CA TECHNOLOGIES GREEN BOOKS

CA Service Desk Manager

Integration Best Practices

Volume 1

- CA SERVICE CATALOG
- CA CLARITY™ PROJECT AND PORTFOLIO MANAGER
- CA BUSINESS SERVICE INSIGHT
- CA IDENTITY MANAGER
- CA SITEMINDER®

LEGAL NOTICE

This publication is based on current information and resource allocations as of its date of publication and is subject to change or withdrawal by CA at any time without notice. The information in this publication could include typographical errors or technical inaccuracies. CA may make modifications to any CA product, software program, method or procedure described in this publication at any time without notice.

Any reference in this publication to non-CA products and non-CA websites are provided for convenience only and shall not serve as CA's endorsement of such products or websites. Your use of such products, websites, and any information regarding such products or any materials provided with such products or at such websites shall be at your own risk.

Notwithstanding anything in this publication to the contrary, this publication shall not (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (iii) serve to amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this publication remain at CA's sole discretion.

The information in this publication is based upon CA's experiences with the referenced software products in a variety of development and customer environments. Past performance of the software products in such development and customer environments is not indicative of the future performance of such software products in identical, similar or different environments. CA does not warrant that the software products will operate as specifically set forth in this publication. CA will support only the referenced products in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product.

Certain information in this publication may outline CA's general product direction. All information in this publication is for your informational purposes only and may not be incorporated into any contract. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "AS IS" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, lost investment, business interruption, goodwill or lost data, even if CA is expressly advised of the possibility of such damages.

COPYRIGHT LICENSE AND NOTICE:

This publication may contain sample application programming code and/or language which illustrate programming techniques on various operating systems. Notwithstanding anything to the contrary contained in this publication, such sample code does not constitute licensed products or software under any CA license or services agreement. You may copy, modify and use this sample code for the purposes of performing the installation methods and routines described in this document. These samples have not been tested. CA does not make, and you may not rely on, any promise, express or implied, of reliability, serviceability or function of the sample code.

TITLE AND PUBLICATION DATE:

CA Service Desk Manager Green Book
Publication Date: February 2012

ACKNOWLEDGEMENTS

Principal Authors

Tyson Bell

Amy Chenard

Christy Druzynski

Jeanne Gaskill

Paul Kitko

Raghu Rudraraju

Christophe Trinquet

Donald Weihs

Daniel Zilberman

The principal authors and CA Technologies would like to thank the following contributors:

Harish Goteti

Randal Locke

David Messineo

Michael Haering

Malcolm Ryder

Paul Stiles

Steve Troy

Richard Wu

CA Technologies Support

Third-Party Acknowledgements

CA TECHNOLOGIES PRODUCT REFERENCES

This document references the following CA Technologies products:

- CA Application Performance Management
- CA Asset Portfolio Management (included with the CA IT Asset Manager solution)
- CA Business Intelligence
- CA Business Service Insight (CA BSI) – formerly known as CA Oblicore Guarantee™
- CA Clarity™ Project and Portfolio Manager (CA Clarity PPM)
- CA Cohesion Application Configuration Manager (CA Cohesion ACM)
- CA Configuration Automation – formerly known as CA Cohesion Application Configuration Manager (CA Cohesion ACM)
- CA Customer Experience Manager (CA CEM)
- CA ecoMeter
- CA Embedded Entitlements Manager (CA EEM)
- CA eHealth® (CA eHealth)
- CA Identity Manager
- CA Introscope
- CA IT Client Manager (CA ITCM)

  CA IT Client Manager provides a set of cross-platform product capabilities for Windows, Linux, UNIX, and MAC environments. While CA ITCM was previously sold as a standalone product, it is now included as part of the CA Client Automation and CA Server Automation solutions. CA Client Automation has focus on managing end-user devices such as desktops, laptops, and end-point devices; while CA Server Automation has focus on managing servers. This document refers to the functionality of the CA ITCM product capabilities.

- CA Management Database (CA MDB)
- CA Network and Systems Management (CA NSM)
- CA Process Automation (formerly CA IT Process Automation Manager, CA IT PAM)
- CA Role and Compliance Manager (CA RCM)
- CA Service Catalog (which includes CA Service Accounting)

- CA Service Desk Manager (CA SDM)
- CA Service Operations Insight (CA SOI) – formerly known as CA Spectrum Service Assurance (CA SSA)
- CA SiteMinder® (CA SiteMinder)
- CA Software Change Manager (CA SCM)
- CA Spectrum® (CA Spectrum)
- CA Spectrum Service Assurance (CA SSA)
- CA Workflow

FEEDBACK

Please email us at greenbooks@ca.com to share your feedback on this publication. Please include the title of this publication in the subject of your email response. For technical assistance with a CA Technologies product, please contact CA Support at http://ca.com/support. For assistance with support specific to Japanese operating systems, please contact CA Technologies at http://www.casupport.jp.

Contents

Chapter 1: Introduction

The *CA Service Desk Manager Integration Best Practices Green Book* is comprised of three volumes. Each volume describes ways to improve the process maturity for various ITIL® processes when CA Service Desk Manager (CA SDM) 12.6 is integrated with other CA Technologies solutions. The following ITIL V3 IT Service Management processes are covered in this Green Book:

- Access Management
- Availability Management
- Capacity Management
- Change Management
- Continual Service Improvement
- Demand Management
- Evaluation
- Event Management
- Financial Management
- Incident Management
- Information Security Management
- IT Service Continuity Management
- Knowledge Management
- Problem Management
- Release and Deployment Management
- Request Fulfillment
- Service Asset and Configuration Management
- Service Catalog Management

- Service Level Management
- Service Portfolio Management
- Service Validation and Testing
- Supplier Management
- Transition Planning and Support

Chapter 2 highlights the key objectives and recommended product and solution integrations for each ITIL process. These integrations can help achieve and mature the process goals. Additional products are available that also add value to the ITIL processes. However, Chapter 2 discusses the product-to-process mappings for the product integrations that are described in this Green Book.

The remaining chapters in each volume describe how to integrate additional CA Technologies solutions with CA SDM. The integrations can help extend the capability of CA SDM and enhance the management and coordination of service management business processes. This Green Book uses a layered approach to technical integrations by starting with a point-to-point integration with CA SDM. This Green Book then includes instructions or recommendations for introducing one or more additional product solutions into the existing integration.

The following information is provided for each product integration:

- An overview that describes the benefits of the integration
- Recommended best practices for the integration
- Steps to set up, configure, test, and troubleshoot the integration
- Steps to introduce additional solutions into the environment, if applicable

The CA SDM integrations that are explained in this Green Book are divided into the following volumes:

- Volume 1

  CA Service Catalog

  CA Clarity™ Project and Portfolio Manager (CA Clarity PPM)

  CA Business Service Insight (CA BSI)

  CA Identity Manager

  CA SiteMinder®

- Volume 2

  CA Integration Platform

  CA Process Automation

- Volume 3

  CA Asset Portfolio Management

  CA IT Client Manager

  CA Patch Manager

  CA Cohesion Application Configuration Manager (CA Cohesion ACM)

  CA ecoMeter

  CA NSM

  CA Spectrum (includes CA eHealth and CA CEM)

All three volumes include the following chapters:

- Introduction
- ITIL V3 Service Lifecycle Support

Important! Some of the product features and functions listed in this Green Book are not described in CA Technologies product documentation and are not supported by CA Technical Support. Your site is responsible for testing and maintaining the integrations that are not described in the CA Technologies product documentation. We recommend that you test the integrations carefully in a nonproduction environment before going into production.

Who Should Read This Book

This Green Book provides the following types of users with the information necessary to integrate CA SDM with various CA Technologies solutions:

- Support technician
- Software architect

- Software developer
- Software engineer
- System administrator

This Green Book is intended for highly technical users who have an advanced knowledge of CA SDM and require integration capabilities to configure and maintain successfully their CA SDM environment.

Chapter 2: ITIL® V3 Service Lifecycle Support

CA Technologies integrated solutions support and align with the 24 processes and 4 functions in the Service Lifecycle of ITIL V3. This chapter lists the objectives for each process and the technologies that support them.

Service Strategy

Demand Management

Objectives

- Influence user and customer demand of IT services.
- Manage the impact on IT resources.
- Develop and maintain service packages and service level packages that are based on patterns of business activity.

How CA Technologies Solutions Help Meet the Objectives for Demand Management

The following process describes how CA eHealth, CA Clarity PPM, CA Service Catalog, and CA SDM integrate to help improve the Demand Management process:

1. CA eHealth provides a service provider with the metrics that can be used to model service demand. CA eHealth metrics can be tied to CA Service Catalog service offerings to enable reporting back to the customers on how their services are used. The reporting also identifies the costs that are associated with providing the service at the given demand.
2. When CA eHealth and CA Service Catalog are integrated with the CMDB component of CA SDM, the relationship of the services and their supporting infrastructure can be analyzed graphically with the CMDB Visualizer for actual and anticipated demand.
3. As improvements (or details of a new service) are defined, the Demand Manager documents the details in the service package of the portfolio within CA Clarity PPM.
4. As updates are approved, CA Clarity PPM creates requests for change (RFCs) in CA SDM to update the CA eHealth monitoring profiles and CA Service Catalog with changes to the service and its costs.

5. CA BSI integrates, at a service view, CA eHealth, CA Clarity PPM, CA Service Catalog, and CA SDM to enable a Demand Manager to review existing and anticipated patterns of business activity for the business.

Other CA Technologies Products that Facilitate the Demand Management Process

Demand Management is also facilitated in other CA Technologies solutions.

- CA ecoMeter automates delivering green service and reports on green IT effectiveness. The reports from CA ecoMeter help IT to convey the savings of having well-defined demand back to the business.
- CA SOI provides infrastructure that is based on demand. Specific service level packages are modeled in CA SOI that helps simplify the deployment of the infrastructure that is based on demand. A Demand Manager can use the metrics that CA SOI gathers to model future service packages.
- CA SDM provides statistics of incident and change requests to understand customer patterns of business activity better.

Financial Management

Objectives

- Quantify the value of IT services and their underlying assets by managing IT budgeting, accounting, and charging.

How CA Technologies Solutions Help Meet the Objectives for Financial Management

The following process describes how CA Asset Portfolio Management, CA Clarity PPM, CA Service Catalog, and CA SDM integrate to help improve the Financial Management process:

1. CA Clarity PPM helps a service provider manage the project and asset costs and evaluate how the services are budgeted and charged to the customer.
2. The integration of CA Clarity PPM with CA Service Catalog helps in managing finances efficiently. The accounting capabilities of CA Service Catalog provide the metrics that an IT Financial Manager uses to model which services are cost-effective and to identify how to gain efficiencies in those services.

3. CA Clarity PPM provides the accounting capabilities of CA Service Catalog with up-to-date costs and services that a customer can request.

4. Each individual asset that is requested through the catalog is tracked through CA SDM as either a request or, if needed, a change order.

5. CA Asset Portfolio Management provides the cost of the assets, contracts, and vendor information. When CA Asset Portfolio Management is integrated with CA Service Catalog, a user sees currently available assets. An asset can be a configuration item (CI), an asset associated with a user, or both a CI and a user asset. If an asset is also a CI, the asset is managed under the full Change Process.

6. CA Asset Portfolio Management integrates into the service provider Enterprise Resource Planning (ERP) solution, strengthening the IT alignment to business budgeting, accounting, and charging.

7. CA Asset Portfolio Management provides details to CA Clarity PPM to enable up-to-date IT financial management decisions for services.

Service Portfolio Management

Objectives

- Provide a dynamic method for governing investments in service management across the enterprise and managing them for value.

- Define, analyze, approve, and offer services.

How CA Technologies Solutions Help Meet the Objectives for Service Portfolio Management

The following process describes how CA Clarity PPM, CA Service Catalog, and CA SDM integrate to help improve the Service Portfolio Management process:

1. CA Technologies has an industry-leading Project and Portfolio Management solution, CA Clarity PPM. Native integration to other solutions such as CA SDM and CA Service Catalog provide three-direction feeds that provide current, planned, and historical data about how services are used.

2. When CA Clarity PPM receives request volumes from CA Service Catalog, CA Clarity PPM can track how often a service is currently being requested as compared with the long-term usage of the service.

3. Incident and problem ticket volumes from CA SDM, together with relationships in the CA SDM CMDB component, enable analysis of how effectively a service delivers on its commitments.

4. The Portfolio Manager uses CA Clarity PPM to analyze all aspects of providing the service to justify further investment.

5. In CA Clarity PPM, the approval process is modeled such that a workflow and decision tree to retain, replace, rationalize, refactor, renew, or retire a service can be documented, assessed, and ultimately approved.

6. Most importantly, the integration helps ensure continuous improvement to the service without the need to recompile data that is natively integrated.

7. CA BSI provides the Service Level Management understanding that supports the Service Portfolio and helps ensure that the Service Level Agreements (SLAs), Operational Level Agreements (OLAs), and Underpinning Contracts (UCs) are being managed properly.

Service Strategy

- Define the best possible value that a service can create for a customer through analysis of competition, market space, asset use, and business capabilities.

How CA Technologies Solutions Help Meet the Objectives for Service Strategy

The following process describes how CA Clarity PPM and CA SDM integrate to help improve the Service Strategy process:

1. CA Clarity PPM analyzes the key attributes with a number of scenarios such as comparisons over time, costing models, resource use, and others.

2. When CA Clarity PPM is integrated with CA SDM, detailed attributes of the CIs, organizations, resources, service use, and ties to other services are added to the analysis within the CMDB Visualizer.

3. With the solutions integrated, CA Clarity PPM and CA SDM provide the ability to analyze which combinations of investments provide the most benefit to the business.

Service Design

Availability Management

Objectives

- Produce and maintain an availability plan that reflects the current and future needs of the business.
- Provide advice and guidance on all availability-related issues.
- Help ensure that service availability achievements meet or exceed all their agreed targets by managing the performance of services and resource-related availability.
- Assist with the diagnosis and resolution of availability-related incidents and problems.
- Assess the impact of all changes on the availability plan and the performance and capacity of all services and resources.
- Help ensure that proactive measures to improve the availability of services are implemented, if the measures are cost-justifiable.

How CA Technologies Solutions Help Meet the Objectives for Availability Management

The following process describes how CA eHealth, CA CEM, CA NSM, CA Spectrum, and CA SDM integrate to help improve the Availability Management process:

1. CA CEM allows for real-time and historical views of the customer experience of the service, such as web page generation and data retrieval.
2. CA Introscope gathers back-end to front-end application performance metrics.
3. CA NSM provides agent level metrics on the operating system, database, and applications.
4. CA Spectrum provides the heuristic measurements of the network and system availability.
5. These four solutions provide details that are sent to CA eHealth for the baseline and real-time availability of the IT infrastructure.
6. The modeling of the infrastructure is maintained in the CMDB component of CA SDM. The CIs that the infrastructure solutions manage are imported into the CMDB component, which is associated to a Management Database Repository (MDR), and visualized at a service layer.

7. Incident metrics are automatically created from the tools and manually created from customers and are added to the analysis within CA SDM.

8. The availability plans are documented as knowledge documents in the knowledge management function of CA SDM. Knowledge management has a flexible document lifecycle, which helps ensure that updates to the availability plan are properly managed.

Other CA Technologies Products that Facilitate Availability Management

Other CA Technologies solutions also facilitate Availability Management. These solutions are added to the Availability Manager planning tools.

- CA BSI automates, activates, and accelerates the management, monitoring, and reporting of business and technology service level agreements (SLAs) and service delivery agreements for enterprises and service providers.

- CA SOI gives a model-based view of critical application monitoring data. CA SOI pulls all the data from domain management systems, such as CA Application Performance Management, CA Spectrum, and CA eHealth, and presents it in a single view to end users. CA SOI provides service impact analysis, service visualization, and integration to service management through CA SDM.

- CA Patch Manager lists computers that are not patched, which enables Availability Management to identify potential threats to availability.

  Note: CA Patch Manager uses the infrastructure and resources of the CA IT Client Manager solution.

Capacity Management

Objectives

- Produce and maintain an up-to-date capacity plan, which reflects the current and future business needs.

- Provide advice and guidance to all business and IT departments on all issues that are related to capacity and performance.

- Help ensure that service performance achievements meet or exceed all of their agreed performance targets.

- Assess the impact of all changes on the capacity plan, and the performance and capacity of all services and resources.

How CA Technologies Solutions Help Meet the Objectives for Capacity Management

Capacity Management relies on metrics from the infrastructure to plan, advise, and react to capacity needs. The metrics are used to analyze historical, current, and future availability through visualization, alerting, and reporting. CA Technologies solutions gather the metrics about a service provider infrastructure and add an integrated management layer to support mature Capacity Management.

1. CA CEM allows for real-time and historical views of the customer experience of the service, such as web page generation and data retrieval.
2. CA Introscope gathers back-end to front-end application performance metrics.
3. CA NSM provides agent-level metrics on the operating system, database, and applications.
4. CA Spectrum provides the heuristic measurements of the network and system availability.
5. These four solutions provide details that are fed to CA eHealth for baseline and real-time capacity of the IT infrastructure.
6. Final service modeling of the infrastructure is maintained in the CMDB component of CA SDM. The CIs that the infrastructure solutions manage are imported into the CA SDM CMDB component, which are associated to a Management Database Repository (MDR), and visualized at a service layer.
7. Incident metrics are automatically created from the tools or from customers and are added to the analysis within CA SDM.
8. The Capacity Plans are documented as knowledge documents in the knowledge management function of CA SDM. Knowledge management has a flexible document lifecycle to help ensure that updates to the plan are properly managed.

Other CA Technologies Products that Facilitate Capacity Management

Other CA Technologies solutions also facilitate Capacity Management. These solutions are added to the Capacity Manager planning tools.

- CA BSI automates, activates, and accelerates the management, monitoring, and reporting of business and technology SLAs in addition to service delivery agreements for enterprises and service providers.

- CA SOI gives a model-based view of critical application monitoring data. CA SOI pulls all the data from domain management systems, such as CA Application Performance Management, CA Spectrum, and CA eHealth, and presents it in a single view to end users. CA SOI provides service impact analysis, service visualization, and integration to service management through CA SDM.

- CA ITCM and CA Server Automation provide alerts and automated actions on desktops and servers that are running low on disk space.

Information Security Management

Objectives

- Help ensure availability, confidentiality, and integrity of data, systems, and the environments that contain them.

- Communicate, implement, and enforce the Information Security Policy.

How CA Technologies Solutions Help Meet the Objectives for Information Security Management

1. CA Technologies IT Security Solutions manage the full scope of Information Security Management as it relates to implementing, evaluating, maintaining, and controlling access, identities, and information.

2. The Service Management solutions leverage and integrate with CA Technologies IT Security Solution enabling a service provider to plan and design an Information Security Policy.

3. CA SDM tracks security incidents, assets and locations, SLAs, UCs, and OLAs that are used to plan the security policy.

4. The CA SDM knowledge management feature is where Information Security is published as a knowledge document and maintained with an enforced review cycle.

5. The service management solution supports implementation, evaluation, maintenance, and control through its technology stack. For example, CA EEM, a component within the IT Security Solutions, is a core component of the Service Management solution enabling service providers a central repository of service management application users. This solution is integrated using LDAP and provides access to features and data within the Service Management suite. This integration supports password reset through the CA SDM end-user self-service interface.

6. CA ITCM, CA Server Automation, and CA Cohesion ACM feed the infrastructure resources contained in the CMDB component of CA SDM. CA ITCM and CA Server Automation identify changes to desktops and servers that can introduce security threats, such as unauthorized USB drives, inappropriate software installs, or changes to browser settings.

7. CA Cohesion ACM baseline comparison lists changes to CIs that affect the availability of service. Moreover, CA Patch Manager (which feeds CA ITCM and CA Server Automation) lists all desktops and servers that are not at the proper patch level. CA SDM integrates with CA Identity Manager to enable pass-through authentication in the most complex security architecture.

IT Service Continuity Management

Objectives

- Maintain a set of IT Service Continuity plans and IT Recovery plans that support the overall organizational business continuity plans.

- Complete regular business impact analysis exercises to help ensure that all continuity plans are maintained in line with changing business impacts and requirements.

- Assess the impact of all changes on the IT Service Continuity plans and IT Recovery plans.

- Negotiate and agree to the necessary supplier contracts for the provision of the recovery capability that supports the continuity plans with Supplier Management.

How CA Technologies Solutions Help Meet the Objectives for IT Service Continuity Management

Helping ensure an effective IT Service Continuity Management (ITSCM) process requires a documented and executed continuity plan. CA Technologies integrated solutions leverage all of the solutions documented in this Green Book to provide inputs to defining the continuity plan. This plan is ultimately published in CA SDM and managed as an ongoing project with the business in CA Clarity PPM.

1. The integration of CA SDM with CA Process Automation can be used to automate recovery plans by notifying key personnel, initiating failover systems, and initiating monitoring of new facilities.

2. Functionally, CA Clarity PPM opens Change Orders in CA SDM to schedule recovery testing, which initiates the CA Process Automation process flow to begin a recovery process.

3. Leveraging the solutions in Capacity and Availability Management, a service provider can identify whether the service levels are being met. The service provider can then feed them back to CA SDM and ultimately back into the ITSCM design improvements.

Service Catalog Management

Objectives

- Provide a single source of consistent information about all the agreed services.

- Help ensure wide availability to users who have access.

How CA Technologies Solutions Help Meet the Objectives for Service Catalog Management

The following process describes how CA SDM, CA Service Catalog, CA Clarity PPM, and CA Asset Portfolio Management integrate to help improve the Service Catalog Management process:

1. CA Service Catalog is a solution that supports all objectives of the Service Catalog Management process in Service Design.

2. CA SDM and CA Service Catalog share a repository of users, locations, organizations, tenants, and CA EEM (for security).

3. RFCs that are created in CA SDM can be linked to CA Service Catalog requests. The assets in the CA SDM CMDB are managed in CA Asset Portfolio Management.

4. When fulfilling a request, a link directly into CA Asset Portfolio Management data is used to assign only available assets to the request. This link helps ensure immediate CA SDM CMDB updates on the asset or CI status for the request throughout its progress into a production state.

5. CA Clarity PPM (which contains the master portfolio) helps ensure that CA Service Catalog is given the proper offerings and deactivates any inactive service offerings too.

Service Level Management

Objectives

- Define, document, agree on, monitor, measure, report, and review the level of IT services provided.
- Help ensure the specific and measurable targets are developed for all IT services.
- Monitor and improve customer satisfaction with the quality of service delivered.
- Verify that IT and the customers have a clear and unambiguous expectation of the level of service that is delivered.

How CA Technologies Solutions Help Meet the Objectives for Service Level Management

The following process describes how CA Clarity PPM, CA eHealth, CA BSI, and CA SDM integrate to help improve the Service Level Management process:

1. The defined and agreed levels of SLAs are developed in CA Clarity PPM and then documented and tracked in CA BSI.

2. The Service Level Manager publishes the details of the SLAs that are maintained in CA BSI or CA Clarity PPM as a CA SDM knowledge document. This document supports communication to the business about the expected levels of service.

3. CA BSI and CA eHealth enforce, alert, and report on the defined levels of service.

4. When there are agreed changes to the SLA, CA Clarity PPM initiates an RFC in CA SDM against the services. The RFC initiates a workflow in CA Process Automation to deploy the updated service levels to CA eHealth and CA BSI for monitoring.

Supplier Management

Objective

- Help ensure the best value of service is obtained from suppliers and contracts.
- Help ensure the underpinning contracts are aligned to business needs and SLAs.
- Manage supplier relationships and performance.
- Maintain a supplier and contracts database.

How CA Technologies Solutions Help Meet the Objectives for Supplier Management

The following process describes how CA BSI, CA Clarity PPM, CA eHealth, CA Asset Portfolio Management, CA ITCM, CA Server Automation, and CA SDM integrate to help improve the Supplier Management process:

1. A service provider uses CA Asset Portfolio Management as the supplier and contracts database (SCD) enabling centralized management of underpinning contracts. The database includes a list of the providers, their products and services, and the value they bring to the business.
2. When integrated with CA ITCM, CA Server Automation, and CA SDM, CA Asset Portfolio Management is able to identify quantitatively the hardware, software, and system performance of the services that the suppliers provide. CA ITCM and CA Server Automation provide up-to-date inventory in a service provider environment.
3. The CA ITCM and CA Server Automation inventory is provided to CA Asset Portfolio Management and linked to the relevant contracts.
4. The CA SDM CMDB component and CA Asset Portfolio Management share the physical asset and CI records that are linked back to the Supplier in CA Asset Portfolio Management. Service contracts in CA BSI enforce service levels against the CIs that are associated to the suppliers through automated escalation and reporting.
5. The CA SDM CMDB component contains the relationships of the services to the CIs and assets that link to CA Asset Portfolio Management. Leveraging the integration of the CMDB component with CA eHealth provides the visibility to the overall health and performance of the services that a supplier provides.
6. CA Asset Portfolio Management and CA SDM ad-hoc reporting enables visibility into the number of incidents that are opened against supplier services. This visibility can be used to help manage supplier relationships and prove their performance.

7. CA Asset Portfolio Management and CA SDM are integrated with CA Clarity PPM, which provides the detailed costs that are associated to the service portfolio. This integration is then used to validate and analyze the value that a supplier provides to the service provider and business.

8. CA BSI consolidates the details from the other technologies to provide insight into how well suppliers are meeting SLAs.

Service Transition

Change Management

Objectives

- Help ensure that standardized methods and procedures are used for efficient and prompt handling of all changes.

- Record all changes to service assets and configuration items in the Configuration Management System and optimize the overall business risk.

How CA Technologies Solutions Help Meet the Objectives for Change Management

The following process describes how CA Cohesion ACM, CA SOI, CA ITCM, CA Server Automation, and CA SDM integrate to help improve the Change Management process:

1. RFCs are recorded, reviewed, assessed, and prioritized in CA SDM.

2. The approval process of the RFC is enforced using CA Process Automation for normal or emergency changes.

3. For standard changes, CA Process Automation automates the end-to-end approval and deployment, through CA ITCM and CA Server Automation or CA SOI, of the requested change using the inventory in the CMDB component of CA SDM.

4. When CA ITCM and CA Server Automation are integrated with CA SDM, RFCs of unauthorized changes are automatically logged as incidents or RFCs for further review.

5. The complex relationships of CIs and the recipients of their services are tracked in CA Cohesion ACM. CA Cohesion ACM baselines help ensure that there are no changes to the complex interconnections of the infrastructure that supplies the service.

6. CA Cohesion ACM is integrated into CA SDM through inventory importing, which helps ensure that the CA SDM CMDB is up-to-date with the latest relationships between CIs.

Evaluation

Objectives

- Evaluate the impact a new or changed service has on the customer perception of capacity, resource, and performance.
- Enable change management to be more effective in the decision about service changes.

How CA Technologies Solutions Help Meet the Objectives for Evaluation

The following process describes how CA eHealth, CA CEM, and CA SDM integrate to help improve the evaluation process:

1. Integrating CA eHealth and CA CEM with the CA SDM CMDB and change management functions enables a service provider to compare previous and new performance metrics.
2. CA SDM surveys gather feedback from customers on the effectiveness of a new release.
3. CA CEM enables measurements from the customer perspective of the service.
4. Using the CMDB Visualizer, together with real-time statistics from CA CEM and performance trends of CA eHealth, a service provider can determine which portions of a change reduced the resource performance. This end-to-end visualization (enabled by CA Technologies integrated solutions) facilitates effective management decisions.

Knowledge Management

Objectives

- Enable the service provider to be more efficient and improve quality of service, reduce the cost of service, and increase customer satisfaction.
- Help ensure that the service provider staff has a clear and common understanding of the following areas:
  - Value that the services provide to customers.
  - Benefits that are realized from the use of those services.

- Help ensure that at a given time and location, the service provider staff has adequate information about the following areas:
  - Who uses the services
  - Current states of consumption
  - Service delivery constraints
  - Difficulties that the customer faces.

How CA Technologies Solutions Help Meet the Objectives for Knowledge Management

The following process describes how CA SDM helps improve the Knowledge Management process:

1. CA SDM Knowledge Management centralizes the administration and management of knowledge for service providers.
2. The integrations to other systems that can automate steps for the customer, such as CA ITCM and CA Server Automation scripts or CA SDM Support Automation Automated Tasks scripts, can be called from Action Content in the knowledge document.

Release and Deployment Management

Objectives

- Provide clear and comprehensive release and deployment plans to align with customer and business change project activities.
- Build, install, test, and deploy release packages efficiently and on schedule.
- Minimize unpredicted impact on the production services, operations, and support organization.
- Improve the satisfaction of customers, users, and service management staff with the service transition practices and outputs.

