructions about the information that you specify.
5. Save the configuration file with the changes you made.

   Your CA SOI instance now has a toolbox configuration file which you can use to run toolbox commands by using the *-x* option.

Note: Include the *-x* option before any call or command instead of specifying specific credentials when using the CA SOI toolbox. For example, you would run the following command to get a list of all the connectors in CA SOI instance after you set up the configuration file:

```
soitoolbox -x --getAvailableConnectors
```

Important! If you use the *-x* option, do not use the *-m* option to specify a machine. If you use both options in a command, an error occurs.

Clean Up History Data

When history data is no longer useful and you do not want to store in your database, you can clean up the history data. Maintenance of history data is important, because the history data can increase over time and can consume memory, thus adversely affecting the operation of the database. You can avoid buildup of unwanted data by cleaning up history data at regular intervals. With this command, you clean data which is older than a specified number of days. To clear unwanted history data in a database, run a cleanup command from the toolbox folder on a command prompt.

Follow these steps:

1. Open the toolbox with a command prompt (see page 315).
2. Run the history cleanup command and specify the database connection password. For example, if your database connection password is *yourpw*, and you want to delete history data that is older than 2 days, you would run:

   ```
   soitoolbox -p yourpw --cleanHistoryData=2
   ```

   -p

   Specifies the password. In this example, the password is *yourpw.*

   --cleanHistoryData

   Runs the command for deleting history data.

   2

   Specifies that only history data that is older than two days is deleted.

   The toolbox confirms that it found the services, connects to the database, and warns that you selected a destructive operation.

   Important! The example command assumes that your CA SOI instance runs entirely on a local system. If you are running a CA SOI instance that is not located entirely in one location, create a toolbox configuration file. For information about creating the toolbox configuration file, see Create a CA SOI Toolbox Configuration File (see page 316).

3. When prompted, confirm the destructive operation by typing Y for Yes.

   The toolbox verifies that CA SOI is running, and then asks you to stop the services before proceeding.

4. Confirm that you want to stop the services by typing Y for Yes.

   The toolbox stops the services and then deletes all the history data in the database.

5. Verify that the imported connector data was deleted by running the --*getStatisticalData* command.

   The toolbox returns information about the statistical data for the connector, confirming that the history data was deleted.

Clean Up Imported Connector Data

When a connector provides data that you do not want to store in your database, you can clean up data from the connector. To clean up imported connector data, run a cleanup command from the toolbox folder on a command prompt.

Follow these steps:

1. Open the toolbox with a command prompt (see page 315).
2. Run the cleanup command with the information about the connector name location and the location of the database where the connector data is stored.

   For example, if you wanted to delete data from the connector *Example_con* stored in a database that resides on the server *server1* with the database connection password *yourpw*, you would run:

   ```
   soitoolbox -p yourpw -m server1 --cleanImportedData --connector=Example_con
   ```

   The toolbox confirms that it found the services, connects to the database, and warns that you selected a destructive operation.

   Important! The example command assumes that your CA SOI instance runs entirely on a single server, *server1* in this case. If you are running a CA SOI instance that is not located entirely in one location, create a toolbox configuration file. For information about creating a toolbox configuration file, see Create a CA SOI Toolbox Configuration File (see page 316).

   Note: If you do not know your connector name, run the --*getAvailableConnectors* command first.
3. When prompted, confirm the destructive operation by typing Y for Yes.

   The toolbox verifies that SOI is running, and then asks you to stop the services before proceeding.
4. Confirm that you want to stop the services by typing Y for Yes.

   The toolbox stops the services and then deletes the imported connector data in the database.
5. Verify that the imported connector data was deleted by specifying the connector name with the --*connector* option and running the --*getStatisticalData* command.

   The toolbox returns information about the statistical data for the connector, confirming that the data was deleted.

   Note: If you are cleaning up data from a connector that is providing incorrect data, fix the connector problems before restarting its services.

Glossary

aggregate propagation

Aggregate propagation indicates a general-purpose relationship that propagates impact from one CI to another.

alert

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

alert escalation

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.

alert filter

An *alert filter* limits the number and alert types that are shown on the Operations Console.

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.

bound propagation

Bound propagation indicates a bidirectional relationship between two CIs. If one CI is bound to another CI and either CI has a severity change, the change results in the same impact on both CIs.

CA Catalyst

CA Catalyst is a platform for federating, correlating, reconciling, and storing high-level, business-relevant data from a wide variety of management products.

CI

See *configuration item*.

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.

custom propagation

Custom propagation indicates that one CI may depend on several other CIs for some behavior or function.

customer

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.

domain manager

A *domain manager* is a management application that provides information to CA Catalyst and CA SOI using a connector.

federation

Federation is the act of joining data from various sources.

group

Groups are intermediate CI objects that collect CIs and relate them to each other by some role or function.

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.

high availability

High availability helps maintain a business continuity during an IT resource interruption. Also known as fault tolerance or failover.

impact

Impact indicates how much a CI affects a service and related CIs.

infrastructure alert

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

integration framework (IFW)

The *integration framework (IFW)* is the mechanism that CA SOI uses to connect to domain managers and gather CI, service, topology, and state information.

JDBC

Java Database Connectivity is a programming interface that lets Java applications access an SQL database.

JMS (Java Message Service)

The *Java Message Service* (*JMS*) is a messaging standard that lets application components that are based on the Java 2 Platform Enterprise Edition (J2EE) create, send, receive, and read messages.

maintenance schedule

A *maintenance schedule* defines a time in the future (which can recur at defined intervals) on which to put a service or CI in maintenance.

MOT

Mean outage time

MTBF

Mean Time Between Failures

MTTR

Mean Time to Repair

operative propagation

Operative propagation indicates that the related item is affected only if the impact value of a CI exceeds a defined threshold.

priority

Priority indicates the importance of a service to the business.

relationship

Relationships in a service model show how CIs are linked to form the service topology.

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).

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.

severity

Severity indicates the condition of a CI as reported from the domain manager to CA SOI through alerts.

significance

Significance indicates the importance of a CI.

subscriber

A *subscriber* is a business service customer.

subservice

A *subservice* is used to indicate a subordinate service model.

synchronization

Synchronization is the CA Catalyst capability of updating source domain manager data due to CI changes. Changes are a result of reconciliation or other changes to data in the Persistent Store, including CI creation and deletion.

UI Server

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

Unified Service Model (USM)

The *Unified Service Model (USM)* is the semantic schema that is used as the CA Catalyst and CA SOI infrastructure.