How CA Technologies Solutions Help Meet the Objectives for Release and Deployment Management

The following process describes how CA Service Catalog, CA Clarity PPM, CA SCM, CA ITCM, CA Server Automation, and CA SDM integrate to help improve the Release and Deployment Management process:

1. The Release and Deployment Management process is the culmination of the work from the strategy, design, and remaining transition processes.
2. The service portfolio in CA Clarity PPM initiates an RFC in CA SDM, where the requested change is classified, reviewed, and approved through a Change Management process.
3. CA Process Automation automates the process and creates the release package in CA SCM. The documents that are related to the release package are centrally controlled in CA SCM through approvals and a check-in and check-out process. Ultimately, the documents are promoted through the test to production. Throughout the process, status updates are provided to the project and the RFC.
4. CA SCM leverages its integration with CA ITCM and CA Server Automation to initiate the deployment of the release package. This action ensures a consistent deployment, which results in a reduced impact to the service at the production roll-out.
5. When the release package is ready to be part of CA Service Catalog, CA SCM notifies the CA Clarity PPM project and portfolio that the service is ready to be promoted into CA Service Catalog.
6. When the RFC is closed, satisfaction surveys are sent to customers. Any incidents that are related to the release can be tied back to the RFC for future analysis and the change impact.

Service Asset and Configuration Management

Objectives

- Identify, control, record, report, audit, and verify service assets and configuration items, including their versions, baselines, constituent components, attributes, and relationships.
- Account for, manage, and protect the integrity of service assets and configuration items throughout the service lifecycle by ensuring that only authorized components are used and only authorized changes are made.
- Help ensure the integrity of the assets and configurations that are required to control the services and IT infrastructure by establishing and maintaining an accurate and complete Configuration Management System.

How CA Technologies Solutions Help Meet the Objectives for Service Asset and Configuration Management

The following process describes how CA Service Catalog, CA Cohesion ACM, CA Asset Portfolio Management, CA ITCM, CA Server Automation, and CA SDM integrate to help improve the Service Asset and Configuration Management process:

1. From the procurement of a new asset to the final support of a service, CA Technologies solutions support the ability of the service provider to perform Service Asset and Configuration Management. The process helps ensure control through a centralized CMDB component.

2. An asset is procured and logged in CA Asset Portfolio Management with the associated contracts, licensing, and classifying attributes that enable it to be tracked throughout its life cycle.

3. When a CA Service Catalog request is initiated, the service provider leverages the CA Asset Portfolio Management and CA Service Catalog integration to retrieve a list of available assets to assign to the request. Unique attributes, such as software to be installed, are also identified.

4. The CA Service Catalog request creates an RFC in CA SDM.

5. CA SDM and CA Asset Portfolio Management share the repository of assets and CIs. When an RFC is initiated from a CA Service Catalog request, it already has the approved linked assets, along with the desired software configuration.

6. The automation and integrated solutions help ensure that the status of the identified asset is updated and auditable by the service provider. The automation and integration also help ensure the continuity of the Release and Deployment Management process.

7. When an asset (for example, a server being provisioned for a particular service) is put onto the network, CA ITCM and CA Server Automation discover the device. CA ITCM and CA Server Automation deploy their agents to begin immediate management of the device and start the deployment of required software.

8. To add to the control of the server, CA Cohesion ACM identifies which part of the service the server is providing (for example, a database server in a cluster). CA Cohesion ACM identifies the relationship, which is then sent back to the CA SDM CMDB component. Change Manager validates the relationship on the RFC.

9. Baselines of the server are contained in CA ITCM, CA Server Automation, and CA Cohesion ACM, allowing a service provider to identify any unauthorized changes to the device.

10. Any updates of software or configuration are provided to CA Asset Portfolio Management by CA ITCM and CA Server Automation or through updates of the CA SDM CMDB through CA Cohesion ACM.

11. As the server depreciates in its ability to provide value to the service, an RFC is created in CA SDM to retire the device. Leveraging historical data from CA SDM (such as incidents, RFCs, performance statistics, and memory upgrades), the service provider can show a full audit trail for the CI over time.

Service Validation and Testing

Objectives

- Validate that a service is "fit for use" or Warranty.
- Validate that a service is "fit for purpose" or Utility.
- Provide confidence that a new or changed service delivers value to the customer.
- Confirm that the requirements for a service are correctly defined and remedy any errors or variances early in the service lifecycle.

How CA Technologies Solutions Help Meet the Objectives for Service Validation and Testing

The following process describes how CA SCM, CA eHealth, CA SOI, and CA SDM integrate to help improve the Service Validation and Testing process:

1. Integrating CA Clarity PPM, CA SDM, and CA SCM enables a service provider to manage the documentation that is required to ensure a new or changed service is fit for use and fit for purpose.

2. CA Clarity PPM contains the quantitative attributes of what is required for the portfolio.

3. CA SCM contains the documents that capture the requirements of the service as well as the testing strategy.

4. The CA SDM CMDB Visualizer enables modeling of the test environment for impact analysis.

   Note: The service model is an abstraction that shows logical elements and their relationships. The service definition is the description of an implemented instance of a service that has been modeled. A service map is a selective view of a service showing desired elements and relationships from an explicit perspective. Different perspectives on a given service generate different maps.

5. CA eHealth measures the availability and capacity of the service.

6. CA SOI automates the deployment of the test environment and testing scripts. These integrated solutions share CI information, test plans, test package promotion and state, and the CA Business Intelligence centralized reporting solution.

Transition Planning and Support

Objectives

- Plan appropriate capacity and resource to package a release and to build, release, test, deploy, and establish a new or changed service into production.

- Provide support for the service transition teams and people.

- Help ensure that service transition issues, risks, and deviations are reported to the appropriate stakeholders and decision makers.

- Coordinate activities across projects, suppliers, and service teams when required.

How CA Technologies Solutions Help Meet the Objectives for Transition Planning and Support

The following process describes how CA Clarity PPM, CA SCM, and CA SDM integrate to help improve the Transition Planning and Support process:

1. CA Technologies integrated solutions enable effective transition planning and facilitate support of new or changed services. For transition planning, resources are scheduled in CA Clarity PPM against a project.

2. In CA SDM, individual work tasks are created as RFCs, incidents, or requests from the CA Clarity PPM project workflow, depending on the work needed.

3. As work for developers and product teams begins, CA SDM initiates packages inside CA SCM. CA SCM helps ensure that activity is properly coordinated, approved, and promoted through a defined lifecycle.

4. In CA SDM, incidents are tracked against the projects providing visibility to management on the success of the transition as well as identifying areas that may require additional support.

Service Operation

Access Management

Objectives

- Provide the access permission for users to access services based on policies and actions defined in security and availability management.

How CA Technologies Solutions Help Meet the Objectives for Access Management

The following process describes how CA SiteMinder, CA Identity Manager, CA Service Catalog, and CA SDM integrate to help improve the Access Management process:

1. From CA Service Catalog, an authorized user can request to change or add security rights as well as initiate approvals that are based on CA Process Automation workflows.

2. After a request is created, CA SDM generates an RFC so that the user profile can be updated in the CA SDM CMDB.

3. CA SDM then initiates a workflow in CA Identity Manager, where security administrators review and implement the security access.

4. CA SiteMinder, integrated with CA Identity Manager, helps ensure that only authorized systems are made available to the user.

Event Management

Objectives

- Detect events, comprehend, and determine the appropriate control action; communicate operational information as well as warnings and exceptions.

- Automate routine operations management activities.

- Provide a way of comparing actual performance and behavior against design standards and Service Level Agreements.

How CA Technologies Solutions Help Meet the Objectives for Event Management

The following process describes how CA NSM, CA Spectrum, CA eHealth, CA CEM, CA Introscope, and CA SDM integrate to help improve the Event Management process:

1. Event Management begins with determining the level of the service that a service provider intends to monitor.
2. CA CEM monitors the service from the customer perspective. For any breach of service level, CA CEM creates an incident in CA SDM.
3. As a service provider delves deeper into monitoring the application communications to back-end systems, CA Introscope generates incidents in CA SDM.
4. For events that occur inside the applications, CA NSM agent technology generates SNMP traps. These traps can be used against a robust correlation engine, which can determine whether an incident must be opened.
5. If there is an event in the environment that results in a cascading failure to multiple users or service, CA Spectrum automatically creates a single incident in CA SDM instead of multiple individual incidents for each affected resource. This single incident helps the Service Desk to manage more effectively the queue and to stay focused on the user perception of service. Incidents are logged for each user and linked to the parent incident.
6. Systems-level SLAs are monitored by CA eHealth. CA eHealth opens incidents based on general service degradation or potential service degradation. Application management and IT operations management functions use this set of integrated solutions to manage their responsibilities. Application managers use the metrics from these solutions to design better services for the customer. For IT Operations Managers, these tools offer the low-level metrics with alerting and automation to ensure day-to-day stability.

Incident Management

Objectives

- Restore normal service operation as quickly as possible and minimize the adverse impact on business operations.
- Help ensure that the best possible service quality and availability are maintained.

How CA Technologies Solutions Meet the Objectives for Incident Management

The following process describes how CA SDM, CA eHealth, CA Spectrum, CA ITCM, and CA Server Automation integrate to help improve the Incident Management process.

1. CA SDM provides the front end to incident, problem, request, and change tickets as well as the Knowledge Documents. The CMDB function of CA SDM integrates into all aspects of IT operations to help ensure that CA SDM can gather facts to restore service quickly to the customer.

2. CA eHealth and CA SOI proactively generate Incidents as a result of potential service degradation.

3. Incidents can be analyzed against impact analysis using the CMDB Visualizer to plan availability and capacity better.

4. CA ITCM and CA Server Automation can generate incidents in CA SDM based on policy violations that result in degradation of client/server ability to provide service.

5. CA Spectrum auto-generates incidents when there is a disruption of service.

6. The CA SDM web services application programming interface (API), email API, and native integration with various CA Technologies solutions enable bidirectional communication that is based on activities that are performed on the ticket. This communication helps ensure the most effective route to restoration of service to the end user.

Problem Management

Objectives

- Prevent problems and resulting incidents from happening.

- Eliminate recurring incidents and minimize the impact of incidents that cannot be prevented.

How CA Technologies Solutions Help Meet the Objectives for Problem Management

The following process describes how CA Spectrum, CA NSM, CA ITCM, CA Server Automation, CA Cohesion ACM, and CA SDM integrate to help improve the Problem Management process:

1. CA SDM provides a robust Problem Management solution that enables a service provider to manage a problem throughout its lifecycle, from Incident creation and known error recording to initiation of an RFC.

2. By leveraging the native integration of CA Spectrum, CA NSM and other Infrastructure Management solutions, Problem Management can become proactive.

3. CA Spectrum and CA NSM monitor the infrastructure for the signs of service degradation that automatically opens problem tickets.

4. CA ITCM and CA Server Automation, when integrated with the CA SDM CMDB, proactively create hardware and software based Incidents. The Problem Manager can leverage the Incidents to perform Root Cause Analysis (RCA) of the problem.

5. CA Cohesion ACM integrates with CA SDM to enable a Problem Manager to identify deviations of a CI-based configuration change that could be the root cause of the problem.

Request Fulfillment

Objectives

- Provide a channel for users to request and receive standard services that have a predefined approval and qualification process.

- Provide information to users and customers about available services and procedures for obtaining them.

- Source and deliver the components of requested services.

- Assist with general information, complaints, or comments.

How CA Technologies Solutions Help Meet the Objectives for Request Fulfillment

The following process describes how CA Service Catalog, CA Asset Portfolio Management, and CA SDM integrate to help improve the Request Fulfillment process:

1. CA Service Catalog provides a list, description, and workflow of services to enable request fulfillment.

   CA Service Catalog provides the list of offerings that the user can access, the pricing, and the expected levels of service for the offering.

2. CA Service Catalog natively integrates with CA Asset Portfolio Management. CA Asset Portfolio Management maintains a list and status of available resources that can fulfill the request. When Service Asset Managers fulfill the order, they link the identified resource to the request and they create an RFC in CA SDM for deployment.

3. The CA SDM end-user self-service interface helps ensure that customers have access to the following information:

   - Knowledge documents
   - Hours of service
   - Requests for general information (single-click access)
   - Complaints or comments
   - View into CA Service Catalog offerings

Continual Service Improvement

Seven-Step Improvement Process

CA Technologies integrated solutions collaboratively enable the Seven-Step Improvement Process. Each solution provides metrics, measures, and process enablers that facilitate the following process:

1. Defining what must be measured: CA Clarity PPM is the central tool to collect these requirements, which are then validated through CA BSI.

2. Defining what you can measure: CA eHealth, CA Wily, and CA NSM help ensure that you can measure all technology attributes to improve your services. CA Clarity PPM, CA BSI, and CA SDM enable you to measure process level metrics.

3. Gathering the data: CA eHealth, CA Wily, and CA NSM enable the collection of the data that your organization identifies for technology and service level metrics. CA Clarity PPM and CA SDM collaboratively provide process metrics.

4. Processing the data: CA Technologies uses CA BSI and CA Business Intelligence reporting to provide a central view of the collected metrics.

5. Analyzing the data: CA Business Intelligence and CA BSI enable robust analysis of the gathered metrics.

6. Presenting and using the data: At this stage of the Seven-Step Improvement Process, you can take your CA Business Intelligence and CA BSI reports to your Service Manager, Continual Service Improvement Manager, and Process owners to review the data that was collected.

7. Implementing corrective actions: Finally, you can update the status of your portfolio in CA Clarity PPM. CA Clarity PPM creates an RFC in CA SDM and the cycle of improvement begins again. You have continuous visibility of business objectives that are tied to critical success factors and the underlying key performance indicators (KPIs) and metrics, all from the integrated suite of solutions CA Technologies provides.

Chapter 3: CA Service Catalog

CA Service Catalog Integration

This chapter discusses how CA SDM Release 12.6 and CA Service Catalog Release 12.6 can be configured to work together. The following key topics are covered:

- Integration points and value among CA Service Catalog, CA SDM, CA Process Automation, and the CMDB component of CA SDM
- How to associate implementation logic and service design
- Integration instructions and example
- Common multi-tenancy
- Extending the integration to include CA Asset Portfolio Management

Overview of CA Service Catalog

CA Service Catalog is a product that presents a portfolio of service offerings to end users. The portfolio is published on behalf of a business unit or enterprise. Offerings describe IT services, including a rate charging structure that is defined by one or more rate plans. CA Service Catalog also allows an organization to model its business units and manage the user accounts contained within those units. The offerings in CA Service Catalog can be organized into a hierarchical structure through folders and can contain detailed information about the price of a service. CA Service Catalog offerings can include one or more metrics and are monitored for compliance with service level agreements.

Integration Points

CA Service Catalog and CA SDM integrate out of the box using CA Workflow or CA Process Automation through the respective web services. This chapter concentrates on the use of the CA Process Automation integration method. For more information about implementing CA Workflow, see the *CA Service Catalog Integration Guide* and the *CA Service Desk Manager Implementation Guide*.

CA Process Automation process definitions are included with CA Service Catalog to provide sample process flows that enable the communication between CA Service Catalog and CA SDM. This communication allows the integration to accommodate a full service lifecycle, taking user requests from submission, through approvals, to generation of CA SDM tickets, with complete fulfillment processes.

Starting with r12.5, CA Service Catalog and CA SDM began sharing a common multi-tenancy model. When configured, this model allows the two products to share a tenancy structure that reduces administrative overhead that is related to tenant maintenance.

Integration Points from CA Service Catalog

The following integration points are available from CA Service Catalog:

- Catalog Request Fulfillment, which can open change orders in CA SDM.
- CA Process Automation predefined workflow processes, which can create, read, and update CA SDM change orders.
- Request and Services user interfaces in CA Service Catalog, which can launch the CMDB Visualizer to find the connections between IT and business.

Integration Points from CA SDM

The following integration points are available from CA SDM:

- CA SDM calls the CA Service Catalog web services to update the original request with the details for the associated CA SDM change order. In the Related Tickets column of the CA Service Catalog request, the CA SDM change order number and link to the change order are populated.
- CA SDM handles Common multi-tenant administration after the common multi-tenancy is enabled.

Integration Points from CA SDM CMDB Component

The following integration points are available using the CMDB component of CA SDM:

- CA Service Catalog services are associated with CIs in the CMDB component of CA SDM. The association can be one-to-one, one-to-many, or many-to-many.
- Reports can be generated on CI associations to services.
- Using the CMDB Visualizer, you can trace the dependencies of the services on other CIs. These dependencies help determine the impact of CIs on services.

Integration Value

The CA Service Catalog integration provides the following value:

- CA Service Catalog can be used to present a total portfolio of service offerings in a single UI, while routing resulting transactions to appropriate back-end products and groups. For the IT help desk, the integration helps ensure that only requests that require service desk analyst involvement are routed to CA SDM. In this way, the integration helps reduce the service desk staff workload and allows service desk analysts to increase productivity and improve customer service.
- CA Service Catalog requests can go through a workflow process in which a subprocess can be invoked to open a CA SDM change order. The change order can also initiate a separate process that is tied to the CA SDM change order that was opened. This process does not interfere with the higher-level process that the CA Service Catalog request is following. The benefit is that the integration can allow for the streamlining of complementary processes.
- Integrating CA SDM with CA Service Catalog completes the Service Delivery Model. When a customer needs to understand costs, financials, and Service Level Management through Service Contracts, then CA SDM and CA Service Catalog requests that are related (regardless of which request initiated the other) can leverage all the financial management components of CA Service Catalog.

Example of the CA Service Catalog Integration

Business Challenge

Paul Kim, IT Director at Forward, Inc. has detected that the service areas in the organization have multiple entry points. Multiple service providers (such as HR, finance, procurement, accounting, and the service desk) use a mix of automatic and manual processes. This situation causes confusion for the end users, errors, and an inability to execute tasks in a timely manner and reduces the quality of service delivery. In addition, Paul has found that multiple requirements and questions that are directed to the service desk are not appropriate for the service desk. These questions reduce the productivity of the service desk staff. Paul needs to find out how to offer a unique front end to all Forward, Inc. users. This front end allows the users to make requests, regardless of which department is the main provider. The front end also helps ensure that the request is sent to the correct department for fulfillment.

CA Approach

Typically, users have separate products and processes that they use to submit requests for IT-related services. To complicate the situation, users may have to know the appropriate product and process that they must use for the specific request that they are submitting. The product that is used to make the request may not be intuitive or user-friendly. When a user requests IT services or goods, they should not have to know detailed and technical specifications for the goods or service. Delivery of the IT services must be performed in a consistent manner so that contracted service levels are met. CA Technologies advises Forward, Inc. to implement CA Service Catalog and to integrate it with the most business critical service applications, such as CA SDM, Procurement, and HR.

Solution Prerequisites

The following list includes the prerequisites for the integration of CA Service Catalog and CA SDM. The following products must be installed with the configurations as outlined:

CA EEM 8.4 SP4

- CA Service Catalog, CA SDM, and CA Process Automation are configured to use the same CA EEM instance.
- CA EEM has sample users that are defined to be leveraged by the workflow.

  Sample users have email addresses defined. Permissions for CA Process Automation (Application Group ITPAMUsers, ITPAMAdmins on an upgraded instance of CA Process Automation 3.1, and PAMUsers and PAMAdmins on a fresh install of CA Process Automation 3.1) have been assigned to those sample users who access the task list.

CA Service Catalog 12.6, 12.7

- Includes best practices content.

CA SDM 12.6

- CA Service Catalog and CA SDM are configured to use the same MDB.
- CA SDM is configured for email notifications.
- Sample users have email addresses defined.
- CA SDM has sample users that are defined as contacts to be leveraged by the workflow.
- Single sign-on is configured (optional) between CA Service Catalog and CA SDM.

CA Process Automation 3.1

- CA Process Automation 3.1 SP01 (minimum) is installed.
- The alert module is configured for email.
- CA Process Automation is integrated with CA SDM using the integration steps documented in the CA Process Automation chapter of the *CA Service Desk Manager Integration Best Practices Green Book*, Volume 2. These products must be already integrated if you want to do full service lifecycle integration (Complex Fulfillment) with CA Service Catalog, CA Process Automation, and CA SDM. From a high level, the following activities are assumed to be complete:
  - CA Service Desk Connector is installed in CA Process Automation.
  - The CA SDM module in CA Process Automation is configured.
  - The CA SDM Options Manager Options are installed for CA Process Automation Workflow.

Unicenter Asset Portfolio Management 11.3.4/CA Asset Portfolio Management 12.6

- Optional integration with CA Service Catalog, as documented in the *CA Service Catalog Integration Guide,* Release 12.6.
- CA Asset Portfolio Management is configured to use the same CA EEM instance as CA Service Catalog and CA SDM.
- CA Asset Portfolio Management is configured to use the same MDB instance as CA Service Catalog and CA SDM.
- Sample users are assigned to the CA Asset Portfolio Management Fulfiller role to allow access to the gold brick icon, which is discussed later in this chapter.
- Create sample hardware CIs to be leveraged by the workflow.

Important Environment Information

This chapter has information that is taken from an environment that has been upgraded from previous versions of CA EEM, CA Service Catalog, CA SDM, and CA Process Automation. If your environment has a fresh install of any of these applications, you may see some slight variations on file names, directory names, and other names.

This chapter includes information about both CA Service Catalog 12.6 and 12.7. Most of the chapter covers both releases. The user interface examples in this chapter reflect both versions.

How to Integrate CA SDM with CA Service Catalog

CA Service Catalog integrates with CA SDM through catalog request fulfillment, which can be configured to open CA SDM change orders automatically. The CA SDM change order can be viewed in the Related Tickets column of the CA Service Catalog request.

Using the integration with CA SDM, the following scenario could occur. A user requests a service from the catalog, such as a standard desktop computer, and it is approved. The fulfillment process, leveraging the CA Process Automation Workflow engine, identifies the correct existing asset. In addition, a CA SDM change order is opened and assigns a configuration and delivery task to a technician for the asset.

Review and complete the integration steps documented in the *CA Service Catalog Integration Guide*. The high-level integration steps include:

1. Validate that prerequisites are met.
2. Understand the key terms.
3. Configure communication between CA Service Catalog and CA SDM by ensuring that a CA SDM primary server is properly defined to CA Service Catalog. Additional notes for this step are listed in Web Services Policy (see page 47).
4. Optionally configure single sign-on between CA Service Catalog and CA SDM.
5. Configure CA Service Catalog to open CA SDM change orders through CA Process Automation for request fulfillment by enabling the CA Service Catalog rule actions. These steps are defined in the *CA Service Catalog Integration Guide.* See Enable Rule Actions in CA Service Catalog (see page 51) for more information.

Create a Web Services Policy

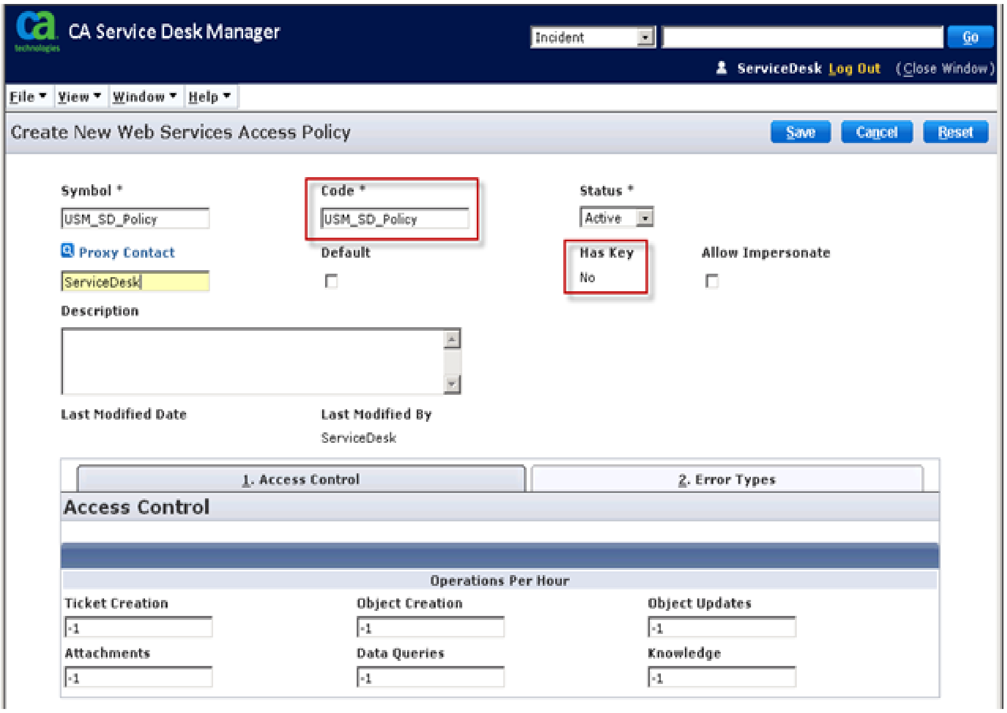
The first step in the process of configuring communication between CA Service Catalog and CA SDM is to create a web services policy in CA SDM. Instructions for creating web services policies are defined in the *CA Service Desk Manager Implementation Guide*.

Follow these steps:

1. Log in to CA SDM as an Administrator.
2. Navigate to Administration, Web Services Policy, Policies, Create New.

3. Create the policy with the attributes that are identified in the following graphic.

   Note: Initially, the web services policy has no key.



Create New Web Services Access Policy

Symbol *	Code *	Status *	
USM_SD_Policy	USM_SD_Policy	Active	
Proxy Contact	Default	Has Key	Allow Impersonate
ServiceDesk	□	No	□

Description

Last Modified Date	Last Modified By
	ServiceDesk

Access Control

Operations Per Hour

Ticket Creation	Object Creation	Object Updates
-1	-1	-1
Attachments	Data Queries	Knowledge
-1	-1	-1

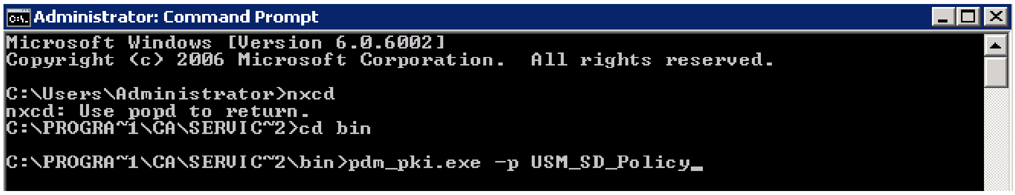
After you create the policy, generate the key for the policy.

4. Open a Windows command prompt and navigate to the $NX_ROOT\bin directory. This directory contains $NX_ROOT as the root directory where CA SDM is installed. A shortcut to get to $NX_ROOT is to type nxcd.

5. Execute the following command:

```
pdm_pki -p USM_SD_Policy
```

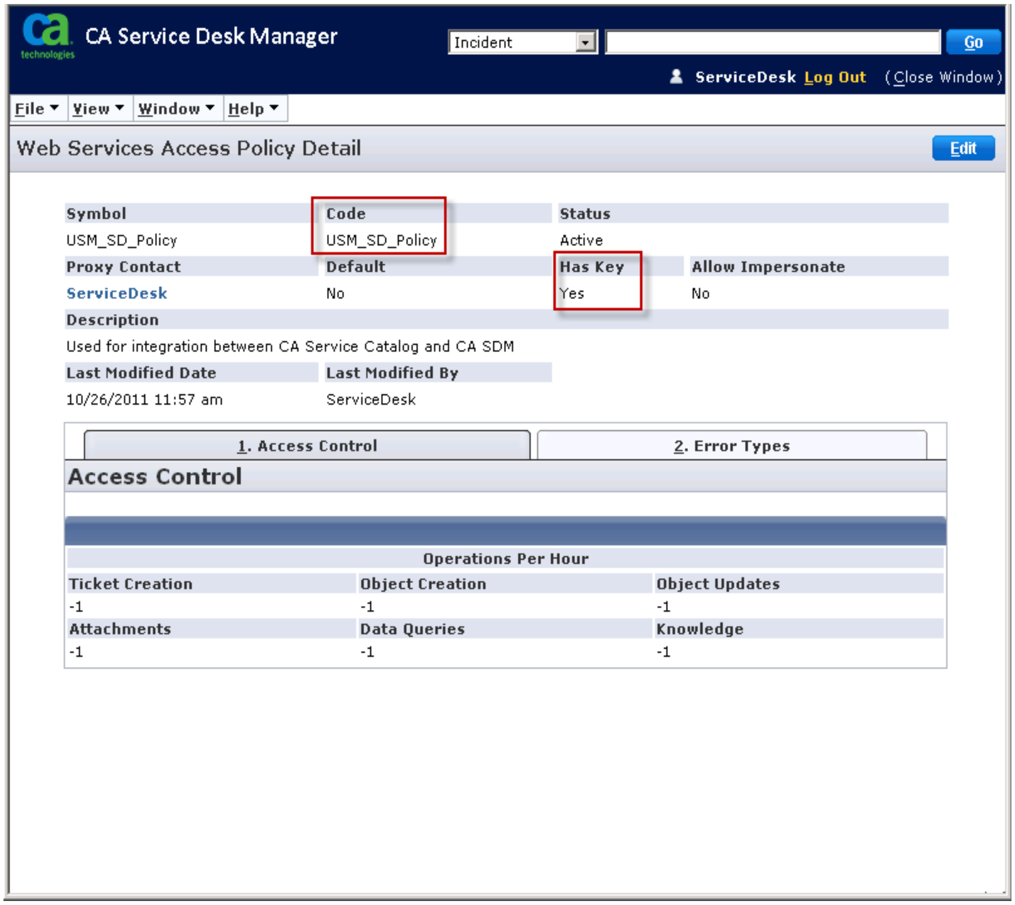
   This action creates a policy file named USM_SD_Policy.p12.



```
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>nxcd
nxcd: Use popd to return.
C:\PROGRA~1\CA\SERVIC~2>cd bin

C:\PROGRA~1\CA\SERVIC~2\bin>pdm_pki.exe -p USM_SD_Policy_
```

6. Copy the policy file named USM_SD_Policy.p12 to the directory %USM_HOME%, where %USM_HOME% is the root directory where CA Service Catalog is installed.

If you navigate back to CA SDM and view details for the policy, you see that the policy now has a key.



Web Services Access Policy Detail

Symbol	Code	Status	
USM_SD_Policy	USM_SD_Policy	Active	
Proxy Contact	**Default**	**Has Key**	**Allow Impersonate**
ServiceDesk	No	Yes	No

Description

Used for integration between CA Service Catalog and CA SDM

Last Modified Date	Last Modified By
10/26/2011 11:57 am	ServiceDesk

1. Access Control | 2. Error Types

Access Control

Operations Per Hour

Ticket Creation	Object Creation	Object Updates
-1	-1	-1
Attachments	**Data Queries**	**Knowledge**
-1	-1	-1

The next step in integrating CA SDM with CA Service Catalog is to identify the location of the CA SDM server for CA Service Catalog.

Set and Test Administration Configuration Parameters

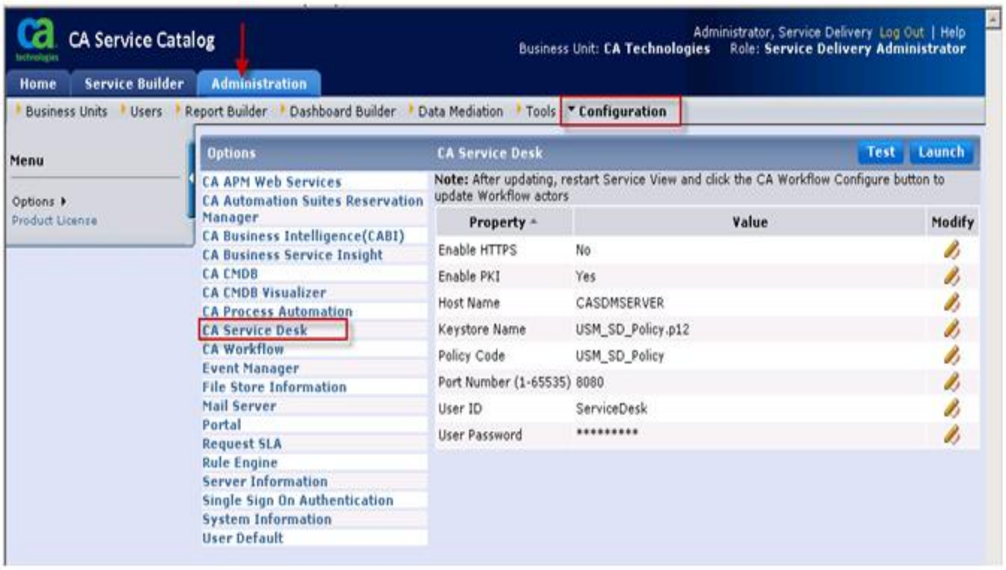
Specifying the configuration settings for CA SDM is a required task for enabling the integration between CA SDM and CA Service Catalog.

Follow these steps:

1. Log in to CA Service Catalog as an Administrator.

2. Navigate to Administration, Configuration, Options, CA Service Desk.

3. Enter the settings for the CA SDM primary server, including the Keystore Name and Policy File that you just created.



Note: After updating, restart Service View and click the CA Workflow Configure button to update Workflow actors

Property	Value	Modify
Enable HTTPS	No	✎
Enable PKI	Yes	✎
Host Name	CASDMSERVER	✎
Keystore Name	USM_SD_Policy.p12	✎
Policy Code	USM_SD_Policy	✎
Port Number (1-65535)	8080	✎
User ID	ServiceDesk	✎
User Password	*********	✎

4. Click Test.

   Note: Do not proceed, unless you receive a Connection Successful message.

5. Click Launch.

   Note: Do not proceed, unless the login screen for the CA SDM web interface launches.

Enable Rule Actions in CA Service Catalog

To allow CA Service Catalog to open a CA SDM change order during request fulfillment, you must enable several rule actions in CA Service Catalog that are disabled by default. In addition, for some of the rules, there are two mutually exclusive actions; one for use with CA SDM and one for use without CA SDM.

The rule conditions that are shipped with CA Service Catalog may not completely match your business processes. You can modify the rules to suit your business needs. In addition, some rules overlap in functionality. Before you activate the rules, understand the full implications of the rules.

You can use the out-of-the-box CA Process Automation processes to open a change order in CA SDM from CA Service Catalog. For example, you have a rule with a filter to launch once for each hardware request item in CA Service Catalog when the request status goes to Filled from Inventory status. You can enable this rule to open a change order in CA SDM. Perform the following steps in CA Service Catalog to activate this rule.

Follow these steps:

1. Log in to CA Service Catalog as an Administrator.
2. From the Home page, navigate to Administration, Tools, Events-Rules-Actions.

   The Events-Rules-Actions page displays.
3. Click the event type that is named Request/Subscription Item Change.
4. Click the rule that is named When Category is Hardware and Status is Filled from Inventory (formerly named WFHWFulfillment).

   The rule Actions list displays.
5. Select the action "Launch FilledFromInventory SRF for Hardware", click Disable, and click OK.
6. Select the action "Launch HWSWFilledFromInv_SDM SRF", click Enable, and click OK.

You can open a change order once for each software request item when its status goes to Filled From Inventory in CA Service Catalog. To perform this action, repeat this procedure for the rule that is named When Category is Software and Status is Filled from Inventory.

For more information about the events, rules, and actions and the out-of-the-box CA Process Automation process that are shipped with CA Service Catalog, see the *CA Service Catalog Integration Guide*.

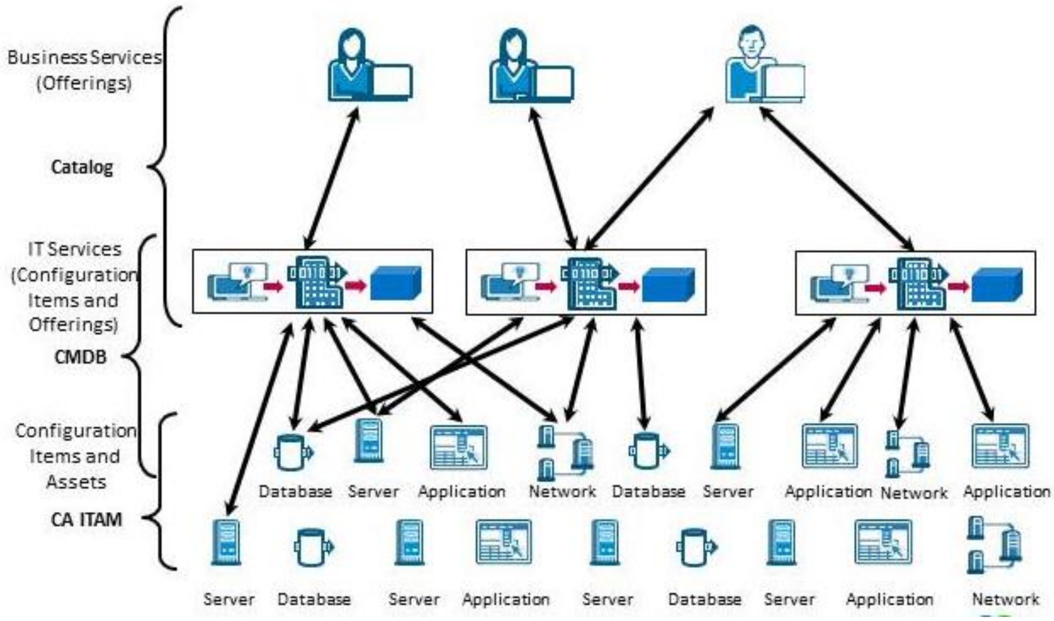
Note: If you are integrating CA SDM, CA Service Catalog and CA Asset Portfolio Management, the associated assets become configuration items on the related change order. For more information about the integration steps, see the *CA Service Catalog Integration Guide*.

Integrate the CA SDM CMDB Component with CA Service Catalog

Integrating CA Service Catalog with the CMDB component of CA SDM helps link infrastructure assets that comprise each service by addressing the following issues that occur when establishing a service catalog:

- Establishing links between the logical service and the physical infrastructure assets.
- Helping determine which infrastructure assets, or configuration items (CIs), comprise each service.
- Helping improve IT service quality, control costs, and align IT with the business.

The following diagram shows the relationships among the business services (which represent the services that customers can request), the CMDB component, and the individual configuration items.



When you associate a service offering in CA Service Catalog to a CI, you can:

- Select CA Service Catalog services for association to CA SDM CMDB component CIs, where the relationship is one-to-one, one-to-many, or many-to-many.
- Start the CA Service Catalog from the CA SDM CMDB component to view and analyze CI changes to services requested or subscribed.
- Report on CIs and service association.

It is important to build your services using terms that your customers understand. Your customers are not concerned about, nor do they understand, the individual CIs. Your customers only know that they want to order email, a cell phone, and so on.

The instructions to integrate CA Service Catalog with the CMDB component of CA SDM, including configuring integration with the CMDB Visualizer, are documented in the *CA Service Catalog Integration Guide*.

Perform Setup Tasks for the CA SDM CMDB Component

The following procedure provides additional details for creating the Web Services Access policy. The creation of this policy is described in the *CA Service Catalog Integration Guide*, along with the instructions for performing the post-installation setup.

Follow these steps:

1. Log in to CA SDM as an Administrator.
2. Click the Administration tab and browse to the Web Services Policy, Policies node.
3. Click Create New to create a Web Services policy.
4. Complete the Create New Web Services Access Policy page with the following values:

Property	Configuration Value
Symbol	USM_CMDB Policy
Code	USM_CMDB Policy
Status	Active
Proxy Contact	Name of a contact with administrative access to CMDB component functions.
Allow Impersonate	Checked (to indicate Yes)

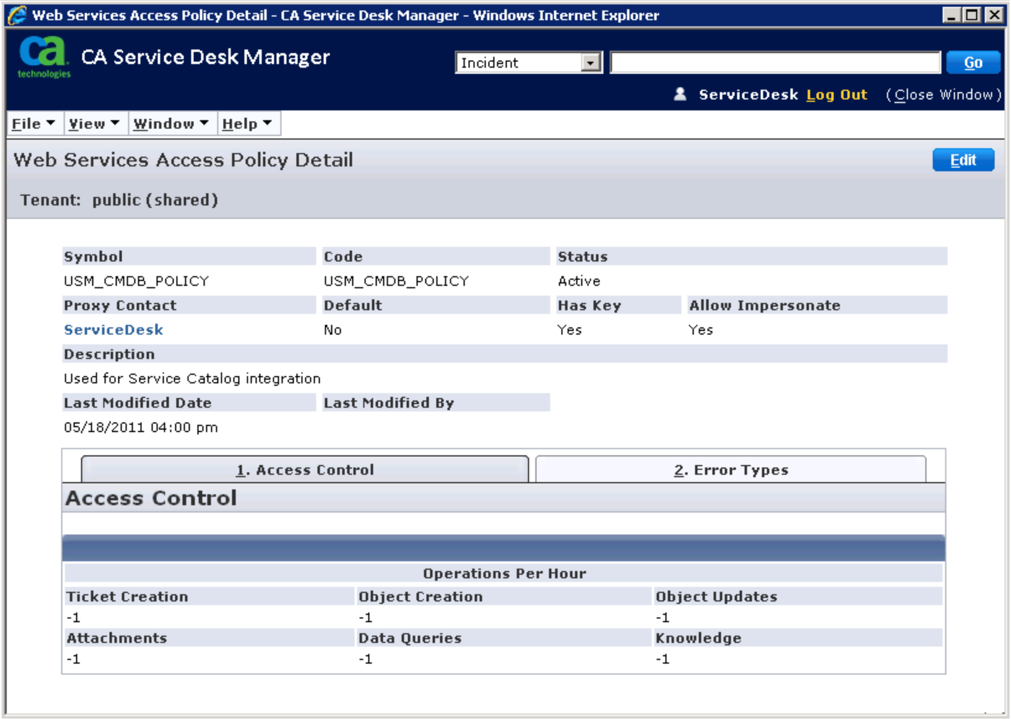
5. Click Save and close the Create New Web Services Access Policy page.

6. On the CA SDM primary server, open a command prompt and type the following command:

```
pdm_pki –p USM_CMDB_Policy
```

7. Copy the newly created USM_CMDB_Policy.p12 file that is located in the C:\ directory to the root directory on the CA Service Catalog server.

8. Verify the web service access policy that was created in CA SDM. Verify that the USM_CMDB_Policy shows a Has Key value that is set to Yes, as shown in the following example. This value should have been updated automatically when the key was generated.


Web Services Access Policy Detail - CA Service Desk Manager - Windows Internet Explorer
CA Service Desk Manager
Incident
Go
ServiceDesk Log Out (Close Window)
File View Window Help
Edit
1. Access Control
2. Error Types

Web Services Access Policy Detail

Tenant: public (shared)

Symbol	Code	Status	
USM_CMDB_POLICY	USM_CMDB_POLICY	Active	
Proxy Contact	**Default**	**Has Key**	**Allow Impersonate**
ServiceDesk	No	Yes	Yes

Description

Used for Service Catalog integration

Last Modified Date	Last Modified By
05/18/2011 04:00 pm	

Access Control

Operations Per Hour

Ticket Creation	Object Creation	Object Updates
-1	-1	-1
Attachments	**Data Queries**	**Knowledge**
-1	-1	-1

9. Copy the policy key file that you created previously to the CA Service Catalog server and save it in the %USM_HOME% directory.

10. Log in to CA SDM as an administrator and verify that the Business Service class of the Enterprise Service family exists. This class is required for CA Service Catalog users to create a configuration item in the CMDB component of CA SDM. If this class does not exist, create it manually or rerun the CMDB component installation to load default data.

Perform Setup Tasks for CA Service Catalog

The following procedure provides some additional details for configuring the CA SDM CMDB component and CMDB Visualizer.

Follow these steps:

1. As a CA Service Catalog administrator on the CA Service Catalog computer, log in to CA Service Catalog.

2. Click the Administration tab and select Configuration.

3. Update the configuration settings for the CMDB component with the following values:

   - Default New CI State: Inactive

     As a best practice, set the “Default New CI State” to Inactive in the CMDB Configuration window. This setting helps ensure that no new unauthorized or unapproved CIs are being added to the CMDB component. New Business Service CIs need to be activated by a CMDB component Administrator and any related CIs need to be associated.

   - Enable HTTPS: (if using https, select the check box for Enable HTTPS).

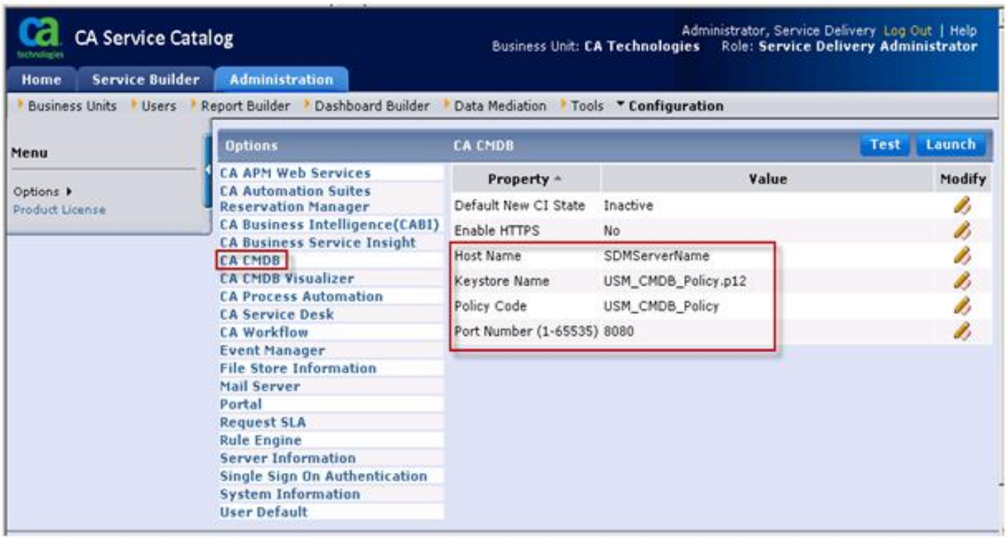
     If the CMDB component is configured to be accessed using https, then set the value for Enable HTTPS to Yes.

     Note: For the CMDB component and CMDB Visualizer configurations, the *CA Service Catalog Integration Guide* states to set the Enable HTTPS to No. However, the value for the Enable HTTPS setting depends on how the CMDB component is configured.

   - Host Name: host name of your CA SDM server

   - Keystore Name: USM_CMDB_Policy.p12 (previously created)

- Policy Code: USM_CMDB_POLICY (previously created)
- Port Number: port number where CA SDM is running



Property	Value	Modify
Default New CI State	Inactive	
Enable HTTPS	No	
Host Name	SDMServerName	
Keystore Name	USM_CMDB_Policy.p12	
Policy Code	USM_CMDB_Policy	
Port Number (1-65535)	8080	

4. Test the connection.

5. Update the configuration settings for CMDB Visualizer with the following values:

   - Enable HTTPS: checked (if you are using https)
   - Host Name: host name of the CA SDM server
   - Port Number: port number for the CMDB Visualizer

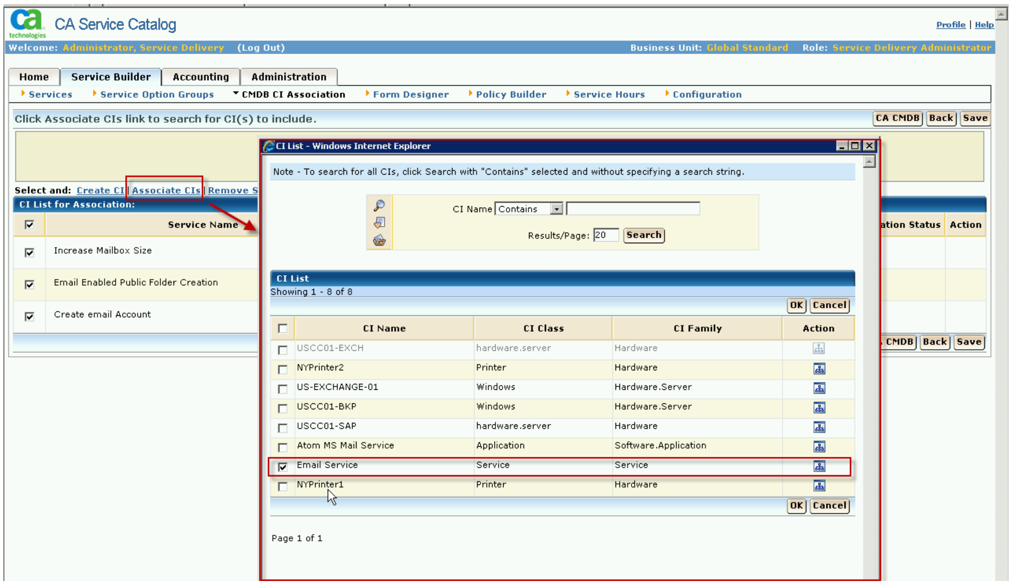
Associate CA Service Catalog Services with CIs

You can view, modify, and create associations between CA Service Catalog services and any CMDB component configuration items. Typically, the most suitable configuration items belong to the Business Service class in the Enterprise Services family. Several configuration items in this family and class are provided by default, but you can create any CIs that you need.

After completing the instructions in the *CA Service Catalog Integration Guide* for setting up the integration, you will be able to associate a CA Service Catalog service with a CA SDM configuration item.

Follow these steps:

1. From CA Service Catalog, click the CMDB CI Association link on the Service Builder tab.
2. Search for and select the CA Service Catalog services that you want to associate with CA SDM CIs.
3. In the CI List for Associations, select the services and click the Associate CIs link, as shown in the following example.



Click Associate CIs link to search for CI(s) to include.

CI List for Association:

☑	Service Name
☑	Increase Mailbox Size
☑	Email Enabled Public Folder Creation
☑	Create email Account

Note - To search for all CIs, click Search with "Contains" selected and without specifying a search string.

CI Name Contains

Results/Page: 20

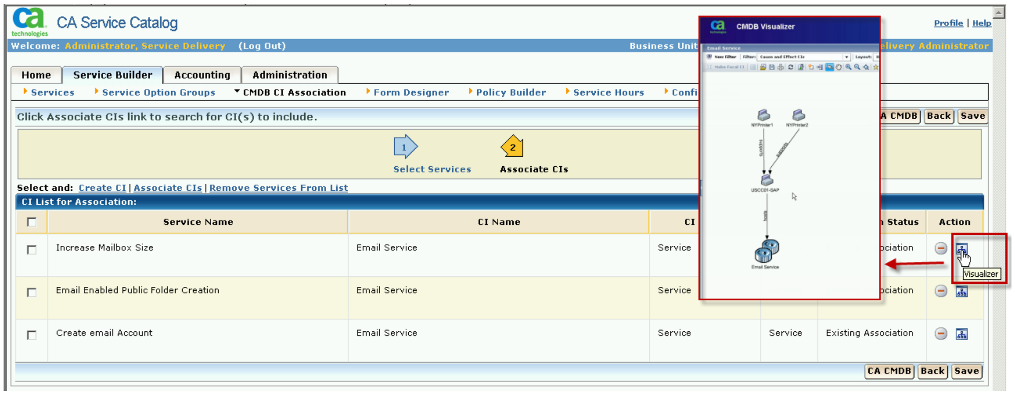
CI List

Showing 1 - 8 of 8

□	CI Name	CI Class	CI Family	Action
□	USCC01-EXCH	hardware.server	Hardware	
□	NYPrinter2	Printer	Hardware	
□	US-EXCHANGE-01	Windows	Hardware.Server	
□	USCC01-BKP	Windows	Hardware.Server	
□	USCC01-SAP	hardware.server	Hardware	
□	Atom MS Mail Service	Application	Software.Application	
☑	Email Service	Service	Service	
□	NYPrinter1	Printer	Hardware	

Page 1 of 1

The list that is displayed shows CA SDM CIs. After the CIs are selected, they are linked to CA Service Catalog. In addition, there is a link to launch the CMDB Visualizer, as shown in the following example, to perform root cause or impact analysis.



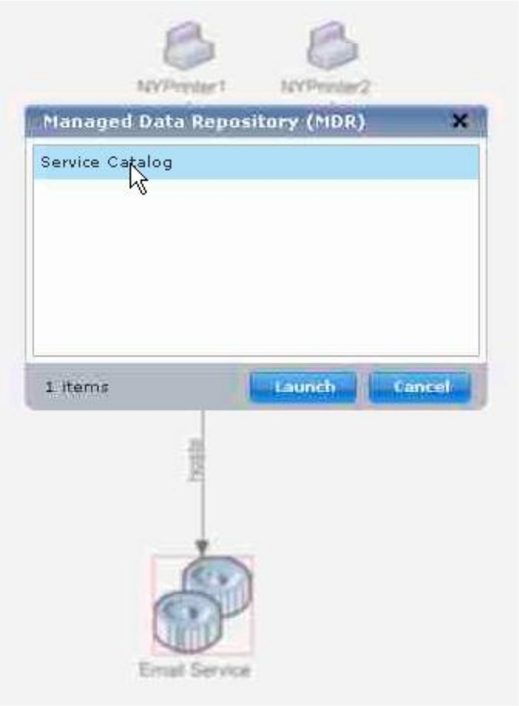
Click Associate CIs link to search for CI(s) to include.

CI List for Association:

□	Service Name	CI Name	CI		n Status	Action
□	Increase Mailbox Size	Email Service	Service		ociation	
□	Email Enabled Public Folder Creation	Email Service	Service		ociation	
□	Create email Account	Email Service	Service	Service	Existing Association	

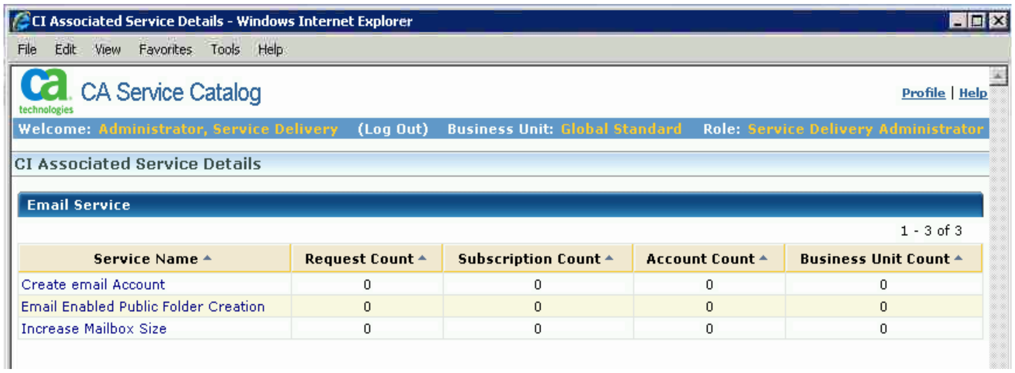
4. Right-click the focal service icon in the CMDB Visualizer and select Launch MDR.

   The Service Catalog MDR appears as a selection as shown in the following example.



5. Select Service Catalog and click Launch.

   The CI Associated Service Details page displays to show current CA Service Catalog counts, as shown in the following example.



Welcome: Administrator, Service Delivery (Log Out) Business Unit: Global Standard Role: Service Delivery Administrator

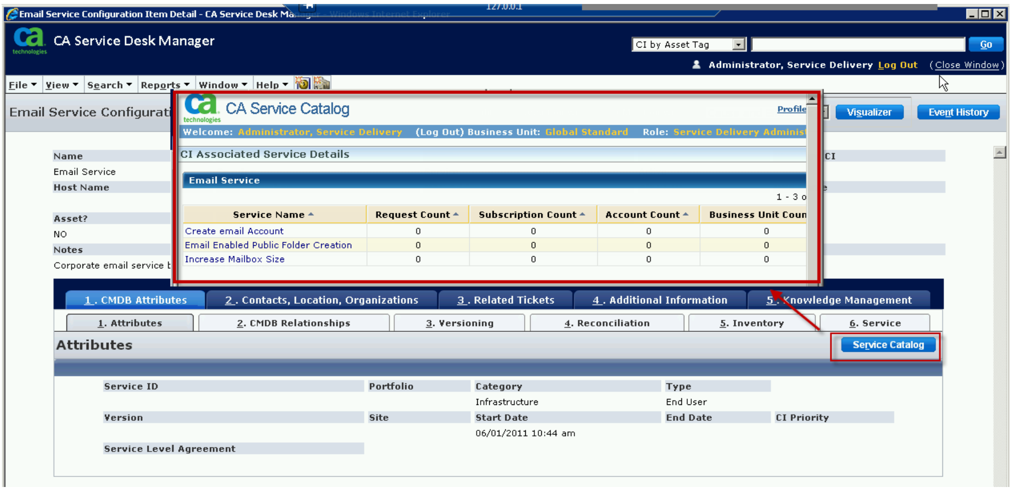
CI Associated Service Details

Email Service

1 - 3 of 3

Service Name	Request Count	Subscription Count	Account Count	Business Unit Count
Create email Account	0	0	0	0
Email Enabled Public Folder Creation	0	0	0	0
Increase Mailbox Size	0	0	0	0

In addition, a link to the CA Service Catalog CI Associated Service Details page becomes available from the CI Attributes tab in CA SDM, as shown in the following example.



Welcome: Administrator, Service Delivery (Log Out) Business Unit: Global Standard Role: Service Delivery Adminis

CI Associated Service Details

Email Service

1 - 3 o

Service Name	Request Count	Subscription Count	Account Count	Business Unit Coun
Create email Account	0	0	0	0
Email Enabled Public Folder Creation	0	0	0	0
Increase Mailbox Size	0	0	0	0

Name
Email Service
Host Name
Asset?
NO
Notes
Corporate email service b

Attributes

Service ID	Portfolio	Category	Type	
		Infrastructure	End User	
Version	Site	Start Date	End Date	CI Priority
		06/01/2011 10:44 am		
Service Level Agreement				

Note: The CI Attributes tab is where MDR links, such as the link to CA Service Catalog, are found.

Integration of CA Process Automation with CA Service Catalog

CA Process Automation is an optional integration for CA Service Catalog. However, completing the integration between CA Process Automation and CA Service Catalog is necessary when integration with CA SDM is required. With this integration, the default CA Process Automation Complex Fulfillment workflows are made available to extend the integration to CA SDM.

This integration provides simple approval and fulfillment of CA Service Catalog requests. For more information about the integration instructions and best-practice advice, see the *CA Service Catalog Integration Guide.*

Note: CA Process Automation was formerly known as CA IT Process Automation Manager, or CA IT PAM. This Green Book uses the current name CA Process Automation, unless referring to user interface instances where the former name is used.

Create a CA Process Automation Certificate

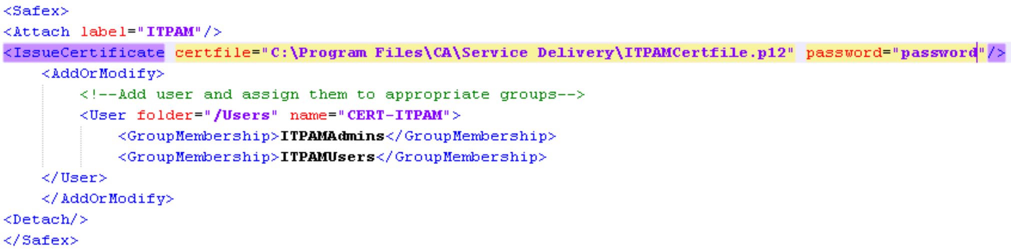
If you want to use certificate-based authentication, generate the certificate (even if you are integrating CA EEM with an external directory). The groups that you create are specific to the application and are still accessible. However, you cannot log in to CA Service Catalog because these users are not part of the global users group. The groups and users that are defined in the external directory become part of the global group and can be accessible to all the applications that are registered for the CA EEM server.

Follow these steps for CA Service Catalog 12.6:

1. Navigate to the following directory:

   `%USM_HOME%/scripts/EIAM`
2. Back up the file IssueITPAMCertificate.xml (on an upgraded instance of CA Process Automation 3.1) or the file IssuePAMCertificate.xml (on a fresh install of CA Process Automation 3.1).

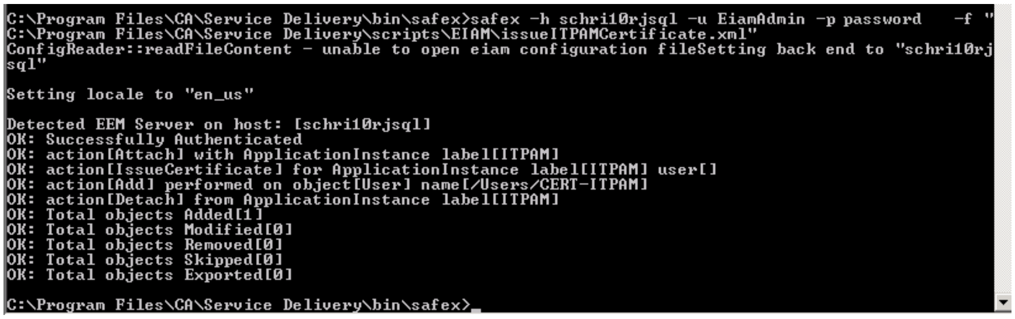
3. Open the original file for editing and edit according to instructions in the *CA Service Catalog Integration Guide,* Release 12.6. The following graphic provides an example:



```
<Safex>
<Attach label="ITPAM"/>
<IssueCertificate certfile="C:\Program Files\CA\Service Delivery\ITPAMCertfile.p12" password="password"/>
    <AddOrModify>
        <!--Add user and assign them to appropriate groups-->
        <User folder="/Users" name="CERT-ITPAM">
            <GroupMembership>ITPAMAdmins</GroupMembership>
            <GroupMembership>ITPAMUsers</GroupMembership>
    </User>
    </AddOrModify>
<Detach/>
</Safex>
```

4. Open a Service Delivery command prompt by selecting Start, Programs, CA, Service Delivery, Service Delivery command prompt.

5. Execute the safex utility, as shown in the following example.



```
C:\Program Files\CA\Service Delivery\bin\safex>safex -h schri10rjsql -u EiamAdmin -p password   -f "
C:\Program Files\CA\Service Delivery\scripts\EIAM\issueITPAMCertificate.xml"
ConfigReader::readFileContent - unable to open eiam configuration fileSetting back end to "schri10rj
sql"

Setting locale to "en_us"

Detected EEM Server on host: [schri10rjsql]
OK: Successfully Authenticated
OK: action[Attach] with ApplicationInstance label[ITPAM]
OK: action[IssueCertificate] for ApplicationInstance label[ITPAM] user[]
OK: action[Add] performed on object[User] name[/Users/CERT-ITPAM]
OK: action[Detach] from ApplicationInstance label[ITPAM]
OK: Total objects Added[1]
OK: Total objects Modified[0]
OK: Total objects Removed[0]
OK: Total objects Skipped[0]
OK: Total objects Exported[0]

C:\Program Files\CA\Service Delivery\bin\safex>_
```

   The safex utility generated an ITPAMCertfile in %USM_HOME%.

6. Open the original XML file again and remove the password.

Follow these steps for CA Service Catalog 12.7:

1. Navigate to the following directory:

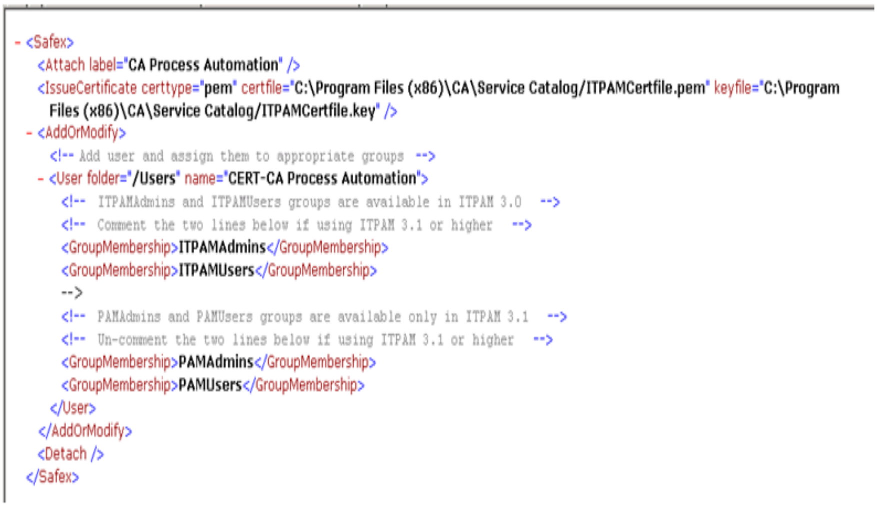
   ```
   %USM_HOME%/scripts/EIAM
   ```

2. Update the file IssueITPAMCertificatePEM.xml by performing the following actions:

   a. Replace __USMHOME_ (a placeholder value) with the actual value of %USM_HOME% (for example, C:\Program Files (x86)\CA\CA Service Catalog).

   b. Replace ITPAMCONTEXT (a placeholder value) with the actual value of the application context name that CA Process Automation uses to connect to CA EEM (for example, "CA Process Automation").

   The following graphic shows a sample file:



```
- <Safex>
    <Attach label="CA Process Automation" />
    <IssueCertificate certtype="pem" certfile="C:\Program Files (x86)\CA\Service Catalog/ITPAMCertfile.pem" keyfile="C:\Program
      Files (x86)\CA\Service Catalog/ITPAMCertfile.key" />
  - <AddOrModify>
      <!-- Add user and assign them to appropriate groups  -->
    - <User folder="/Users" name="CERT-CA Process Automation">
        <!--  ITPAMAdmins and ITPAMUsers groups are available in ITPAM 3.0   -->
        <!--  Comment the two lines below if using ITPAM 3.1 or higher   -->
        <GroupMembership>ITPAMAdmins</GroupMembership>
        <GroupMembership>ITPAMUsers</GroupMembership>
        -->
        <!--  PAMAdmins and PAMUsers groups are available only in ITPAM 3.1   -->
        <!--  Un-comment the two lines below if using ITPAM 3.1 or higher   -->
        <GroupMembership>PAMAdmins</GroupMembership>
        <GroupMembership>PAMUsers</GroupMembership>
      </User>
    </AddOrModify>
    <Detach />
  </Safex>
```

3. Create a .pem file by performing the following actions:

   a. Open the Windows command prompt and change to the %USM_HOME%\bin\safex folder.

   b. Execute the following command:

   ```
   safex.exe -u EiamAdmin -p password -h eemserver
   -f %USM_HOME%\scripts\eiam\issueitpamcertificatepem.xml -sdkconfig
   %USMHOME%\eiam.config
   ```

   This action creates the ITPAMCertfile.pem and the ITPAMCertfile.key files. Both files are required for the .pem file authentication to work.

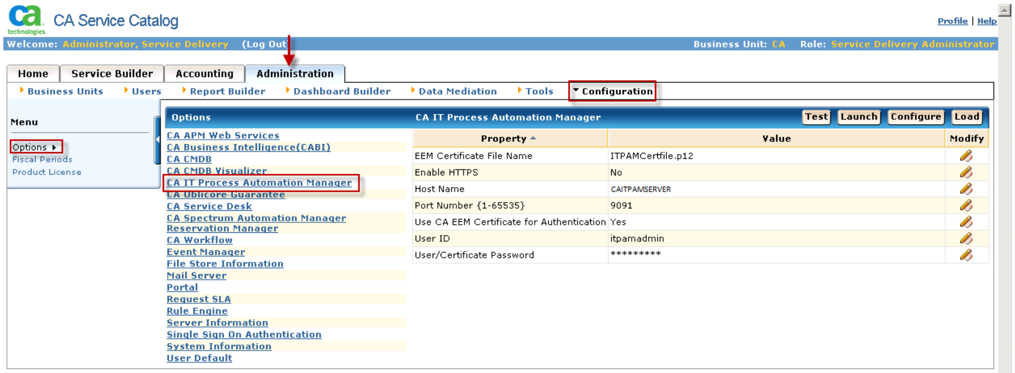
Set and Test Administration Configuration Parameters

Specifying the configuration settings for CA Process Automation is a required task for enabling the integration between CA Process Automation and CA Service Catalog. If you are running multiple instances of CA Process Automation, these settings apply to all instances.

Follow these steps:

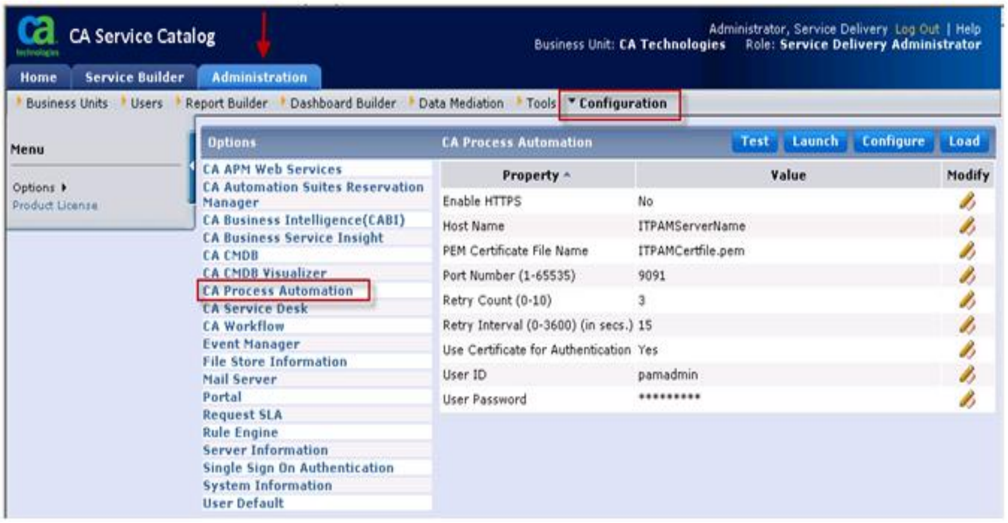
1. Log in to CA Service Catalog as an Administrator.
2. Navigate to Administration, Configuration, Options, CA Process Automation. (In version 12.6, CA IT Process Automation Manager is displayed.)
3. Enter the settings for your CA SDM primary server, including the CA EEM Certificate Name that you created.

   Example for CA Service Catalog 12.6:



Property	Value	Modify
EEM Certificate File Name	ITPAMCertfile.p12	
Enable HTTPS	No	
Host Name	CAITPAMSERVER	
Port Number {1-65535}	9091	
Use CA EEM Certificate for Authentication	Yes	
User ID	itpamadmin	
User/Certificate Password	*********	

   Example for CA Service Catalog 12.7:



Property	Value	Modify
Enable HTTPS	No	
Host Name	ITPAMServerName	
PEM Certificate File Name	ITPAMCertfile.pem	
Port Number (1-65535)	9091	
Retry Count (0-10)	3	
Retry Interval (0-3600) (in secs.)	15	
Use Certificate for Authentication	Yes	
User ID	pamadmin	
User Password	*********	

4. Click Test.

   Note: Do not proceed unless you receive the Connection Successful message. If the test fails, retype the password for the ITPAMADMIN (or pamadmin) user and run the test again. This password must match the password that is defined in the CA EEM Certificate.

5. Click Launch.

   Note: Do not proceed unless the login screen for the CA Process Automation web interface appears. Do not click Configure or Load yet. You do that next.

Load and Configure the CA Process Automation Content

The CA Process Automation content refers to the processes, start request forms (SRFs), rules, actions, and other content that are supplied with CA Service Catalog. This content is installed when you install CA Service Catalog. After you install CA Process Automation, load this content to activate it. For more information about loading and configuring the CA Process Automation content, see the *CA Service Catalog Integration Guide*.

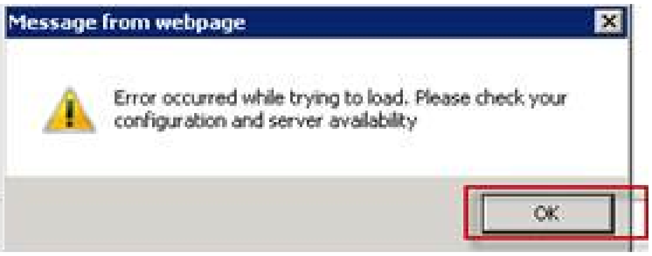
Follow these steps:

1. Log in to CA Service Catalog as an Administrator.

2. Click Administration, Configuration, Options, CA IT Process Automation Manager.

3. Disable the use of the CA EEM Certificate by setting Use CA EEM for Authentication to No and clearing the line for EEM Certificate Name.

   If you try to load the content while using the CA EEM Certificate for Authentication, it fails with the following error:



Message from webpage

Error occurred while trying to load. Please check your configuration and server availability

   Note: After the load is successful, you can switch Use CA EEM Certificate for Authentication back to Yes.

4. Click Load and check the box for "Set imported version of CA Process Automation Objects as current version". Also check the box for "Make imported Custom Operators/Sensors available".

   You should get the following return message: Content was loaded successfully. For more information about additional configuration instructions, see the *CA Service Catalog Integration Guide*.

   This step loads the SRFs, rules, and actions that you want to use for approval and fulfillment. This step includes loading the content.

5. Click Configure.

   This step executes a process in CA Process Automation. This process takes all of the information that you previously supplied to update the location information for CA SDM, CA Process Automation, and CA Asset Portfolio Management and updates the necessary GlobalDataSets in CA Process Automation. This step does not move over password information, which is a manual step.

   You should get the following return message: Configuration Successful

6. If you want to use the CA EEM Certificate, set Use CA EEM for Authentication back to Yes and enter the name of the CA EEM Certificate for EEM Certificate Name.

Configure Additional Content from CA Process Automation

Additional configuration is necessary for CA Process Automation to communicate with CA SDM and CA Service Catalog. For more information, see the *CA Service Catalog Integration Guide*.

Follow these steps:

1. Log in to CA Process Automation as an Administrator.

2. Launch the client by clicking CA Process Automation Client.

3. In the configuration browser, click the tab Default Environment: Orchestrator.

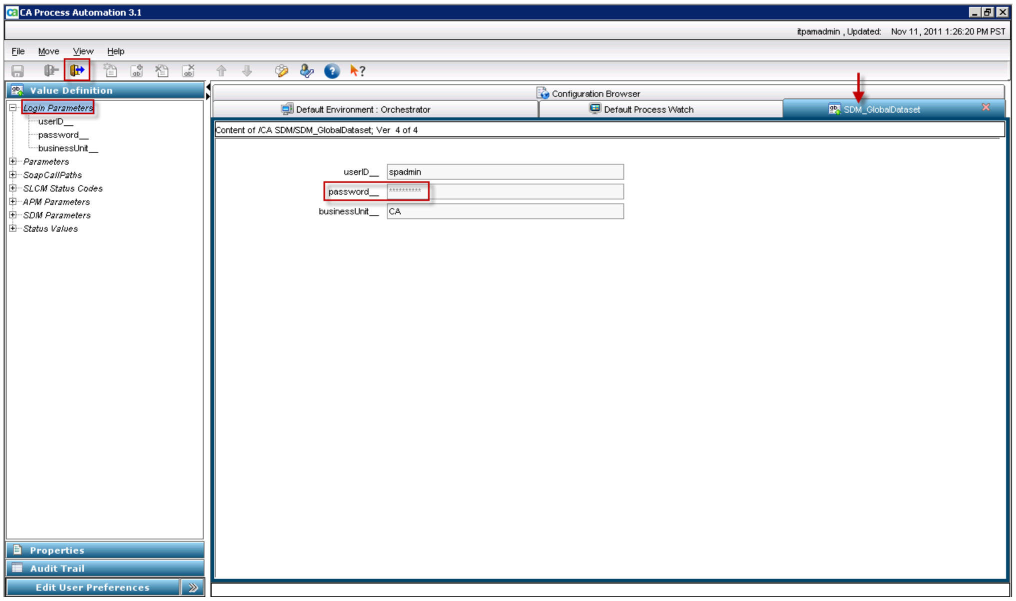
   All of the content loaded in the last step is placed into the CA SDM, CA SLCM, and Custom Operators directories, respectively.

4. Click the CA SDM folder. On the right are all of the processes, interaction request forms (IRFs), and datasets that are required to run the Complex Fulfillment process.

5. Double-click SDM_GlobalDataset to modify the Login Parameters.

   Most of the connection information should have been brought over after you loaded the content in CA Service Catalog and clicked Configure. The way that this process happened in the back end was by running the UpdateGlobalDatasets process. However, the password was not brought over, so we need to update it here.

6. Update the password for the CA Service Catalog Administrative user. To update the password, check out the dataset (highlighted in red in the following example), make the change, and click Save and Check In.



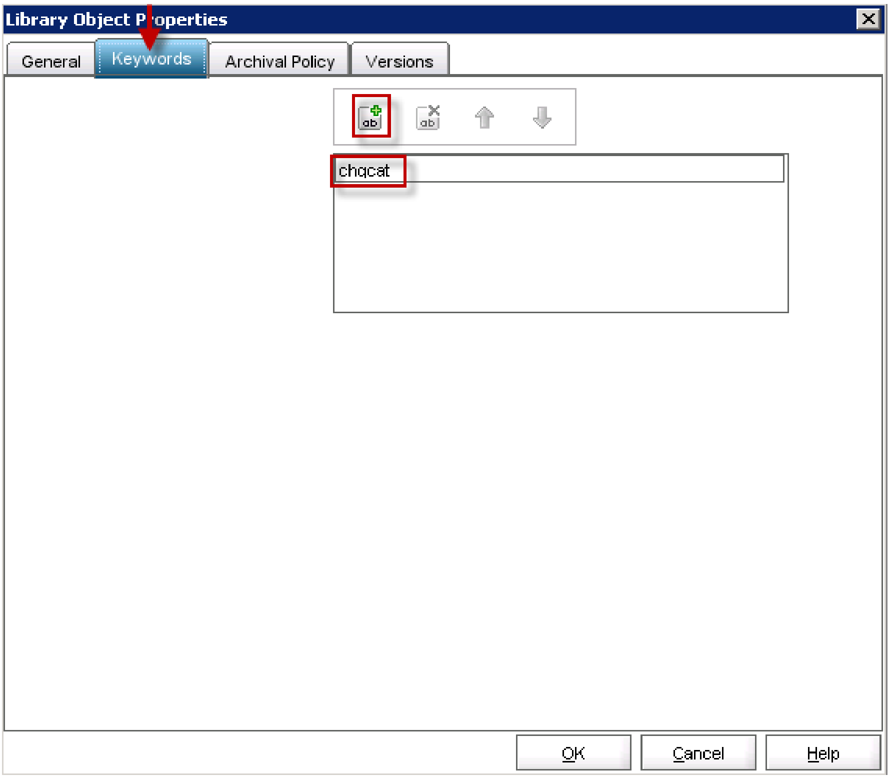
Content of /CA SDM/SDM_GlobalDataset; Ver 4 of 4

userID__ spadmin
password__ **********
businessUnit__ CA

The subdirectory SRFs contains all of the SRFs that are required to run the Complex Fulfillment process.

7. Under the CA SDM, SRF folder, update each of the start request forms by right-clicking them and selecting Properties. On the Keywords tab, click Add and enter chgcat in the text area.

   Note: Adding this keyword enables the process to be launched from within a CA SDM Change Order Category. The integration is designed so that you attach an SRF to a Change Order Category. This action invokes the underlying process definition.



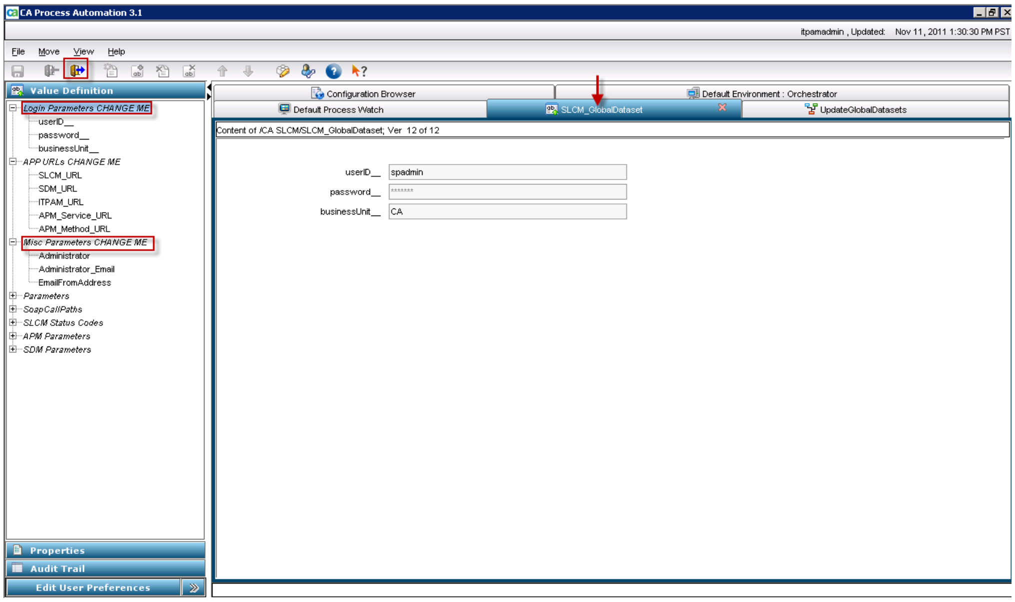
chgcat

8. Navigate to the CA SLCM folder.

   The process is the same, but you modify the SLCM_GlobalDataset for Login parameters, APP URLs, and Misc Parameters.

   The URLs should have been brought over after you loaded the content in CA Service Catalog and clicked Configure. The way that this process happened in the back end was by running the UpdateGlobalDatasets process. However, passwords and email addresses were not brought over, so you need to update them here.

9. Check out the dataset SLCM_GlobalDataset (highlighted by the red arrow in the following graphic) and make the change. Click Save and Check In.



Content of /CA SLCM/SLCM_GlobalDataset; Ver 12 of 12

userID__ spadmin
password__ *******
businessUnit__ CA

After communication is established between the two applications from an Administrative perspective, configure CA Service Catalog to open CA SDM change orders through CA Process Automation for request fulfillment by enabling the CA Service Catalog rule actions.

CA Service Catalog Launch Points - Events, Rules, Actions

Both CA SDM and CA Service Catalog can launch a CA Process Automation process definition by tying a launch point (described in this section) to a CA Process Automation SRF. The CA Process Automation SRFs are tied to CA Process Automation process definitions.

Events, rules, and actions are used in CA Service Catalog to perform specific actions when triggered. Events can have rules that are associated with them. Rules can have a set of filter conditions that define when the rules apply. When the filter conditions are satisfied and the rule is enabled, the rule actions are launched.

When a request is initiated in CA Service Catalog, the event Request Subscription/Item Change is triggered. This event has many rules that check for criteria within the request and, if met, invoke a CA Process Automation process accordingly.

Note: The rule conditions that are shipped with CA Service Catalog may not completely match your business processes. You can modify the rules to suit your business needs. In addition, some rules overlap in functionality. Before you activate rules, understand the full implications.

To allow CA Service Catalog to open a CA SDM change order during request fulfillment using the out-of-the-box CA Process Automation process definitions, you must enable several rule actions in CA Service Catalog that are disabled by default. In addition, for some of the rules, there are two mutually exclusive actions: one for use with CA SDM (Complex Fulfillment) and one for use without CA SDM (Simple Fulfillment).

This section focuses on the Complex Fulfillment process, using the out-of-the-box CA Process Automation processes provided with CA Service Catalog that you imported previously. The example that is discussed in this section is the fulfillment of a hardware request.

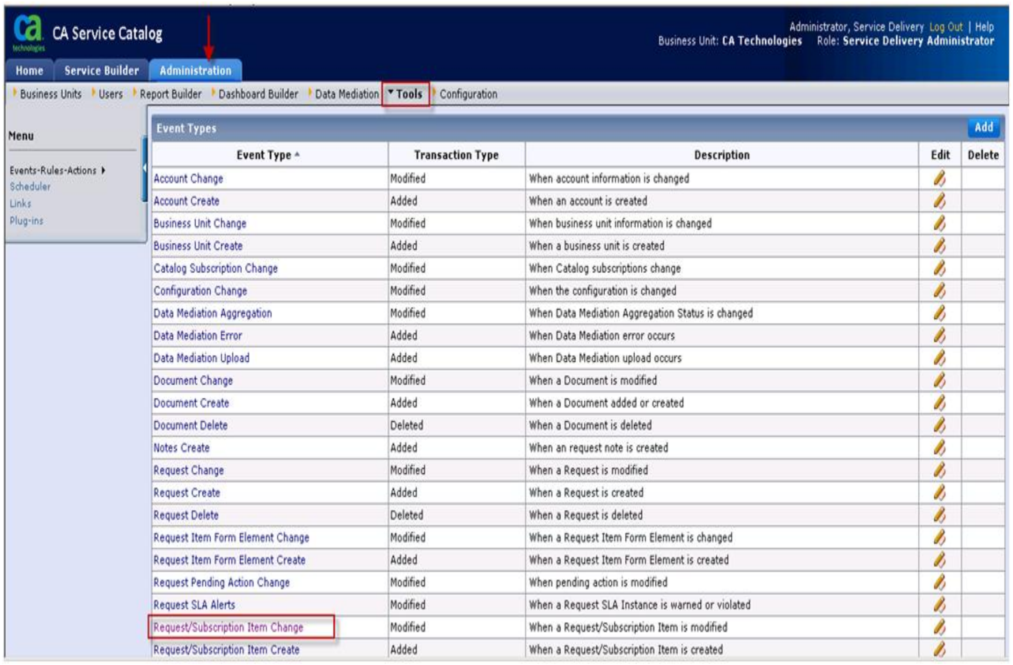
Enable Launch Points

To activate rules and rule actions, perform the following steps in CA Service Catalog.

Follow these steps:

1. Log in to CA Service Catalog as an Administrator.
2. Navigate to Administration, Tools, Events-Rules-Actions.

   The Events-Rules-Action page is displayed.

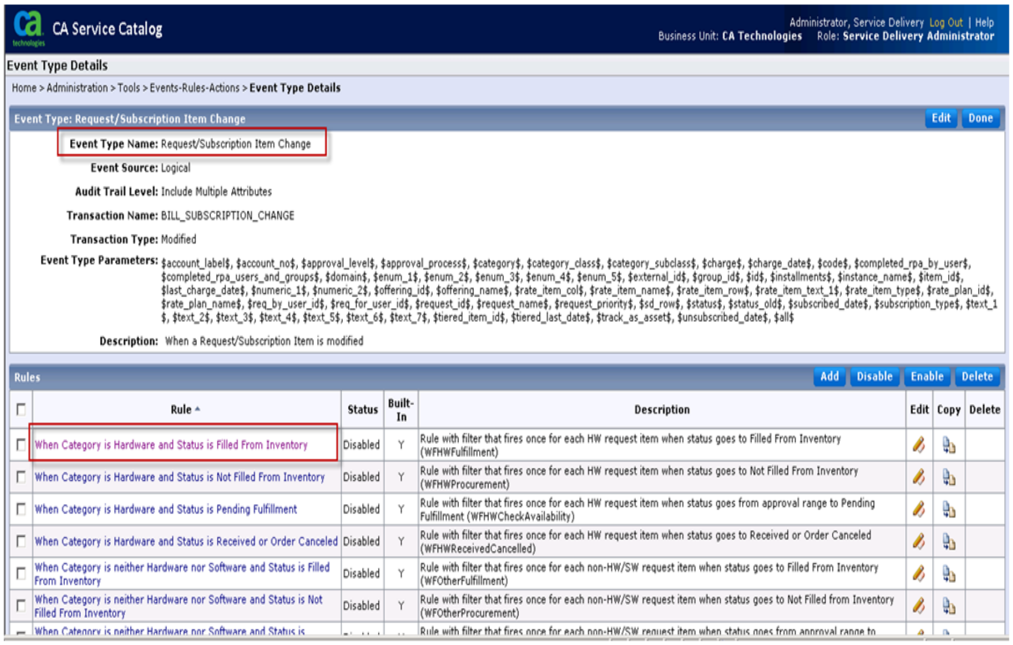


Event Type	Transaction Type	Description	Edit	Delete
Account Change	Modified	When account information is changed	✎	
Account Create	Added	When an account is created	✎	
Business Unit Change	Modified	When business unit information is changed	✎	
Business Unit Create	Added	When a business unit is created	✎	
Catalog Subscription Change	Modified	When Catalog subscriptions change	✎	
Configuration Change	Modified	When the configuration is changed	✎	
Data Mediation Aggregation	Modified	When Data Mediation Aggregation Status is changed	✎	
Data Mediation Error	Added	When Data Mediation error occurs	✎	
Data Mediation Upload	Added	When Data Mediation upload occurs	✎	
Document Change	Modified	When a Document is modified	✎	
Document Create	Added	When a Document added or created	✎	
Document Delete	Deleted	When a Document is deleted	✎	
Notes Create	Added	When an request note is created	✎	
Request Change	Modified	When a Request is modified	✎	
Request Create	Added	When a Request is created	✎	
Request Delete	Deleted	When a Request is deleted	✎	
Request Item Form Element Change	Modified	When a Request Item Form Element is changed	✎	
Request Item Form Element Create	Added	When a Request Item Form Element is created	✎	
Request Pending Action Change	Modified	When pending action is modified	✎	
Request SLA Alerts	Modified	When a Request SLA Instance is warned or violated	✎	
Request/Subscription Item Change	Modified	When a Request/Subscription Item is modified	✎	
Request/Subscription Item Create	Added	When a Request/Subscription Item is created	✎	

3. Click the Event Type named Request/Subscription Item Change.

4. Verify that the rule named When Category is Hardware and Status is Filled from Inventory (formerly WFHWFulfillment) is enabled. If it is not enabled, select the check box for the rule and click Enable.

5. Click the rule When Category is Hardware and Status is Filled from Inventory (the rule has a hyperlink).


CA Service Catalog
Administrator, Service Delivery Log Out | Help
Business Unit: CA Technologies Role: Service Delivery Administrator
Edit
Done
Add
Disable
Enable
Delete

Event Type Details

Home > Administration > Tools > Events-Rules-Actions > **Event Type Details**

Event Type: Request/Subscription Item Change

Event Type Name: Request/Subscription Item Change

Event Source: Logical

Audit Trail Level: Include Multiple Attributes

Transaction Name: BILL_SUBSCRIPTION_CHANGE

Transaction Type: Modified

Event Type Parameters: $account_label$, $account_no$, $approval_level$, $approval_process$, $category$, $category_class$, $category_subclass$, $charge$, $charge_date$, $code$, $completed_rpa_by_user$, $completed_rpa_users_and_groups$, $domain$, $enum_1$, $enum_2$, $enum_3$, $enum_4$, $enum_5$, $external_id$, $group_id$, id, $installments$, $instance_name$, $item_id$, $last_charge_date$, $numeric_1$, $numeric_2$, $offering_id$, $offering_name$, $rate_item_col$, $rate_item_name$, $rate_item_row$, $rate_item_text_1$, $rate_item_type$, $rate_plan_id$, $rate_plan_name$, $req_by_user_id$, $req_for_user_id$, $request_id$, $request_name$, $request_priority$, sd_row, $status$, $status_old$, $subscribed_date$, $subscription_type$, $text_1$, $text_2$, $text_3$, $text_4$, $text_5$, $text_6$, $text_7$, $tiered_item_id$, $tiered_last_date$, $track_as_asset$, $unsubscribed_date$, all

Description: When a Request/Subscription Item is modified

Rules

□	Rule ▲	Status	Built-In	Description	Edit	Copy	Delete
□	When Category is Hardware and Status is Filled From Inventory	Disabled	Y	Rule with filter that fires once for each HW request item when status goes to Filled From Inventory (WFHWFulfillment)	✎	⧉	
□	When Category is Hardware and Status is Not Filled From Inventory	Disabled	Y	Rule with filter that fires once for each HW request item when status goes to Not Filled From Inventory (WFHWProcurement)	✎	⧉	
□	When Category is Hardware and Status is Pending Fulfillment	Disabled	Y	Rule with filter that fires once for each HW request item when status goes from approval range to Pending Fulfillment (WFHWCheckAvailability)	✎	⧉	
□	When Category is Hardware and Status is Received or Order Canceled	Disabled	Y	Rule with filter that fires once for each HW request item when status goes to Received or Order Canceled (WFHWReceivedCancelled)	✎	⧉	
□	When Category is neither Hardware nor Software and Status is Filled From Inventory	Disabled	Y	Rule with filter that fires once for each non-HW/SW request item when status goes to Filled From Inventory (WFOtherFulfillment)	✎	⧉	
□	When Category is neither Hardware nor Software and Status is Not Filled From Inventory	Disabled	Y	Rule with filter that fires once for each non-HW/SW request item when status goes to Not Filled from Inventory (WFOtherProcurement)	✎	⧉	
□	When Category is neither Hardware nor Software and Status is			Rule with filter that fires once for each non-HW/SW request item when status goes from approval range to			

The rule Actions list is displayed.

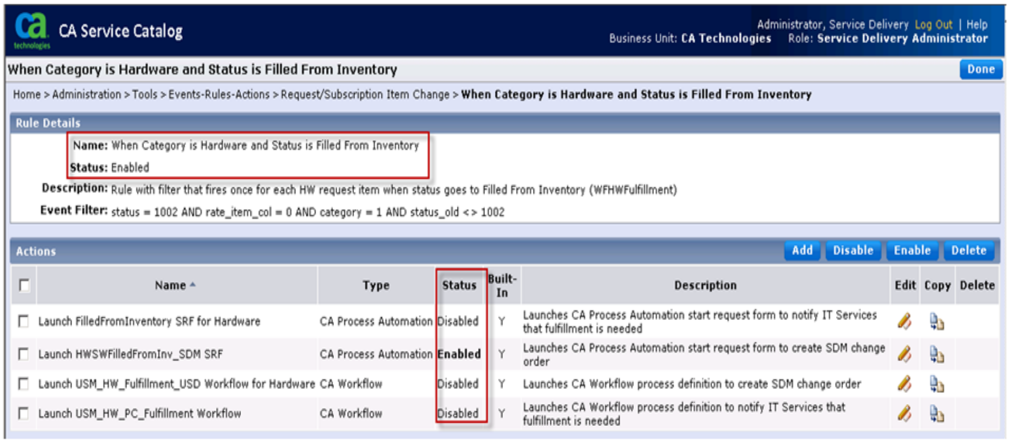
6. Select the action "Launch FilledFromInventory SRF for Hardware", click Disable, and click OK.

7. Select the action "Launch HWSWFilledFromInv_SDM SRF", click Enable, and click OK.

8. Select the action "Launch USM_HW_Fulfillment_USD Workflow for Hardware", click Disable, and click OK.

9. Select the action "Launch USM_HW_PC_Fulfillment Workflow", click Disable, and click OK.

   The Actions list appears as shown in the following example.


CA Service Catalog
Administrator, Service Delivery Log Out | Help
Business Unit: CA Technologies Role: Service Delivery Administrator
Done
Add
Disable
Enable
Delete

When Category is Hardware and Status is Filled From Inventory

Home > Administration > Tools > Events-Rules-Actions > Request/Subscription Item Change > **When Category is Hardware and Status is Filled From Inventory**

Rule Details

Name: When Category is Hardware and Status is Filled From Inventory
Status: Enabled
Description: Rule with filter that fires once for each HW request item when status goes to Filled From Inventory (WFHWFulfillment)
Event Filter: status = 1002 AND rate_item_col = 0 AND category = 1 AND status_old <> 1002

Actions

□	Name	Type	Status	Built-In	Description	Edit	Copy	Delete
□	Launch FilledFromInventory SRF for Hardware	CA Process Automation	Disabled	Y	Launches CA Process Automation start request form to notify IT Services that fulfillment is needed	✎	⎘	
□	Launch HWSWFilledFromInv_SDM SRF	CA Process Automation	**Enabled**	Y	Launches CA Process Automation start request form to create SDM change order	✎	⎘	
□	Launch USM_HW_Fulfillment_USD Workflow for Hardware	CA Workflow	Disabled	Y	Launches CA Workflow process definition to create SDM change order	✎	⎘	
□	Launch USM_HW_PC_Fulfillment Workflow	CA Workflow	Disabled	Y	Launches CA Workflow process definition to notify IT Services that fulfillment is needed	✎	⎘	

10. (Optional) Repeat this procedure for the rule When Category is Software and Status is Filled from Inventory (if you want to enable rules and actions for the category of software or none).

For information about verifying the rules and actions that need to be disabled and enabled for hardware requests, see the Rules and Actions Checklist for the Request Subscription/Item Change Event (see page 70).

For more information about the events, rules, and actions and the out-of-the-box CA Process Automation process that are shipped with CA Service Catalog, see the *CA Service Catalog Integration Guide.*

Rules and Actions Checklist for the Hardware Request Subscription/Item Change Event

You can use the following checklist to cross-reference the rules and actions that are required for the hardware Request Subscription/Item Change Event. The checklist identifies the rules and actions that need to be disabled and enabled for hardware requests. The name differences between CA Service Catalog 12.6 and 12.7 are also noted.

Enable Rule	Enable Action	Disable Action	Complete (Y/N)
When Category is Hardware and Status is filled from Inventory	Launch HWSWFilledFromInv_SDM SRF		

Enable Rule	Enable Action	Disable Action	Complete (Y/N)
When Category is Hardware and Status is filled from Inventory		12.6: Launch FilledFromInventory SRF 12.7: Launch FilledFromInventory SRF for Hardware	
When Category is Hardware and Status is filled from Inventory		12.6: Launch USM_Notify_Fulfillment Workflow 12.7: Launch USM_HW_PC_Fulfillment Workflow	
When Category is Hardware and Status is filled from Inventory		12.6: Launch USM_HW_Fulfillment_USD Workflow 12.7: Launch USM_HW_Fulfillment_USD Workflow for Hardware	
When Category is Hardware and Status Not Filled from Inventory	Launch SLCM_Fulfillment_SRF		
When Category is Hardware and Status Not Filled from Inventory		12.6: Launch USM_Notify_Procurement Workflow 12.7: Launch USM_HW_PC_Procurement Workflow	
When Category is Hardware and Status is Pending Fulfillment	12.6: Launch CheckAvailability SRF 12.7: Launch Check_Availability SRF for Hardware		
When Category is Hardware and Status is Pending Fulfillment		12.6: Launch USM_CheckAvailability Workflow 12.7: Launch USM_CheckAvailability Workflow for Hardware Availability	

Enable Rule	Enable Action	Disable Action	Complete (Y/N)
When Category is Hardware and Status is Received or Canceled	12.6: Launch CheckAvailability SRF 12.7: Launch Hardware CheckAvailability SRF		
When Category is Hardware and Status is Received or Canceled		12.6: Launch USM_CheckAvailability Workflow 12.7: Launch USM_CheckAvailability Workflow for Hardware Cancel	
When Status is Pending Fulfillment	12.6: Launch SLCM_Fulfillment SRF 12.7: Launch SLCM_Fulfillment SRF for Simple Fulfillment		
When Status is Pending Fulfillment		Launch HWSWFilledFromInv_SDM SRF	
When Status is Pending Fulfillment		Launch USM_FulfillmentUSDRequest Workflow	
When Status is Pending Fulfillment		12.6: Launch USM_Notify_Fulfillment Workflow 12.7: Launch USM_Notify_Fulfillment Workflow for Simple Fulfillment	
When Status is Submitted and Approval Process is driven by Workflow	Launch Approval SRF		
When Status is Submitted and Approval Process is driven by Workflow	Launch Policy Driven Approval SRF		
When Status is Submitted and Approval Process is driven by Workflow		Launch USM_ManagerApproval Workflow	

Create Launch Point Change Order Categories

After the request in CA Service Catalog has been fulfilled in the Complex Fulfillment process, a change order in CA SDM is opened in order to complete the request lifecycle and fulfill the request. The change order that was created through CA Process Automation is passed a Change Category through the CA Process Automation Workflow. When the change order is opened, it can launch a change process to fulfill the change.

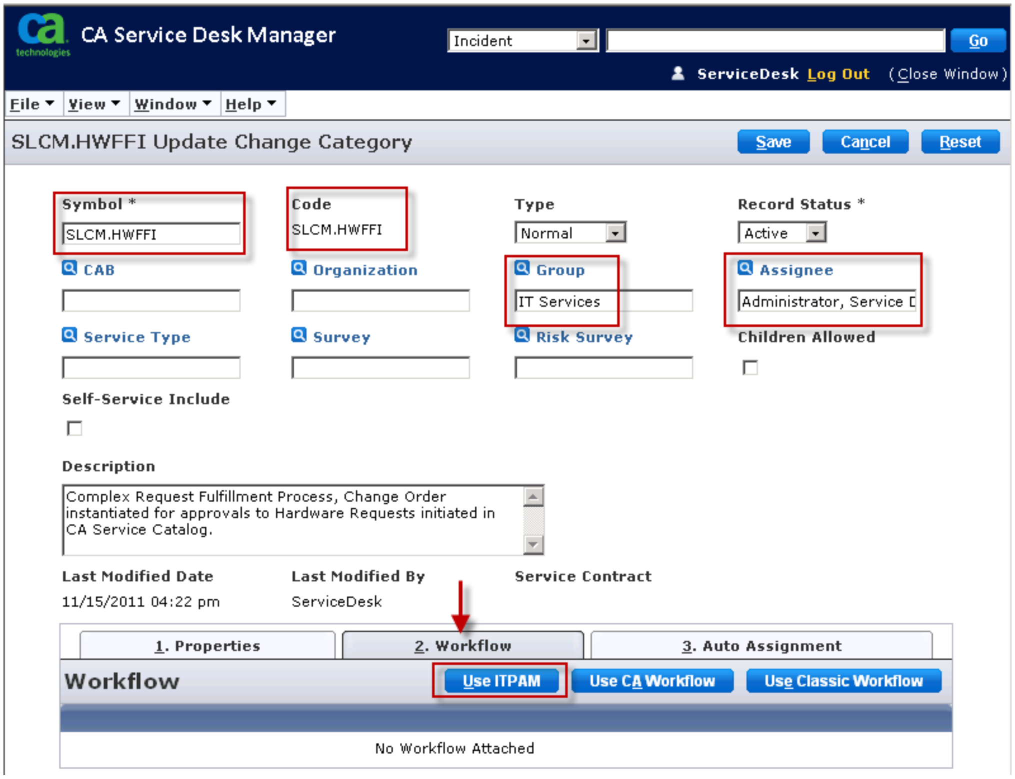
To configure the change order category, first create Change Categories in CA SDM and attach the CA Process Automation SRF for the process you want to launch.

Follow these steps:

1. Log in to CA SDM as an Administrator.
2. From the Administration tab, click Service Desk, Change Orders, Categories. Then click Create New.

3. Create a Category with the attributes shown in the following example.

   Note: You must create the category with the code SLCM.HWFFI%. (This code includes the letter "I", not the number "1".) This code is hard-coded in the SRF that is launched to instantiate the CA Process Automation Workflow. To change the code to another name, follow the instructions in the section Change the Default Category Code that is Passed (see page 75).



SLCM.HWFFI Update Change Category

Symbol *: SLCM.HWFFI

Code: SLCM.HWFFI

Type: Normal

Record Status *: Active

CAB:

Organization:

Group: IT Services

Assignee: Administrator, Service D

Service Type:

Survey:

Risk Survey:

Children Allowed: □

Self-Service Include: □

Description: Complex Request Fulfillment Process, Change Order instantiated for approvals to Hardware Requests initiated in CA Service Catalog.

Last Modified Date: 11/15/2011 04:22 pm

Last Modified By: ServiceDesk

Service Contract:

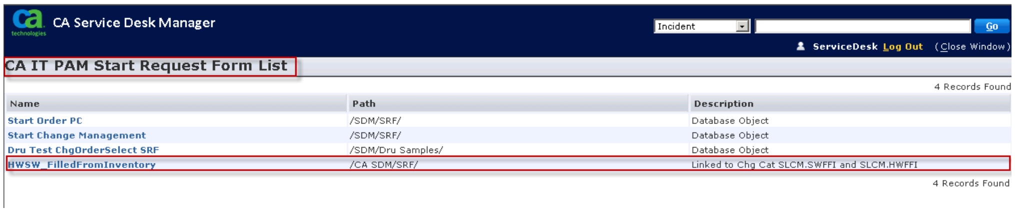
Workflow

No Workflow Attached

4. Click the Workflow tab and then select Use IT PAM to associate the CA Process Automation process (the SRF that invokes the process).

   The CA IT PAM Start Request Form List appears.

5. Click the SRF for HWSW_FilledFromInventory_SDM.



CA IT PAM Start Request Form List

4 Records Found

Name	Path	Description
Start Order PC	/SDM/SRF/	Database Object
Start Change Management	/SDM/SRF/	Database Object
Dru Test ChgOrderSelect SRF	/SDM/Dru Samples/	Database Object
HWSW_FilledFromInventory	/CA SDM/SRF/	Linked to Chg Cat SLCM.SWFFI and SLCM.HWFFI

4 Records Found

Note: If you do not see this SRF appear in the SRF List, follow the instructions in Configure Additional Content from CA Process Automation (see page 64).

Change the Default Category Code that is Passed

During Complex Fulfillment, change the default category code that is passed to the CA SDM change order. After a request status becomes Filled from Inventory, you can open a change order and view the details in CA SDM. The action that you perform from CA Service Catalog is Launch HWSWFilledFromInv_SDM SRF.

Follow these steps:

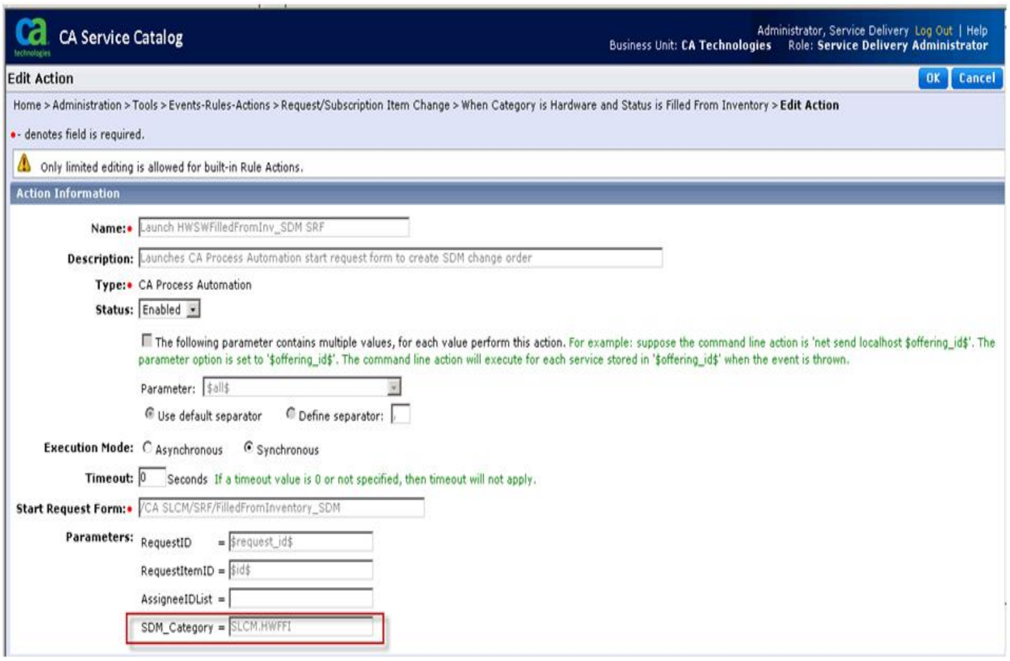
1. Log in to CA Service Catalog as an Administrator.
2. Navigate to Administration, Tools, Events-Rules-Actions.

   The Events-Rules-Actions page appears.
3. Click the Event Type named Request/Subscription Item Change.
4. Double-click the first rule in the list, which is "When Category is Hardware and Status is Filled from Inventory".

   The details for this rule appear. The action that you enabled launches an SRF HWSWFilledFromInv_SDM. You can now view the details for this action.
5. On the right of this action, click Edit to open the detail view.

   In the detail view, you see that the Category SDM_Category is hard-coded as SLCM.HWFFI. A category with this code must exist in CA SDM in order to open the change order with this category.

Note: If a category with this code does not exist and you made the Category field in CA SDM required, the change order is not created. If the Category field is not required in CA SDM, the change order is created but is not passed a Category.



CA Service Catalog
Administrator, Service Delivery Log Out | Help
Business Unit: CA Technologies Role: Service Delivery Administrator
OK
Cancel

Edit Action

Home > Administration > Tools > Events-Rules-Actions > Request/Subscription Item Change > When Category is Hardware and Status is Filled From Inventory > **Edit Action**

•- denotes field is required.

Only limited editing is allowed for built-in Rule Actions.

Action Information

Name:• Launch HWSWFilledFromInv_SDM SRF

Description: Launches CA Process Automation start request form to create SDM change order

Type:• CA Process Automation

Status: Enabled

□ The following parameter contains multiple values, for each value perform this action. For example: suppose the command line action is 'net send localhost $offering_id$'. The parameter option is set to '$offering_id$'. The command line action will execute for each service stored in '$offering_id$' when the event is thrown.

Parameter: all

● Use default separator ○ Define separator: ,

Execution Mode: ○ Asynchronous ● Synchronous

Timeout: 0 Seconds If a timeout value is 0 or not specified, then timeout will not apply.

Start Request Form:• /CA SLCM/SRF/FilledFromInventory_SDM

Parameters:
RequestID = $request_id$
RequestItemID = id
AssigneeIDList =
SDM_Category = SLCM.HWFFI

Only limited editing is allowed for built-in Rule Actions as specified at the top of the Action Information page. To modify the name of the code for the SDM_Category that is passed, you must create an SRF. This SRF is launched by the action When Category is Hardware and Status is Filled from Inventory.

6. Use the breadcrumbs to navigate back to the details for When Category is Hardware and Status is Filled from Inventory.

7. On the right of the "Launch HWSWFilledFromInv_SDM SRF" Action, click Copy.

8. Name the new Action.

   After you create a copy of this Action, the details that are passed to this SRF become editable.

9. Modify the value of the SDM_Category parameter to match the code of the Category that you want to pass to the CA SDM change order.

10. Enable the new action that calls this SRF and disable the previous action.

Testing the Integration

Before you test the solution integration, make sure that you have associated CA Service Catalog services and CA SDM configuration items as documented in the *CA Service Catalog Integration Guide*. Alternatively, if you have CA Asset Portfolio Management integrated (optional), then create sample assets in CA Asset Portfolio Management that the Workflow can leverage.

Test the CA Service Catalog Integration

After you have completed all integration activities, test the CA Service Catalog integration.

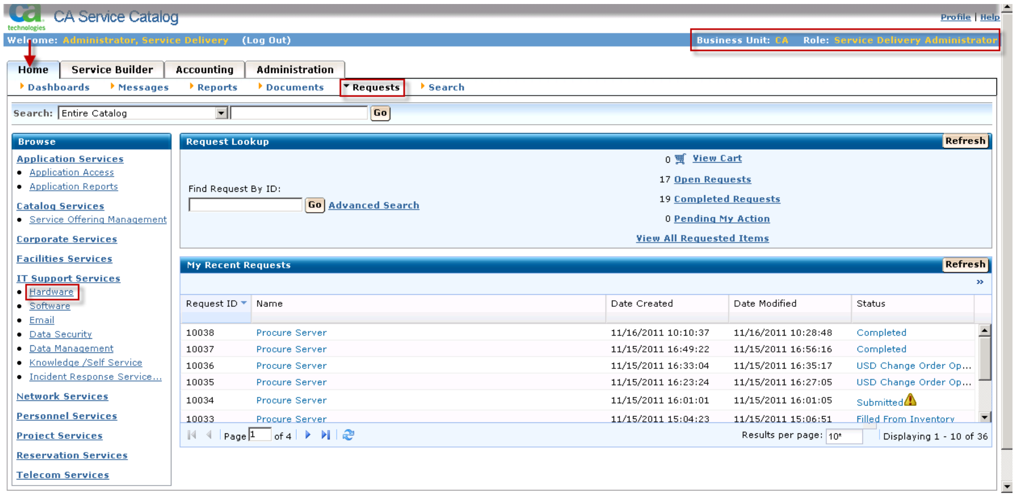
Follow these steps:

1. Log in to CA Service Catalog.

   Note: By default, all tasks are assigned to the spadmin user, so we will log in to CA Service Catalog as spadmin for simplicity.

2. Navigate to Requests and open a new Request under IT Support Services for Hardware.

   Note: This procedure includes Release 12.6 user interface examples.

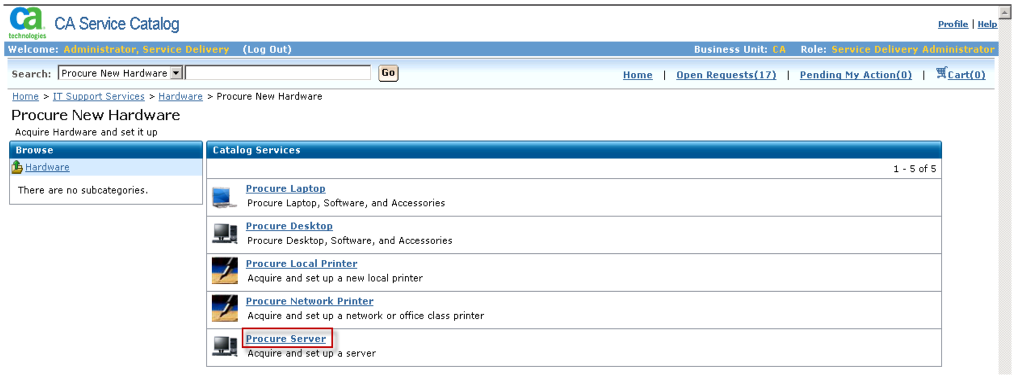


0 View Cart
17 Open Requests
19 Completed Requests
0 Pending My Action
View All Requested Items

Request ID	Name	Date Created	Date Modified	Status
10038	Procure Server	11/16/2011 10:10:37	11/16/2011 10:28:48	Completed
10037	Procure Server	11/15/2011 16:49:22	11/15/2011 16:56:16	Completed
10036	Procure Server	11/15/2011 16:33:04	11/15/2011 16:35:17	USD Change Order Op...
10035	Procure Server	11/15/2011 16:23:24	11/15/2011 16:27:05	USD Change Order Op...
10034	Procure Server	11/15/2011 16:01:01	11/15/2011 16:01:05	Submitted⚠
10033	Procure Server	11/15/2011 15:04:23	11/15/2011 15:06:51	Filled From Inventory

Page 1 of 4 Results per page: 10* Displaying 1 - 10 of 36

In this case, you request a new server to support expansion of the HR Application at Forward Inc.



CA Service Catalog

Profile | Help

Welcome: Administrator, Service Delivery (Log Out) Business Unit: CA Role: Service Delivery Administrator

Search: Procure New Hardware Go

Home | Open Requests(17) | Pending My Action(0) | Cart(0)

Home > IT Support Services > Hardware > Procure New Hardware

Procure New Hardware

Acquire Hardware and set it up

Browse

Hardware

There are no subcategories.

Catalog Services

1 - 5 of 5

Procure Laptop
Procure Laptop, Software, and Accessories

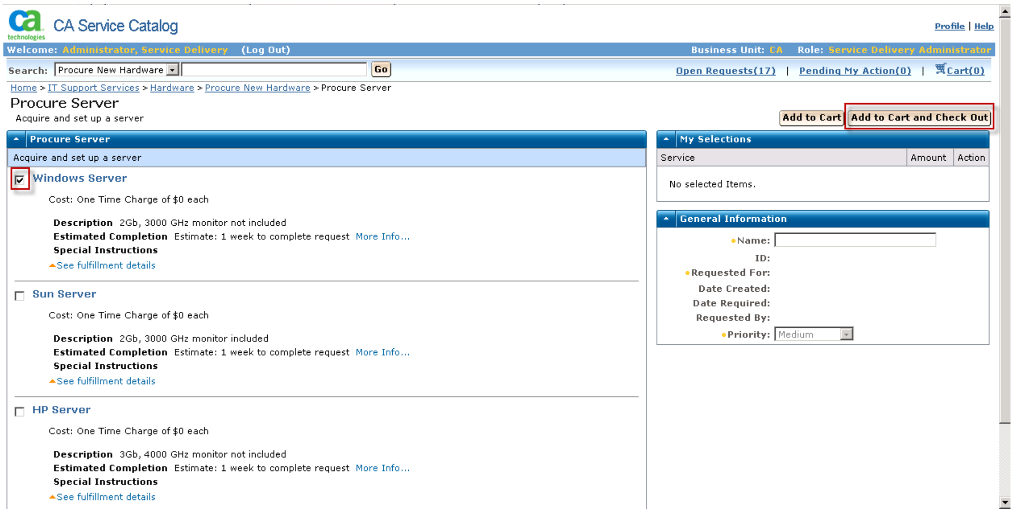
Procure Desktop
Procure Desktop, Software, and Accessories

Procure Local Printer
Acquire and set up a new local printer

Procure Network Printer
Acquire and set up a network or office class printer

Procure Server
Acquire and set up a server

3. Select Server Type of Windows Server and then click Add this to cart and check out.



CA Service Catalog

Profile | Help

Welcome: Administrator, Service Delivery (Log Out) Business Unit: CA Role: Service Delivery Administrator

Search: Procure New Hardware Go

Open Requests(17) | Pending My Action(0) | Cart(0)

Home > IT Support Services > Hardware > Procure New Hardware > Procure Server

Procure Server

Acquire and set up a server

Add to Cart | Add to Cart and Check Out

Procure Server

Acquire and set up a server

☑ Windows Server

Cost: One Time Charge of $0 each

Description 2Gb, 3000 GHz monitor not included
Estimated Completion Estimate: 1 week to complete request More Info...
Special Instructions
See fulfillment details

☐ Sun Server

Cost: One Time Charge of $0 each

Description 2Gb, 3000 GHz monitor included
Estimated Completion Estimate: 1 week to complete request More Info...
Special Instructions
See fulfillment details

☐ HP Server

Cost: One Time Charge of $0 each

Description 3Gb, 4000 GHz monitor not included
Estimated Completion Estimate: 1 week to complete request More Info...
Special Instructions
See fulfillment details

My Selections

Service	Amount	Action
No selected Items.		

General Information

*Name:
ID:
*Requested For:
Date Created:
Date Required:
Requested By:
*Priority: Medium

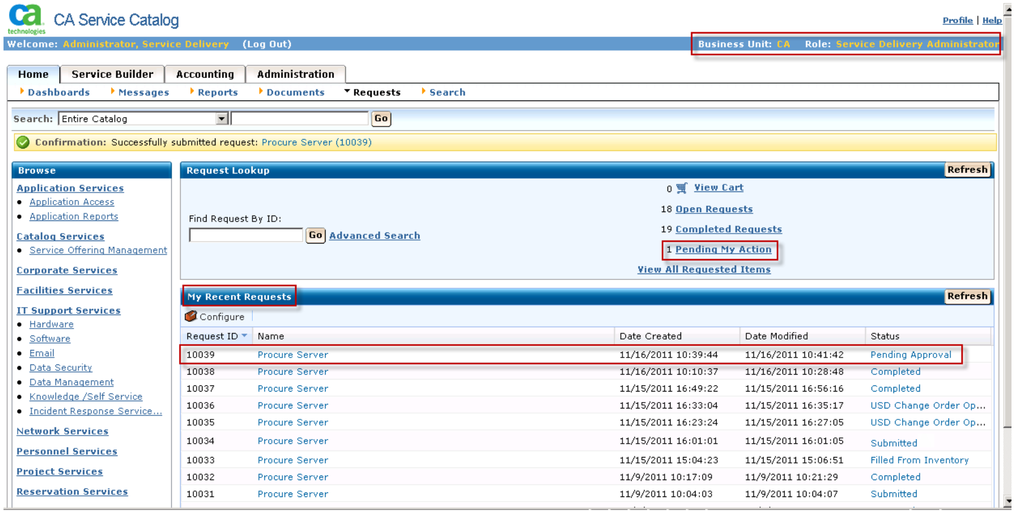
4. On the page after Procure Server, click Save and Submit Cart.

The request for procurement of the server has now been submitted and the Complex Fulfillment workflow has been instantiated.

5. Navigate to My Recent Requests.

Our process has started and is in the status Pending Approval. The first step in the workflow process is management approval. The spadmin user has one Pending Action.

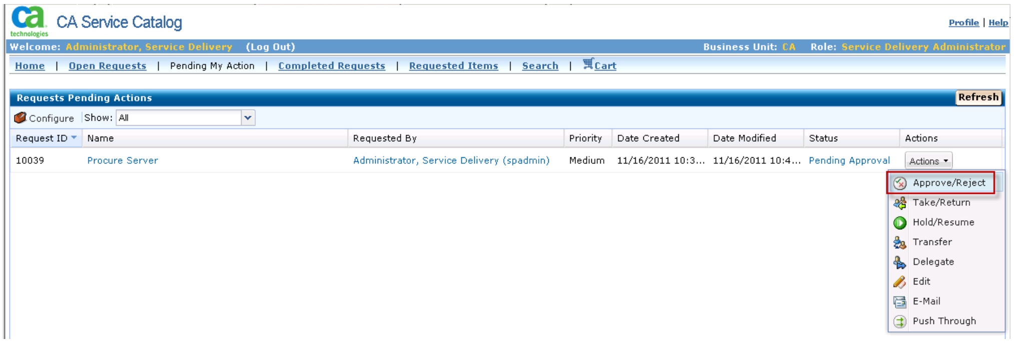
6. Complete the pending action by clicking the Pending My Action link.



Confirmation: Successfully submitted request: Procure Server (10039)

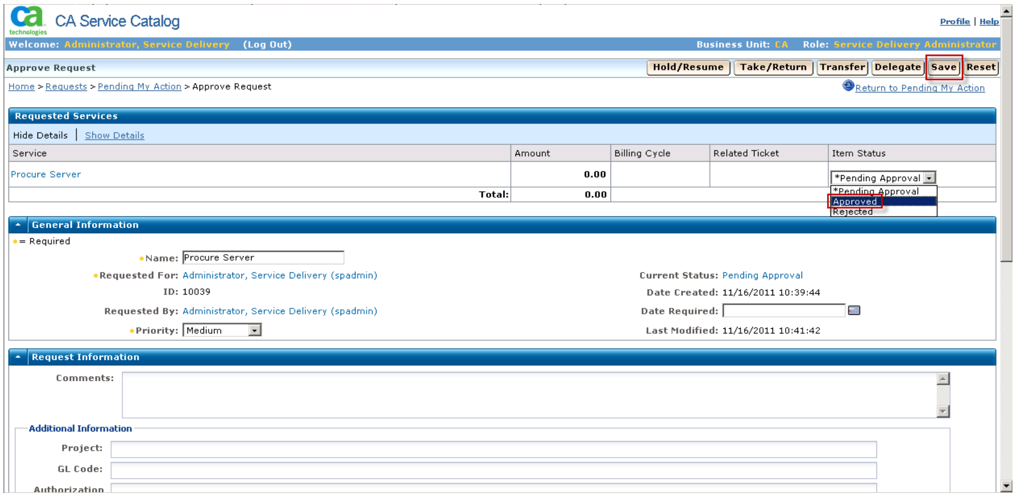
Request ID	Name	Date Created	Date Modified	Status
10039	Procure Server	11/16/2011 10:39:44	11/16/2011 10:41:42	Pending Approval
10038	Procure Server	11/16/2011 10:10:37	11/16/2011 10:28:48	Completed
10037	Procure Server	11/15/2011 16:49:22	11/15/2011 16:56:16	Completed
10036	Procure Server	11/15/2011 16:33:04	11/15/2011 16:35:17	USD Change Order Op...
10035	Procure Server	11/15/2011 16:23:24	11/15/2011 16:27:05	USD Change Order Op...
10034	Procure Server	11/15/2011 16:01:01	11/15/2011 16:01:05	Submitted
10033	Procure Server	11/15/2011 15:04:23	11/15/2011 15:06:51	Filled From Inventory
10032	Procure Server	11/9/2011 10:17:09	11/9/2011 10:21:29	Completed
10031	Procure Server	11/9/2011 10:04:03	11/9/2011 10:04:07	Submitted

7. Select Action, Approve/Reject (as the spadmin user) to approve the provision of this server.


CA Service Catalog
Profile | Help
Welcome: Administrator, Service Delivery (Log Out)
Business Unit: CA Role: Service Delivery Administrator
Home | Open Requests | Pending My Action | Completed Requests | Requested Items | Search | Cart
Requests Pending Actions
Refresh
Configure
Show: All
Actions
Approve/Reject
Take/Return
Hold/Resume
Transfer
Delegate
Edit
E-Mail
Push Through

Request ID	Name	Requested By	Priority	Date Created	Date Modified	Status	Actions
10039	Procure Server	Administrator, Service Delivery (spadmin)	Medium	11/16/2011 10:3...	11/16/2011 10:4...	Pending Approval	Actions

8. On the next page, select Approved and then Save.



Service	Amount	Billing Cycle	Related Ticket	Item Status
Procure Server	0.00			*Pending Approval
Total:	0.00			

● = Required

●Name: Procure Server

●Requested For: Administrator, Service Delivery (spadmin)

ID: 10039

Requested By: Administrator, Service Delivery (spadmin)

●Priority: Medium

Current Status: Pending Approval

Date Created: 11/16/2011 10:39:44

Date Required:

Last Modified: 11/16/2011 10:41:42

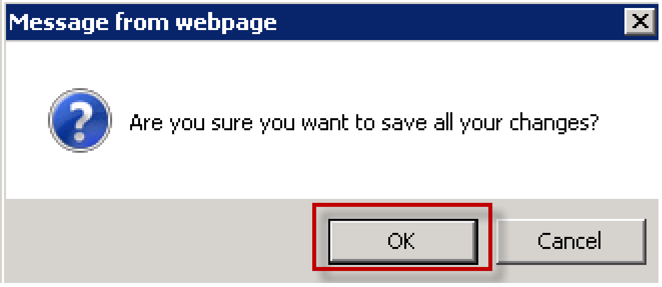
Comments:

Project:

GL Code:

Authorization

9. Click OK to confirm saving your approval of the request.



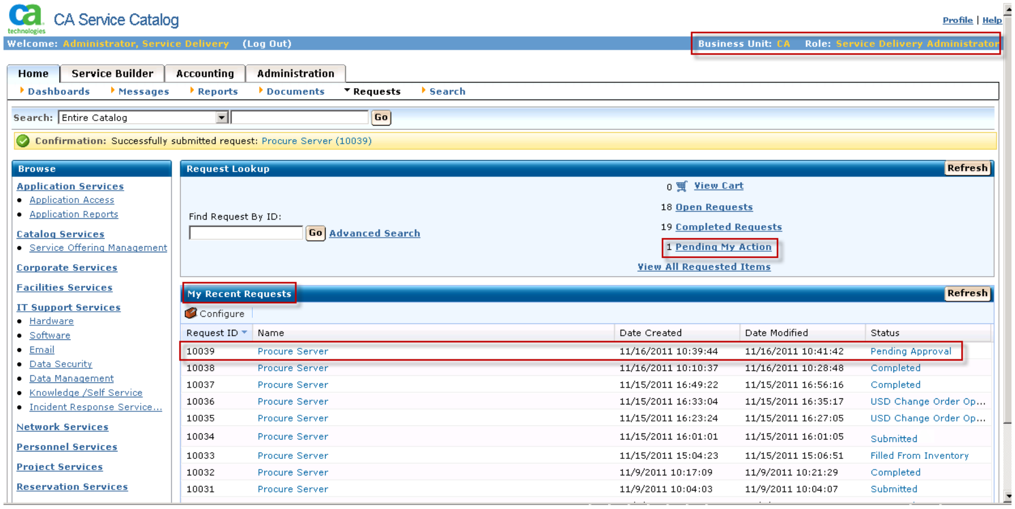
Message from webpage

Are you sure you want to save all your changes?

10. Navigate to My Recent Requests.

    The status of the request should change to Check Availability, and another Pending Action is assigned to the spadmin user.

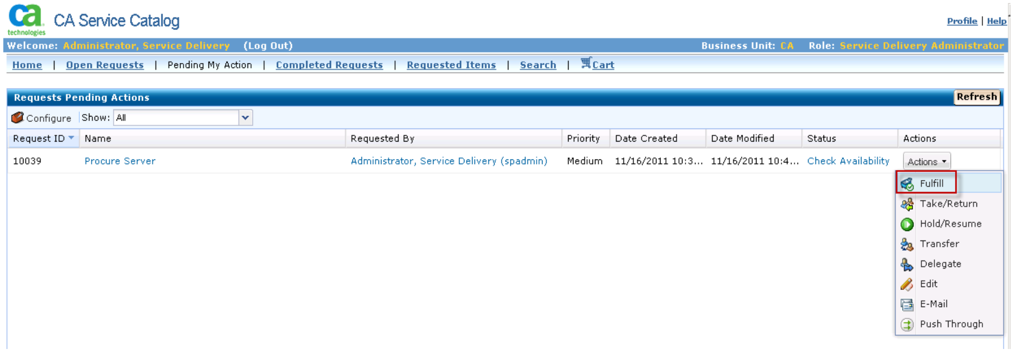
11. Click the Pending My Action link.



Confirmation: Successfully submitted request: Procure Server (10039)

Request ID	Name	Date Created	Date Modified	Status
10039	Procure Server	11/16/2011 10:39:44	11/16/2011 10:41:42	Pending Approval
10038	Procure Server	11/16/2011 10:10:37	11/16/2011 10:28:48	Completed
10037	Procure Server	11/15/2011 16:49:22	11/15/2011 16:56:16	Completed
10036	Procure Server	11/15/2011 16:33:04	11/15/2011 16:35:17	USD Change Order Op...
10035	Procure Server	11/15/2011 16:23:24	11/15/2011 16:27:05	USD Change Order Op...
10034	Procure Server	11/15/2011 16:01:01	11/15/2011 16:01:05	Submitted
10033	Procure Server	11/15/2011 15:04:23	11/15/2011 15:06:51	Filled From Inventory
10032	Procure Server	11/9/2011 10:17:09	11/9/2011 10:21:29	Completed
10031	Procure Server	11/9/2011 10:04:03	11/9/2011 10:04:07	Submitted

12. From the Actions drop-down list, select Actions and then Fulfill.

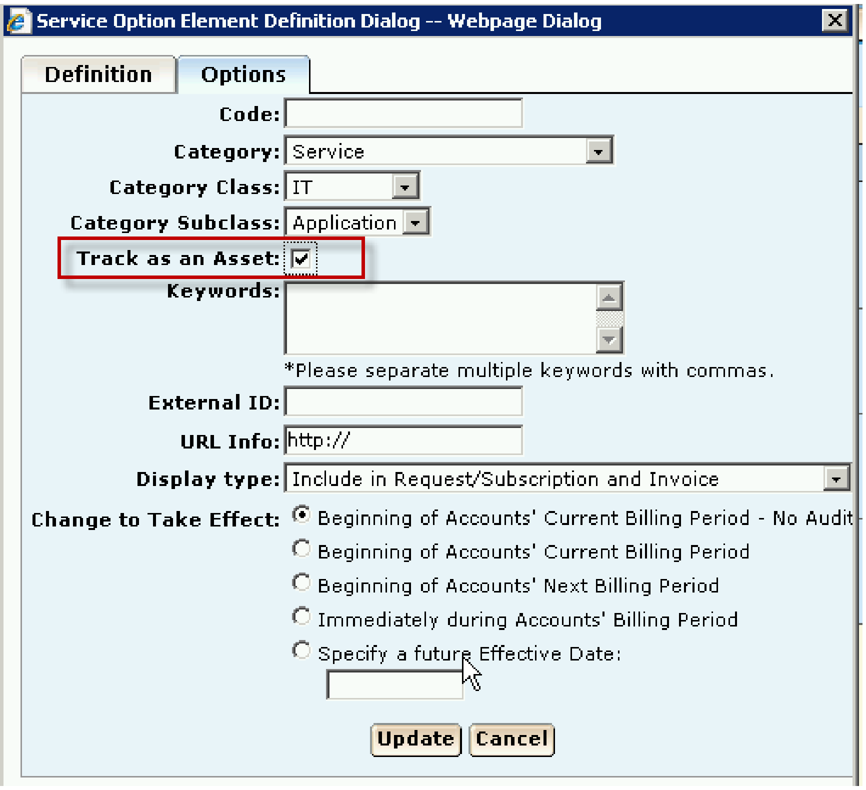


CA Service Catalog
Profile | Help
Welcome: Administrator, Service Delivery (Log Out)
Business Unit: CA Role: Service Delivery Administrator
Home | Open Requests | Pending My Action | Completed Requests | Requested Items | Search | Cart
Requests Pending Actions
Refresh
Configure
Show: All
Fulfill
Take/Return
Hold/Resume
Transfer
Delegate
Edit
E-Mail
Push Through

Request ID	Name	Requested By	Priority	Date Created	Date Modified	Status	Actions
10039	Procure Server	Administrator, Service Delivery (spadmin)	Medium	11/16/2011 10:3...	11/16/2011 10:4...	Check Availability	Actions

The next step in the process is to fulfill the request. Depending on your configuration, you either choose an asset to assign the request and fill from inventory using the gold brick icon, or you fill from inventory without an asset assigned. The gold brick icon indicates that this service option is eligible to have one or more assets assigned, indicating that it was filled from available inventory. If the following conditions are met, you will see the Assigned Assets gold brick icon in the Actions column for a requested service option after the approval step:

- You have integrated CA Service Catalog and CA Asset Portfolio Management.
- Your role in CA Asset Portfolio Management is CA APM Fulfiller.
- The service that you requested in CA Service Catalog has the Track as an Asset check box checked in the Service Option Element Definition Dialog in Service Builder. The following example shows the Track as an Asset check box.

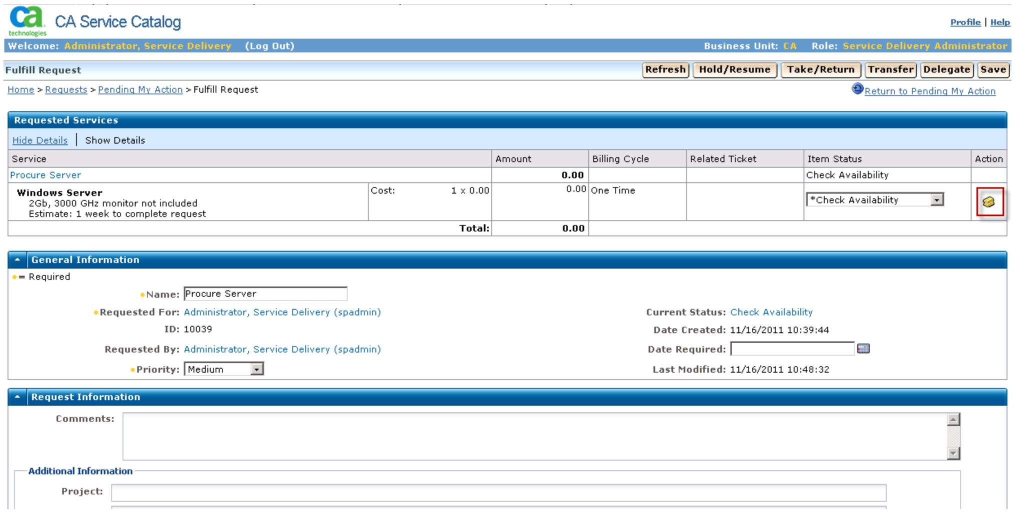


Code:
Category: Service
Category Class: IT
Category Subclass: Application
Track as an Asset: ☑
Keywords:
*Please separate multiple keywords with commas.
External ID:
URL Info: http://
Display type: Include in Request/Subscription and Invoice
Change to Take Effect:
● Beginning of Accounts' Current Billing Period - No Audit
○ Beginning of Accounts' Current Billing Period
○ Beginning of Accounts' Next Billing Period
○ Immediately during Accounts' Billing Period
○ Specify a future Effective Date:

For more information about the integration steps, see the *CA Service Catalog Integration Guide*.

13. If the assigned assets gold brick icon is available, click the icon to search the available inventory.

    If the icon is not available, skip to Step 17 (from CA Service Catalog, Item Status, select Filled from Inventory).


CA Service Catalog
Profile | Help
Welcome: Administrator, Service Delivery (Log Out)
Business Unit: CA Role: Service Delivery Administrator
Fulfill Request
Refresh
Hold/Resume
Take/Return
Transfer
Delegate
Save
Home > Requests > Pending My Action > Fulfill Request
Return to Pending My Action
Requested Services
Hide Details | Show Details

Service		Amount	Billing Cycle	Related Ticket	Item Status	Action
Procure Server		0.00			Check Availability	
Windows Server 2Gb, 3000 GHz monitor not included Estimate: 1 week to complete request	Cost: 1 x 0.00	0.00	One Time		*Check Availability	
	Total:	0.00				

General Information

● = Required

●Name: Procure Server

●Requested For: Administrator, Service Delivery (spadmin)

ID: 10039

Requested By: Administrator, Service Delivery (spadmin)

●Priority: Medium

Current Status: Check Availability

Date Created: 11/16/2011 10:39:44

Date Required:

Last Modified: 11/16/2011 10:48:32

Request Information

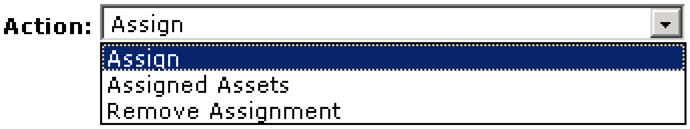
Comments:

Additional Information

Project:

This action opens CA Asset Portfolio Management so that you can select an asset to fulfill this request.

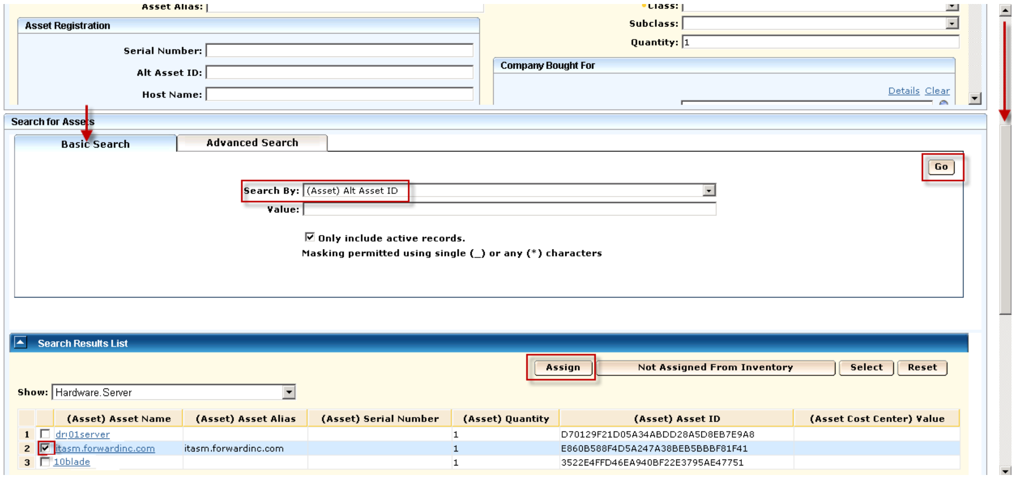
14. In CA Asset Portfolio Management, click Assign in the Action menu.


Action: Assign

The CA Asset Portfolio Management Assign Assets window is displayed. By default, the Assigned Assets action is selected so the list of assets that are already assigned to the requested service option is displayed.

15. Scroll to the Basic Search tab and click Go.

16. Select an Asset to fulfill this hardware request and click Assign.



Asset Alias:

Class:

Subclass:

Quantity: 1

Asset Registration

Serial Number:

Alt Asset ID:

Host Name:

Company Bought For

Details Clear

Search for Assets

Search By: (Asset) Alt Asset ID

Value:

☑ Only include active records.

Masking permitted using single (_) or any (*) characters

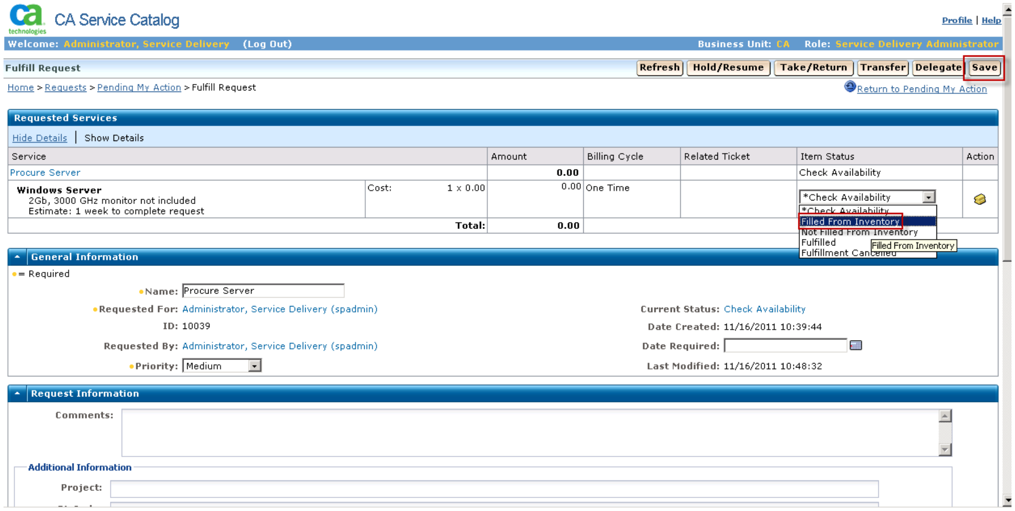
Search Results List

Show: Hardware.Server

		(Asset) Asset Name	(Asset) Asset Alias	(Asset) Serial Number	(Asset) Quantity	(Asset) Asset ID	(Asset Cost Center) Value
1	☐	dri01server			1	D70129F21D05A34ABDD28A5D8EB7E9A8	
2	☑	itasm.forwardinc.com	itasm.forwardinc.com		1	E860B588F4D5A247A38BEB5BBBF81F41	
3	☐	10blade			1	3522E4FFD46EA940BF22E3795AE47751	

The hardware request is ready for configuration by an internal technician in preparation for delivering the unit ready-for-use.

17. Navigate to CA Service Catalog and, under Item Status, select Filled From Inventory and click Save.



CA Service Catalog

Welcome: Administrator, Service Delivery (Log Out) Business Unit: CA Role: Service Delivery Administrator

Fulfill Request

Home > Requests > Pending My Action > Fulfill Request

Return to Pending My Action

Requested Services

Hide Details | Show Details

Service		Amount	Billing Cycle	Related Ticket	Item Status	Action
Procure Server		0.00			Check Availability	
Windows Server 2Gb, 3000 GHz monitor not included Estimate: 1 week to complete request	Cost: 1 x 0.00	0.00	One Time		*Check Availability	
Total:		0.00				

General Information

= Required

Name: Procure Server

Requested For: Administrator, Service Delivery (spadmin)

ID: 10039

Requested By: Administrator, Service Delivery (spadmin)

Priority: Medium

Current Status: Check Availability

Date Created: 11/16/2011 10:39:44

Date Required:

Last Modified: 11/16/2011 10:48:32

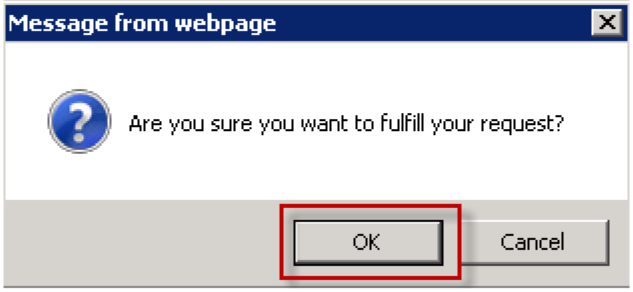
Request Information

Comments:

Additional Information

Project:

18. Click OK.

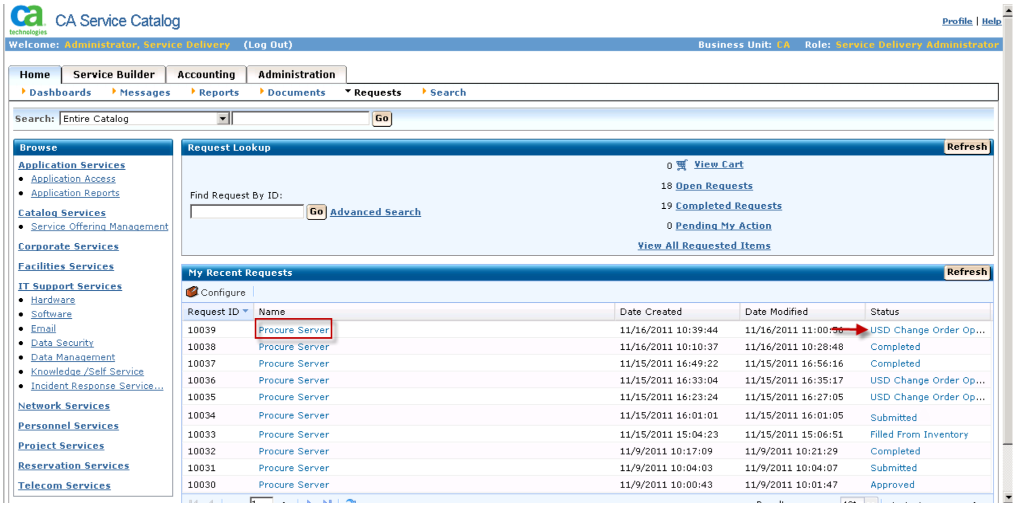


Message from webpage

Are you sure you want to fulfill your request?

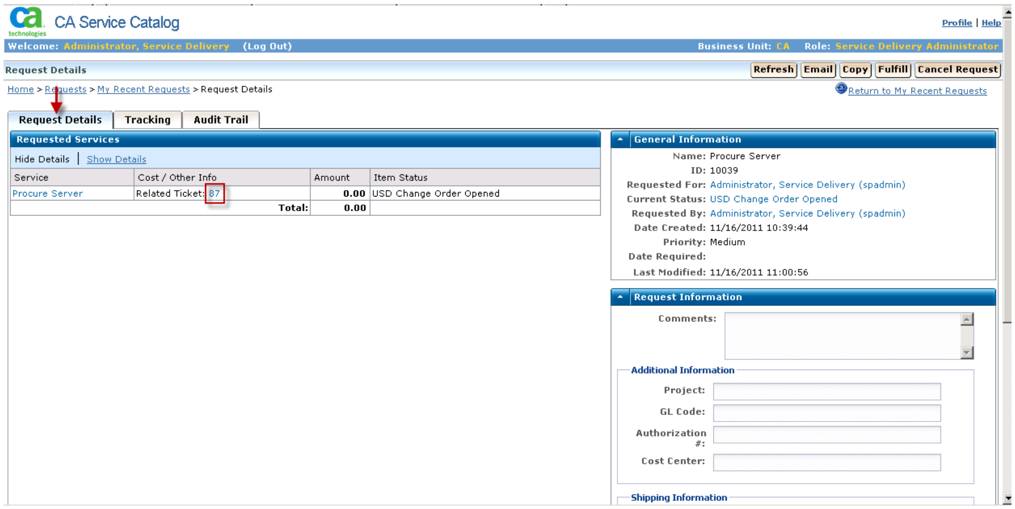
19. Navigate to My Recent Requests.

    The status is now changed to Filled From Inventory and will then change to USD Change Order Opened. After the status changes to USD Change Order Opened, click the hyperlink for Procure Server.



Request ID	Name	Date Created	Date Modified	Status
10039	Procure Server	11/16/2011 10:39:44	11/16/2011 11:00:56	USD Change Order Op...
10038	Procure Server	11/16/2011 10:10:37	11/16/2011 10:28:48	Completed
10037	Procure Server	11/15/2011 16:49:22	11/15/2011 16:56:16	Completed
10036	Procure Server	11/15/2011 16:33:04	11/15/2011 16:35:17	USD Change Order Op...
10035	Procure Server	11/15/2011 16:23:24	11/15/2011 16:27:05	USD Change Order Op...
10034	Procure Server	11/15/2011 16:01:01	11/15/2011 16:01:05	Submitted
10033	Procure Server	11/15/2011 15:04:23	11/15/2011 15:06:51	Filled From Inventory
10032	Procure Server	11/9/2011 10:17:09	11/9/2011 10:21:29	Completed
10031	Procure Server	11/9/2011 10:04:03	11/9/2011 10:04:07	Submitted
10030	Procure Server	11/9/2011 10:00:43	11/9/2011 10:01:47	Approved

20. Click the Request Details tab and click the hyperlink next to Related Ticket, indicating the change order that was opened for this hardware request. In our example, the change order that was opened is 87.



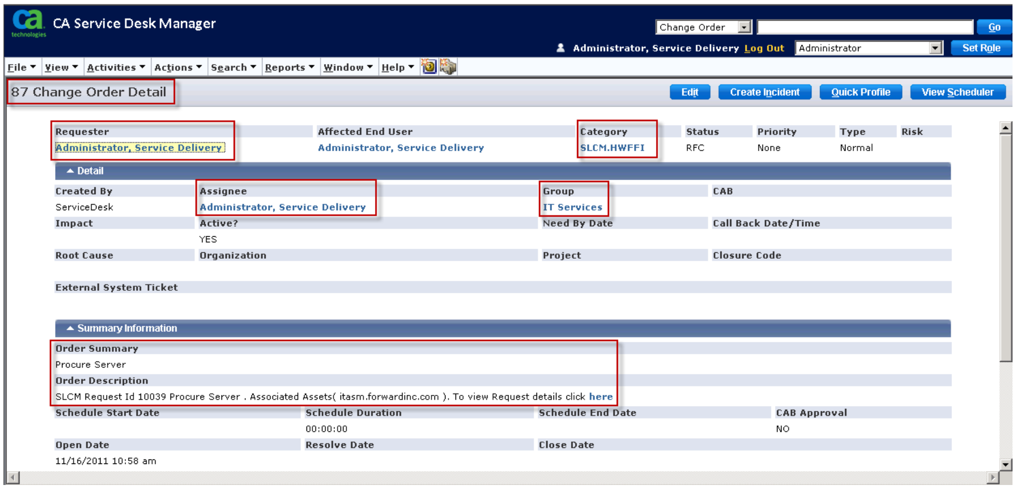
Service	Cost / Other Info	Amount	Item Status
Procure Server	Related Ticket: 87	0.00	USD Change Order Opened
	Total:	0.00	

Name: Procure Server
ID: 10039
Requested For: Administrator, Service Delivery (spadmin)
Current Status: USD Change Order Opened
Requested By: Administrator, Service Delivery (spadmin)
Date Created: 11/16/2011 10:39:44
Priority: Medium
Date Required:
Last Modified: 11/16/2011 11:00:56

Comments:

Project:
GL Code:
Authorization #:
Cost Center:

Clicking the hyperlink prompts you for a login to CA SDM. After you log in (in this case, as spadmin), you are brought into the context of the change order 87 that was created. All of the details of the request that was instantiated by CA Service Catalog have been brought over into CA SDM, including a link back to the request in CA Service Catalog.



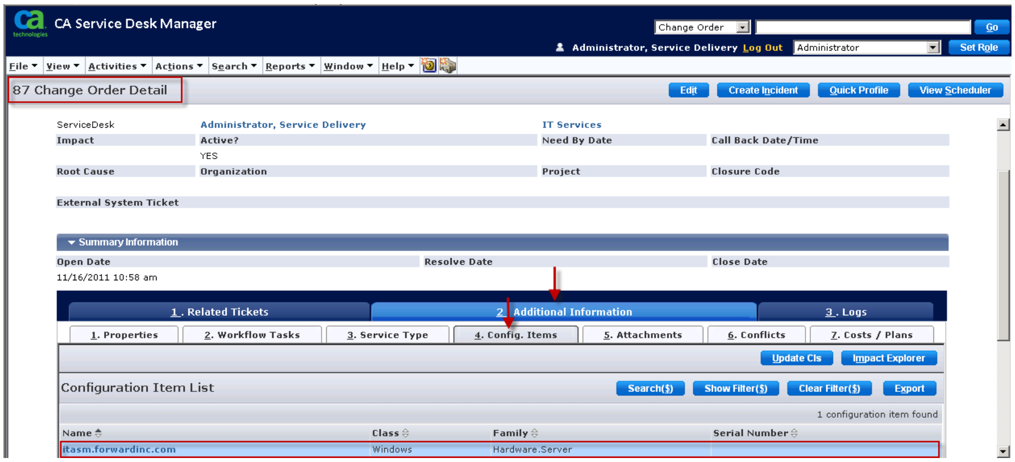
Requester	Affected End User	Category	Status	Priority	Type	Risk
Administrator, Service Delivery	Administrator, Service Delivery	SLCM.HWFFI	RFC	None	Normal	

Created By	Assignee	Group	CAB
ServiceDesk	Administrator, Service Delivery	IT Services	
Impact	Active?	Need By Date	Call Back Date/Time
	YES		
Root Cause	Organization	Project	Closure Code
External System Ticket			

Order Summary
Procure Server
Order Description
SLCM Request Id 10039 Procure Server . Associated Assets(itasm.forwardinc.com). To view Request details click here

Schedule Start Date	Schedule Duration	Schedule End Date	CAB Approval
	00:00:00		NO
Open Date	Resolve Date	Close Date	
11/16/2011 10:58 am			

Note: If you are integrating CA SDM, CA Service Catalog, and CA Asset Portfolio Management, the associated assets become configuration items on the related change order as shown in the following example. For more information about the integration steps, see the *CA Service Catalog Integration Guide*.



87 Change Order Detail

ServiceDesk: Administrator, Service Delivery — IT Services

Impact — Active? YES — Need By Date — Call Back Date/Time

Root Cause — Organization — Project — Closure Code

External System Ticket

Open Date: 11/16/2011 10:58 am — Resolve Date — Close Date

Configuration Item List

1 configuration item found

Name	Class	Family	Serial Number
itasm.forwardinc.com	Windows	Hardware.Server	

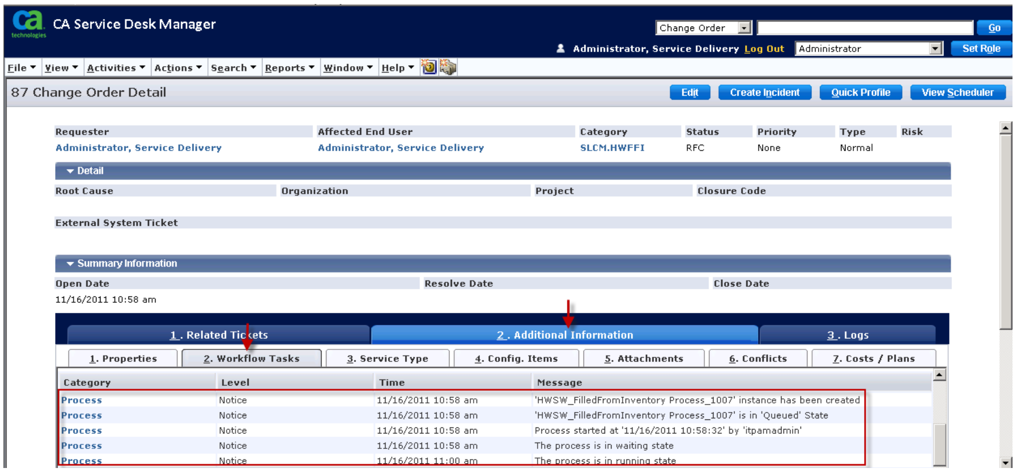
Note: If you do not have CA Asset Portfolio Management integrated with CA Service Catalog, the gold brick icon is not available. Skip to step 21 (click the Workflow Tasks tab).

We now have another approval process that was initiated by the SLCM.HWFFI category.

21. Click the Workflow Tasks tab.

    By default, only tasks of the Process category appear on the CA SDM Workflow Tasks tab.

    Note: If you want to enhance this out-of-the-box process definition to include business-like human interaction tasks, see Enhancing the CA Service Catalog Content (see page 91).



87 Change Order Detail

Requester	Affected End User	Category	Status	Priority	Type	Risk
Administrator, Service Delivery	Administrator, Service Delivery	SLCM.HWFFI	RFC	None	Normal	

Root Cause — Organization — Project — Closure Code

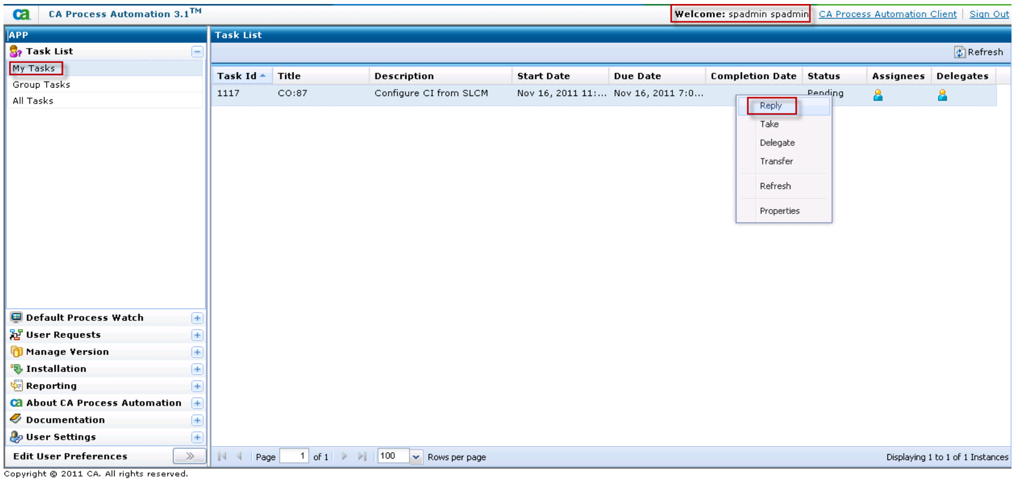
External System Ticket

Open Date: 11/16/2011 10:58 am — Resolve Date — Close Date

Category	Level	Time	Message
Process	Notice	11/16/2011 10:58 am	'HWSW_FilledFromInventory Process_1007' instance has been created
Process	Notice	11/16/2011 10:58 am	'HWSW_FilledFromInventory Process_1007' is in 'Queued' State
Process	Notice	11/16/2011 10:58 am	Process started at '11/16/2011 10:58:32' by 'itpamadmin'
Process	Notice	11/16/2011 10:58 am	The process is in waiting state
Process	Notice	11/16/2011 11:00 am	The process is in running state

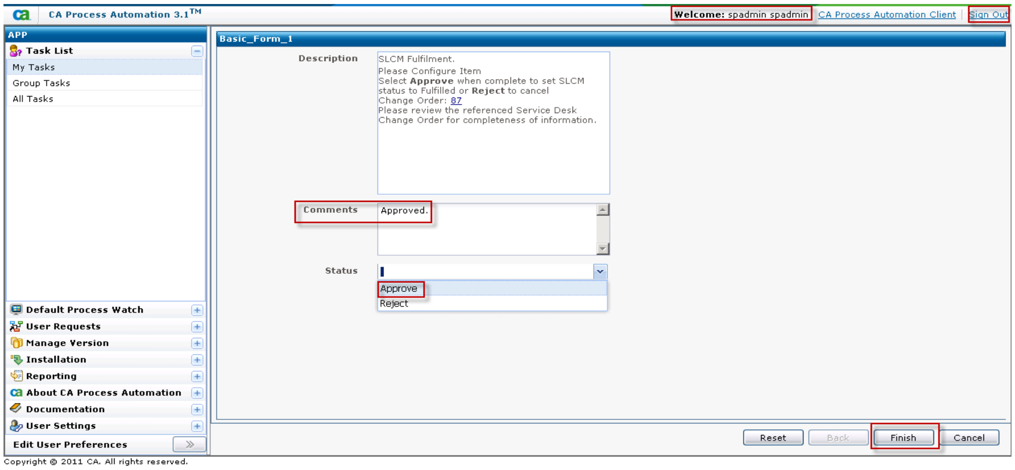
The first step in this process is to approve the change order.

22. Log in to CA Process Automation as spadmin. Right-click the task for CO:87 and click Reply to reply to this task.



Task Id	Title	Description	Start Date	Due Date	Completion Date	Status	Assignees	Delegates
1117	CO:87	Configure CI from SLCM	Nov 16, 2011 11:...	Nov 16, 2011 7:0...		Pending	👤	👤

23. Enter approval comments, select Approve, click Finish, and log out of CA Process Automation.



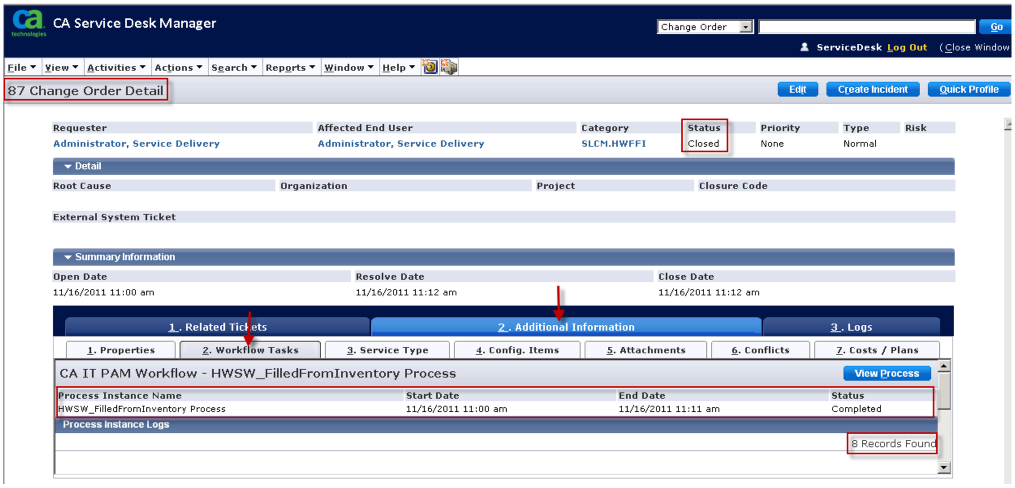
Description: SLCM Fulfilment.
Please Configure Item
Select **Approve** when complete to set SLCM status to Fulfilled or **Reject** to cancel
Change Order: 87
Please review the referenced Service Desk Change Order for completeness of information.

Comments: Approved.

Status: Approve / Reject

24. Log in to the change order.

    You see that the workflow is completed and the status of the change order is now closed. The hardware request has now been fulfilled, and additional steps can be added depending on your business process.



87 Change Order Detail

Requester	Affected End User	Category	Status	Priority	Type	Risk
Administrator, Service Delivery	Administrator, Service Delivery	SLCM.HWFFI	Closed	None	Normal	

Root Cause

Organization

Project

Closure Code

External System Ticket

Open Date	Resolve Date	Close Date
11/16/2011 11:00 am	11/16/2011 11:12 am	11/16/2011 11:12 am

CA IT PAM Workflow - HWSW_FilledFromInventory Process

Process Instance Name	Start Date	End Date	Status
HWSW_FilledFromInventory Process	11/16/2011 11:00 am	11/16/2011 11:11 am	Completed

8 Records Found

Troubleshooting Configuration Issues

If you encounter any of the following content configuration issues, follow the instructions to resolve the issue.

CA Process Automation Content Does not Load

Symptom:

When the CA Process Automation content from CA Service Catalog is loading, the following error message appears:

```
Error occurred while trying to load. Please check your configuration and server availability.
```

Solution:

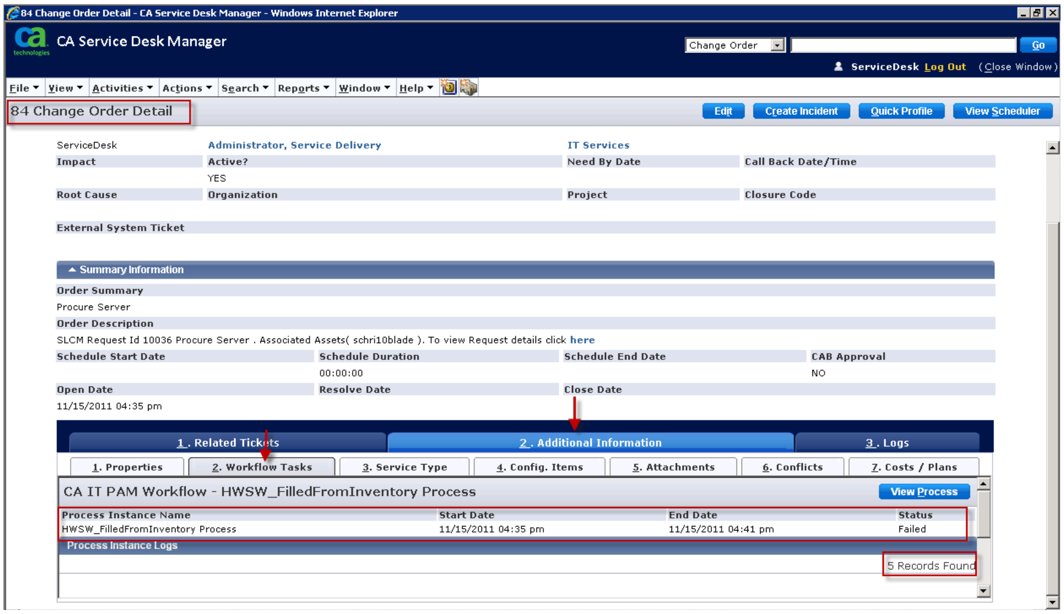
Disable the use of the CA EEM Certificate by specifying No for the option Use CA EEM for Authentication. Clear the entry for EEM Certificate Name.

Note: After the load is successful, you can switch the setting for Use CA EEM Certificate for Authentication back to Yes.

HWSW_FilledFromInventory Process Fails

Symptom:

The SLCM_HWFFI Category, HWSW_FilledFromInventory process fails when it reaches five records after being launched from CA SDM.



84 Change Order Detail

ServiceDesk Administrator, Service Delivery IT Services

Impact

Active? YES

Need By Date

Call Back Date/Time

Root Cause

Organization

Project

Closure Code

External System Ticket

Summary Information

Order Summary
Procure Server

Order Description
SLCM Request Id 10036 Procure Server . Associated Assets(schri10blade). To view Request details click here

Schedule Start Date

Schedule Duration 00:00:00

Schedule End Date

CAB Approval NO

Open Date 11/15/2011 04:35 pm

Resolve Date

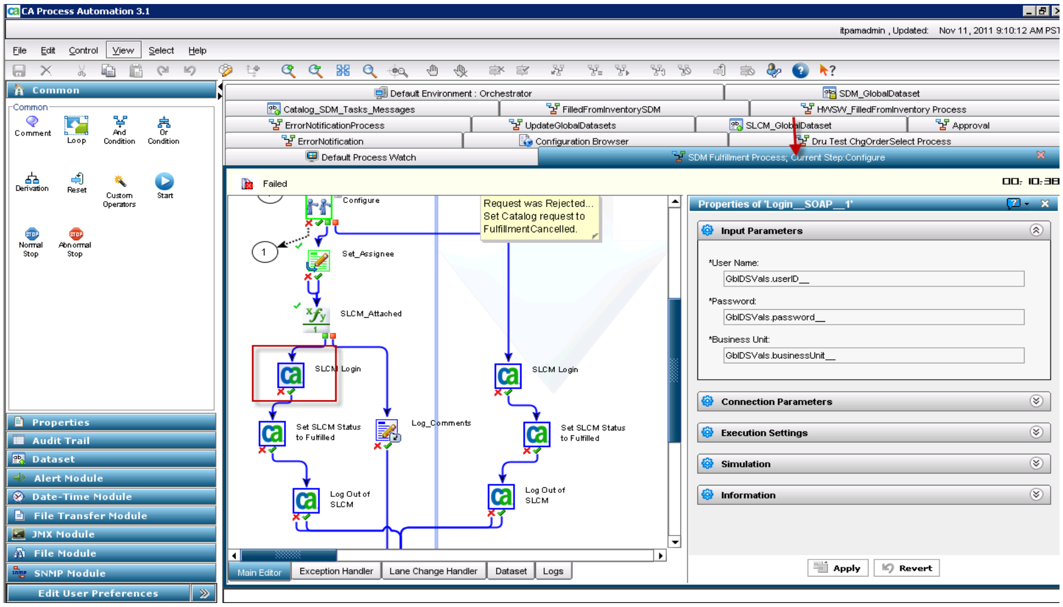
Close Date

CA IT PAM Workflow - HWSW_FilledFromInventory Process

Process Instance Name	Start Date	End Date	Status
HWSW_FilledFromInventory Process	11/15/2011 04:35 pm	11/15/2011 04:41 pm	Failed

5 Records Found

You can determine the step that failed by viewing the process instance logs in CA Process Automation. The following example shows that the step that is failing is at node SLCMLogin.



Request was Rejected... Set Catalog request to FulfillmentCancelled.

*User Name: GblDSVals.userID__

*Password: GblDSVals.password__

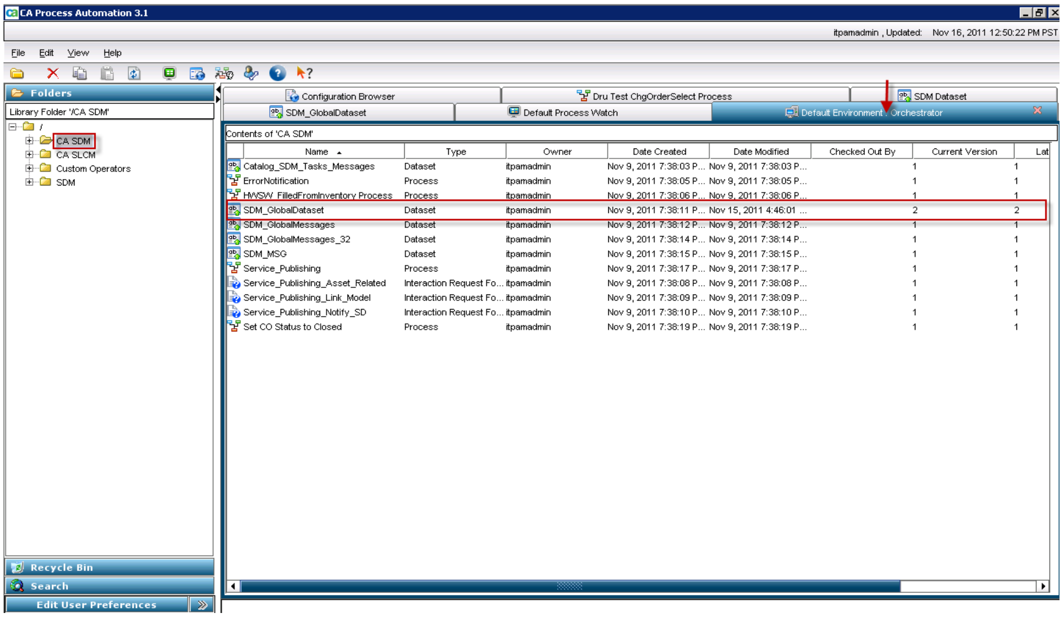
*Business Unit: GblDSVals.businessUnit__

The failure at this node produces the following error message in the CA Process Automation process instance dataset:

```
username\password are invalid.
```

Solution:

In CA Process Automation, verify that you have updated the SDM_GlobalDataset with the correct password for the spadmin user. The dataset is located in the CA SDM directory.



Contents of 'CA SDM'

Name	Type	Owner	Date Created	Date Modified	Checked Out By	Current Version	Lat
Catalog_SDM_Tasks_Messages	Dataset	itpamadmin	Nov 9, 2011 7:38:03 P...	Nov 9, 2011 7:38:03 P...		1	1
ErrorNotification	Process	itpamadmin	Nov 9, 2011 7:38:05 P...	Nov 9, 2011 7:38:05 P...		1	1
HWSW_FilledFromInventory Process	Process	itpamadmin	Nov 9, 2011 7:38:06 P...	Nov 9, 2011 7:38:06 P...		1	1
SDM_GlobalDataset	Dataset	itpamadmin	Nov 9, 2011 7:38:11 P...	Nov 15, 2011 4:46:01 ...		2	2
SDM_GlobalMessages	Dataset	itpamadmin	Nov 9, 2011 7:38:12 P...	Nov 9, 2011 7:38:12 P...		1	1
SDM_GlobalMessages_32	Dataset	itpamadmin	Nov 9, 2011 7:38:14 P...	Nov 9, 2011 7:38:14 P...		1	1
SDM_MSG	Dataset	itpamadmin	Nov 9, 2011 7:38:15 P...	Nov 9, 2011 7:38:15 P...		1	1
Service_Publishing	Process	itpamadmin	Nov 9, 2011 7:38:17 P...	Nov 9, 2011 7:38:17 P...		1	1
Service_Publishing_Asset_Related	Interaction Request Fo...	itpamadmin	Nov 9, 2011 7:38:08 P...	Nov 9, 2011 7:38:08 P...		1	1
Service_Publishing_Link_Model	Interaction Request Fo...	itpamadmin	Nov 9, 2011 7:38:09 P...	Nov 9, 2011 7:38:09 P...		1	1
Service_Publishing_Notify_SD	Interaction Request Fo...	itpamadmin	Nov 9, 2011 7:38:10 P...	Nov 9, 2011 7:38:10 P...		1	1
Set CO Status to Closed	Process	itpamadmin	Nov 9, 2011 7:38:19 P...	Nov 9, 2011 7:38:19 P...		1	1

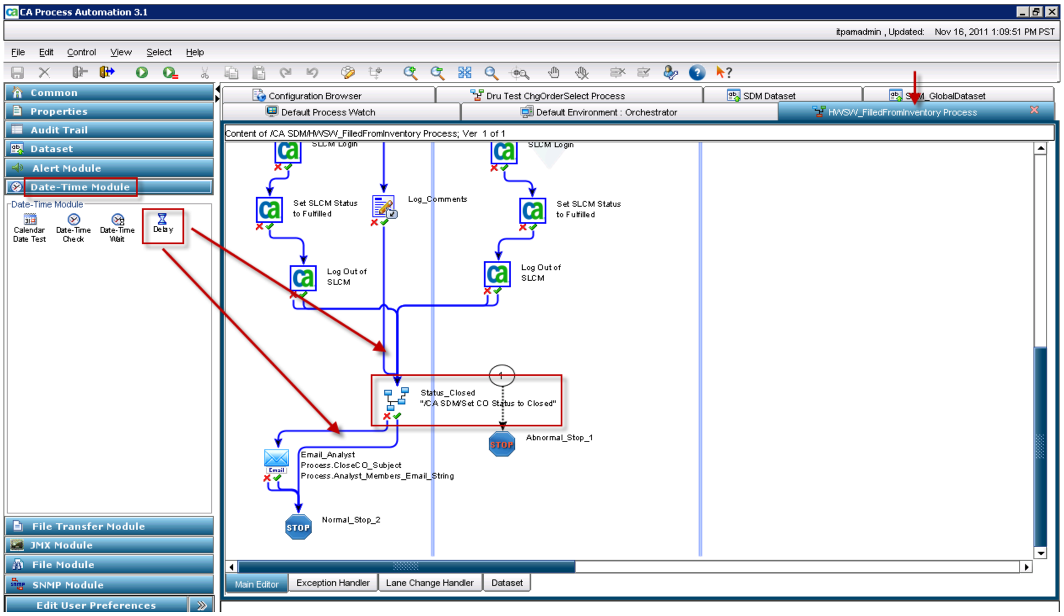
Change Order Remains in RFC Status

Symptom:

A change order that is opened from CA SDM with the attached HWSW_FilledFromInventory workflow remains in RFC status even after the workflow shows that the change order is complete. The change order status does not change to Closed.

Solution:

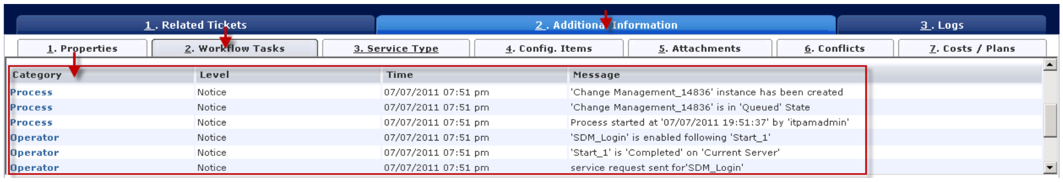
Add a delay before and after the node Status Closed in the process definition in CA Process Automation.



Enhancing the CA Service Catalog Content

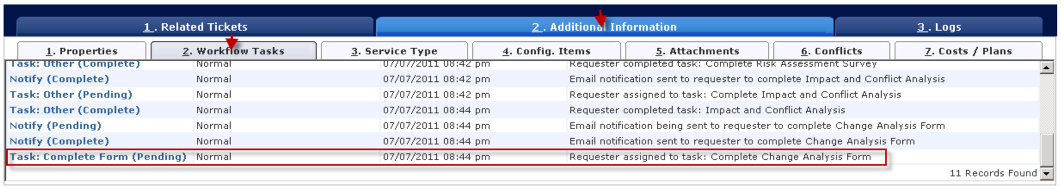
Adding Business-Like Entries for a CA SDM Change Order

You can add business-like entries in the Workflow Tasks tab for a CA SDM change order. By default, the category of tasks that are written to the CA SDM Change Order Workflow Tasks tab are of type process or operator, which are very low level.



Category	Level	Time	Message
Process	Notice	07/07/2011 07:51 pm	'Change Management_14836' instance has been created
Process	Notice	07/07/2011 07:51 pm	'Change Management_14836' is in 'Queued' State
Process	Notice	07/07/2011 07:51 pm	Process started at '07/07/2011 19:51:37' by 'itpamadmin'
Operator	Notice	07/07/2011 07:51 pm	'SDM_Login' is enabled following 'Start_1'
Operator	Notice	07/07/2011 07:51 pm	'Start_1' is 'Completed' on 'Current Server'
Operator	Notice	07/07/2011 07:51 pm	service request sent for'SDM_Login'

You can modify the types of messages that are brought from CA Service Catalog into this tab. In this way, human interaction tasks, notifications, and so on, can be displayed as pending tasks, as shown in the following example:



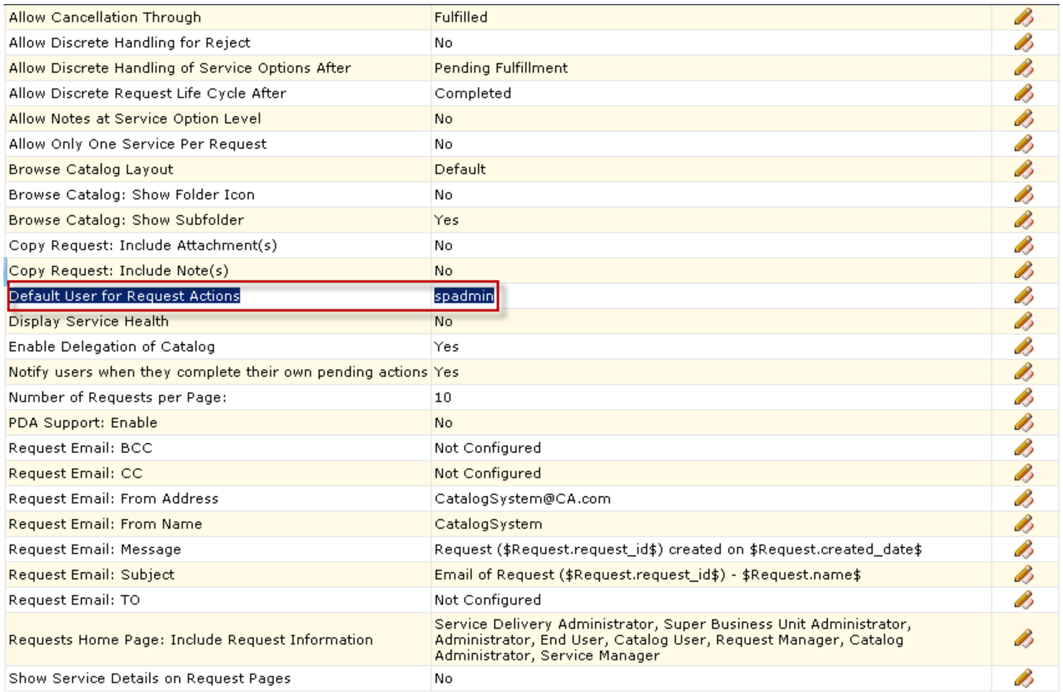
Task: Other (Complete)	Normal	07/07/2011 08:42 pm	Requester completed task: Complete Risk Assessment Survey
Notify (Complete)	Normal	07/07/2011 08:42 pm	Email notification sent to requester to complete Impact and Conflict Analysis
Task: Other (Pending)	Normal	07/07/2011 08:42 pm	Requester assigned to task: Complete Impact and Conflict Analysis
Task: Other (Complete)	Normal	07/07/2011 08:44 pm	Requester completed task: Impact and Conflict Analysis
Notify (Pending)	Normal	07/07/2011 08:44 pm	Email notification being sent to requester to complete Change Analysis Form
Notify (Complete)	Normal	07/07/2011 08:44 pm	Email notification sent to requester to complete Change Analysis Form
Task: Complete Form (Pending)	Normal	07/07/2011 08:44 pm	Requester assigned to task: Complete Change Analysis Form

11 Records Found

For more information about how to configure this enhancement, see the *CA Service Desk Manager Integration Best Practices Green Book*, Volume 2.

Changing the Approver of CA Service Catalog Requests

All out-of-the-box CA Service Catalog content is configured to use the spadmin user as the default approver for CA Service Catalog requests. This default is set this way because the Default User for Request Action is set to spadmin.



Allow Cancellation Through	Fulfilled	✎
Allow Discrete Handling for Reject	No	✎
Allow Discrete Handling of Service Options After	Pending Fulfillment	✎
Allow Discrete Request Life Cycle After	Completed	✎
Allow Notes at Service Option Level	No	✎
Allow Only One Service Per Request	No	✎
Browse Catalog Layout	Default	✎
Browse Catalog: Show Folder Icon	No	✎
Browse Catalog: Show Subfolder	Yes	✎
Copy Request: Include Attachment(s)	No	✎
Copy Request: Include Note(s)	No	✎
Default User for Request Actions	spadmin	✎
Display Service Health	No	✎
Enable Delegation of Catalog	Yes	✎
Notify users when they complete their own pending actions	Yes	✎
Number of Requests per Page:	10	✎
PDA Support: Enable	No	✎
Request Email: BCC	Not Configured	✎
Request Email: CC	Not Configured	✎
Request Email: From Address	CatalogSystem@CA.com	✎
Request Email: From Name	CatalogSystem	✎
Request Email: Message	Request ($Request.request_id$) created on $Request.created_date$	✎
Request Email: Subject	Email of Request ($Request.request_id$) - $Request.name$	✎
Request Email: TO	Not Configured	✎
Requests Home Page: Include Request Information	Service Delivery Administrator, Super Business Unit Administrator, Administrator, End User, Catalog User, Request Manager, Catalog Administrator, Service Manager	✎
Show Service Details on Request Pages	No	✎

For information about changing the approver, see the CA Service Catalog documentation.

Common Multi-Tenancy – Integrated Tenancy Model

Releases 12.5 and 12.6 of CA Service Catalog and CA SDM are capable of sharing a common tenant model. This model offers the ability to reduce the administrative overhead of managing tenants in two systems. With common multi-tenancy, you can use CA SDM to administer and manage tenants for both CA SDM and CA Service Catalog.

Configuring Common Multi-Tenancy

In common tenant administration (also known as multi-tenant administration), you create and maintain a single tenant structure for CA Service Catalog and CA SDM.

Using common tenant administration in CA Service Catalog, you can create, copy, cut, and paste tenants in CA SDM only. Similarly, you can edit common (shared) attributes of tenants in CA SDM only. CA Service Catalog "inherits" the tenants, their structure, and their common attributes from CA SDM. These features appear as read-only in CA Service Catalog. In CA Service Catalog, you can still edit CA Service Catalog-specific attributes. If the CA SDM release is earlier than r12.5, then common tenant administration is not applicable. You must use stand-alone tenant administration in CA Service Catalog.

You must enable multi-tenancy in CA SDM before enabling it in CA Service Catalog because CA Service Catalog requires a tenant of type Service Provider in CA SDM as a prerequisite. This requirement must be met before you can complete the steps in this process and the related procedures.

If your organization has CA SDM r12.5 or r12.6 installed with CA Service Catalog r12.6, you can create and maintain tenants using common tenant administration. Instructions for configuring common multi-tenancy in CA Service Catalog are documented in the *CA Service Catalog Administration Guide*.

Note: In the *CA Service Catalog Administration Guide,* “How to Configure Common Tenant Administration” section, the step that states “Verify that the multi-tenancy option is on” is incorrect. In CA SDM, set the multi-tenancy option to On Warn initially. After you have merged the tenants and set common multi-tenancy to Yes in CA Service Catalog, set the multi-tenancy in CA SDM to On.

Integration Multi-Tenancy Issues

When you integrate CA Service Catalog with CA SDM, you need to be aware of some issues that are related to multi-tenancy. These issues include the following items:

- Cannot use CA Service Catalog to create change orders in CA SDM when multi-tenancy is enabled.
- Moving CA Service Catalog tenants causes problems with request management, user management, and other functions.
- The predefined report Requests_Change Orders_CI Association does not display some column values.

For more information about these and other known issues, see the *CA Service Catalog Release Notes* for Release 12.6.

Extending the Integration to Include CA Asset Portfolio Management

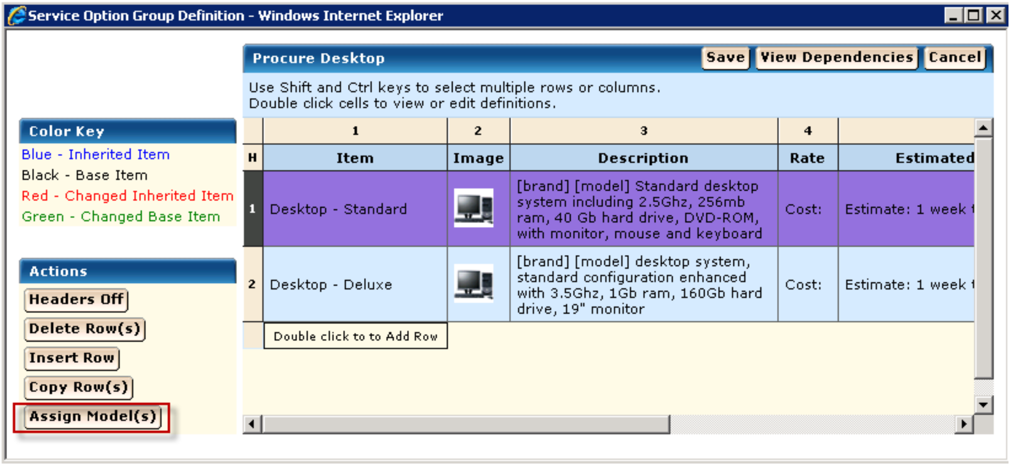
Asset managers can associate CA Asset Portfolio Management assets with items that are requested from the catalog during request fulfillment. This association is shown in the Testing the Integration (see page 77) section of this chapter. The integration with CA Asset Portfolio Management provides the following capabilities:

- Align CA Service Catalog services to CA Asset Portfolio Management models for process automation for the asset allocation process.
- Manage assets as services in CA Service Catalog.
- Define asset-specific service offerings for publishing in CA Service Catalog.
- Align managed models to services and leverage CA Process Automation to automate the allocation of assets.
- Perform the availability check and assignment process for the fulfillment of asset requests.
- Enhance the integration with CA SDM by automatically adding the associated assets on the service request as configuration items on the related CA SDM change order.

Assign a CA Asset Portfolio Management Model to a CA Service Catalog Service

Follow these steps:

1. Log in to CA Service Catalog as an administrator and select the Service Builder tab.
2. Click the Service Option Groups link and view the definition of one of the groups in the list.
3. Highlight the row of the item that you want to link and click Assign Model(s).



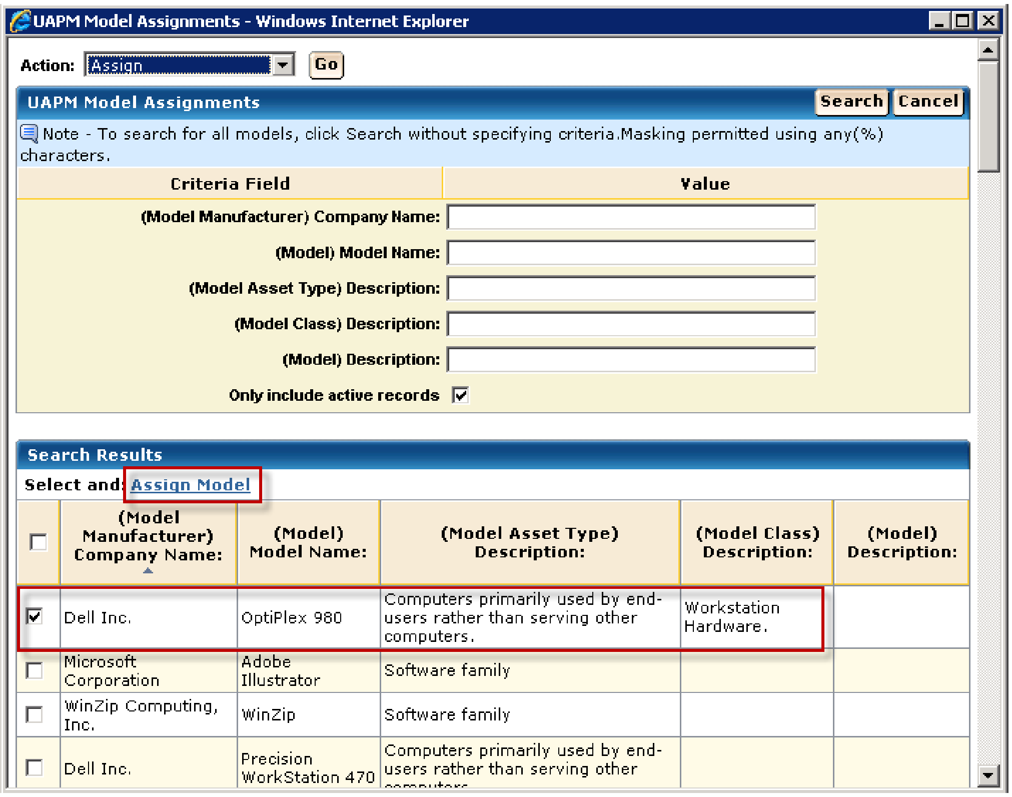
Use Shift and Ctrl keys to select multiple rows or columns.
Double click cells to view or edit definitions.

Color Key
Blue - Inherited Item
Black - Base Item
Red - Changed Inherited Item
Green - Changed Base Item

	1	2	3	4	
H	Item	Image	Description	Rate	Estimated
1	Desktop - Standard		[brand] [model] Standard desktop system including 2.5Ghz, 256mb ram, 40 Gb hard drive, DVD-ROM, with monitor, mouse and keyboard	Cost:	Estimate: 1 week
2	Desktop - Deluxe		[brand] [model] desktop system, standard configuration enhanced with 3.5Ghz, 1Gb ram, 160Gb hard drive, 19" monitor	Cost:	Estimate: 1 week

The UAPM Model Assignments page appears.

4. Select a model and click Assign Model.



Note - To search for all models, click Search without specifying criteria.Masking permitted using any(%) characters.

Criteria Field	Value
(Model Manufacturer) Company Name:	
(Model) Model Name:	
(Model Asset Type) Description:	
(Model Class) Description:	
(Model) Description:	
Only include active records	☑

Search Results

Select and: Assign Model

□	(Model Manufacturer) Company Name:	(Model) Model Name:	(Model Asset Type) Description:	(Model Class) Description:	(Model) Description:
☑	Dell Inc.	OptiPlex 980	Computers primarily used by end-users rather than serving other computers.	Workstation Hardware.	
□	Microsoft Corporation	Adobe Illustrator	Software family		
□	WinZip Computing, Inc.	WinZip	Software family		
□	Dell Inc.	Precision WorkStation 470	Computers primarily used by end-users rather than serving other computers		

Integration Summary

Integrating CA Service Catalog with CA SDM lets you:

- Automatically open change orders in CA SDM.
- Associate CIs to the related change order.
- Streamline the fulfillment process.
- Administer common multi-tenancy.

CA SDM CMDB component integration addresses issues faced in establishing a service catalog by:

- Establishing linkages between the logical service as consumed and the physical infrastructure asset.
- Helping determine which infrastructure assets comprise each service.
- Helping improve IT service quality, cost control, and the alignment of IT with the business.

Chapter 4: CA Clarity™ Project and Portfolio Manager

Overview of CA Clarity PPM

CA Clarity™ Project and Portfolio Manager (CA Clarity PPM) Release 12.1 is an IT Governance solution. CA Clarity PPM enables IT organizations to achieve improved efficiency and performance by improving the quality of their engagements with the business. CA Clarity PPM integrates portfolio planning, demand management, project management, resource planning, and time and cost management functionalities.

Features

CA Clarity PPM provides the following features:

- Structured environment for deciding which projects, programs, or initiatives to fund, sustain, or cancel.
- Single, integrated system that provides easy access to any portfolio type.
- Out-of-the-box metrics that offer flexibility and accuracy when measuring investment evaluations.
- Multiple what-if scenarios that help identify best business alternatives.
- Real-time investment status that allows faster response to obstacles.
- Efficient frontier graphical analysis that optimizes the portfolio.

Integration Details

CA SDM Analysts use CA SDM to manage and evaluate change orders. When CA SDM is integrated with CA Clarity PPM, an additional Project field is available on the CA SDM Change Order Detail window. In addition, new change order categories that are associated to predefined workflows have been added as part of the integration. The CA SDM Administrator can define additional categories and workflows using these out-of-the-box components.

If a change order in CA SDM represents work that is tracked and managed on an existing CA Clarity PPM project, the integration can create CA Clarity PPM Change Order tasks, incidents, or ideas by selecting the appropriate category and completing the required information on the CA SDM change order. When CA Clarity PPM creates and updates a workflow task for the project, it updates CA SDM by logging a comment in the CA SDM Change Order Activity Log.

In this integration, CA SDM uses a remote reference call to send data to CA Clarity PPM using its XML Open Gateway (XOG) API. CA Clarity PPM, in turn, updates CA SDM using its web services.

Note: Refer to the CA Clarity PPM product documentation or the product page on http://ca.com/support for information about the current Java version that CA Clarity PPM supports with this integration.

CA SDM can create the following CA Clarity PPM elements from a CA SDM Change Order:

- **CA Clarity PPM Change Order Task**

  CA SDM Analysts manage and evaluate CA SDM change orders. When integrated with CA Clarity PPM, an additional Project field is available on the CA SDM Change Order Detail window.

  If a change order represents work that is tracked and managed on an existing CA Clarity PPM project, selecting the category field Project.Maint Clarity Only on the Change Order Detail window creates a change order task for the corresponding CA Clarity PPM project. When that task is created, CA Clarity PPM sends an update to CA SDM. The update adds a log comment to the Change Order Activity Log.

- **CA Clarity PPM Incidents**

  A CA SDM Analyst typically initiates a CA Clarity PPM incident after the change order that represents the demand has been analyzed and it has been determined that a CA Clarity PPM incident report must be created. This process is invoked by selecting Project.Other Maint Work in the category field of the Change Order Detail window. After the incident is created, the incident can remain as an incident or the CA Clarity PPM Change Manager can convert the incident to a CA Clarity PPM project.

  Note: For information about CA Clarity PPM incidents and how to convert them to projects, see the *CA Clarity PPM Using Demand Management Guide*.

  When a CA Clarity PPM incident is created using this integration, CA Clarity PPM in turn sends an update to CA SDM. This update is entered as a log comment in the CA SDM Change Order Activity Log List.

- **CA Clarity PPM Ideas**

  A CA SDM Analyst typically initiates a CA Clarity PPM idea after the change order that represents the demand has been analyzed and it has been determined that a CA Clarity PPM idea must be created. This process is invoked by selecting Project.New System Development in the category field of the Change Order Detail window.

  The idea can remain as an idea, or the CA Clarity PPM Demand Manager can convert the idea to a project.

  Note: For information about CA Clarity PPM ideas and how to convert them to projects, see the *CA Clarity PPM Using Demand Management Guide*.

  When a CA Clarity PPM idea is created using this integration, CA Clarity PPM in turn sends an update to CA SDM. This update is entered as a log comment in the CA SDM Change Order Activity Log List.

Integration Points and Functionality from CA SDM

The following integration points are available from CA SDM:

- Automatic creation of CA Clarity PPM Change Order tasks, incidents, and ideas from the CA SDM Change Order Detail window by selecting the correct change order category.
- Status updates to the correct workflow tasks associated with the selected category.

Note: See the Field Mappings appendix in the *CA Clarity PPM Connector Guide* to see how the fields are mapped between the two products. Only these fields can act as integration points between these products. If you need to map some custom fields also, contact the CA Technologies Services team.

Integration Points from CA Clarity PPM

When CA Clarity PPM and CA SDM are integrated, certain CA Clarity PPM actions trigger an update that is sent to CA SDM. These updates are logged as comments on the CA SDM Change Order Activity Log. The following CA Clarity PPM actions trigger comments that are logged:

- Converting CA Clarity PPM incidents to projects
- Converting CA Clarity PPM ideas to projects
- Marking CA Clarity PPM change order tasks as Scheduled
- Creating CA SCM for Distributed packages from CA Clarity PPM change order tasks
- Canceling CA Clarity PPM change order tasks
- Marking CA Clarity PPM change order tasks as Complete
- Marking CA Clarity PPM projects as Complete

Integration Value

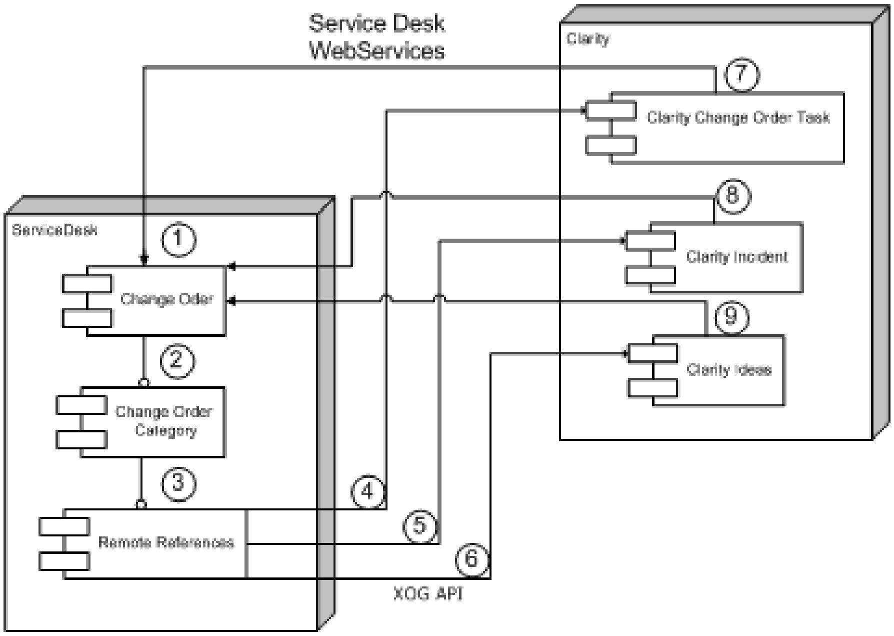
The CA Clarity PPM integration provides the following value:

- Help ensure the most efficient and cost-effective use of IT resources by providing complete cost and resource visibility for the change process.
- Gain greater alignment between your business units and the teams that are responsible for application maintenance and operations.

- Integrate change management processes throughout the change lifecycle, from initiation through closure.
- Eliminate manual and error-prone double entry of information.

How the Integration Works

The following diagram illustrates how the CA Clarity PPM integration works:



The integration between CA Clarity PPM and CA SDM works as follows:

1. From the CA SDM Change Order Detail window, the Administrator selects the Change Order category.
2. Based on the Change Order category, CA SDM creates one of the following items using Remote Reference functionality to call and send data to CA Clarity PPM through its XOG API:
    - CA Clarity PPM change order
    - CA Clarity PPM incident
    - CA Clarity PPM ideas

3. CA Clarity PPM sends updates to CA SDM when certain events occur. These updates are logged as comments on the CA SDM Change Order Activity Log. The following CA Clarity PPM events trigger comments that are logged:

   - Converting CA Clarity PPM incidents to projects
   - Converting CA Clarity PPM ideas to projects
   - Marking CA Clarity PPM change order tasks as Scheduled
   - Creating CA SCM for Distributed packages from CA Clarity PPM change order tasks
   - Canceling CA Clarity PPM change order tasks
   - Marking CA Clarity PPM change order tasks as Complete
   - Marking CA Clarity PPM projects as Complete

   Note: In CA SDM, you can view the Change Order Activity Log List from the Activities tab of the Change Order Detail window. For more information, see the CA SDM online help.

The following URLs are sample URLs for this integration when both products are using Tomcat as the Application Server.

CA Clarity PPM URL:

```
http://ClarityServerName/niku/app
```

CA Clarity PPM NSA URL:

```
http://ClarityServerName:8090/niku/app
```

CA SDM URL:

```
http://ServiceDeskManagerHostName:8080/CAisd/pdmweb.exe
```

Configure the Integration from CA Clarity PPM

Configuring the integration from CA Clarity PPM requires installing and configuring the Connector CA SDM/CA SCM add-in. The connector includes processes, views, objects, tabs, lookups, pages, and portlets that allow CA Clarity PPM to integrate with CA SDM and CA SCM. The add-in must be installed during the installation of the connector.

The following sections describe the steps for installing and configuring the add-in.

Note: For more information about what is included in an add-in, see the *CA Clarity PPM Administration Guide*.

How to Install the Connector

Install the connector add-in so that the content is available to CA Clarity PPM users. You must complete these steps on your CA Clarity PPM application server.

Download the ISO Image File

All add-ins are delivered through the CA Clarity PPM Connector for CA SDM and CA SCM ISO (.iso) image file. The .iso image file includes a .jar file. The .jar file contains the files that are needed to install the add-in. The installer updates the existing CA Clarity PPM installation with the newly downloaded files.

To download the .iso image file, go to the CA Clarity PPM product support page on http://ca.com/support and download the .iso image to your computer or an accessible network location. After you can access the .iso image file, mount it using a mount tool (for example, magicISO).

Follow these steps:

1. Mount the ISO image (refer to http://ca.com/support for instructions to mount the ISO image).

   Note: You can use the MagicISO tool to assist in mounting the ISO image.

2. Extract the JAR file to a directory on the application server.

3. Stop the CA Clarity PPM Application (app) and CA Clarity PPM Background (bg) services.

4. Install the add-in.

5. Start the app and bg services.

If you have already installed an older version of the add-in, you can upgrade to the new version using the following steps:

1. Apply the add-in.

2. Publish the applied add-in items.

Extract the .jar File

Extract the .jar file to a temporary directory location (for example, C:\temp) on the CA Clarity PPM application server where you will be completing the installation process.

The .jar file includes the following files:

install.sh

Includes the UNIX system installation script.

install.bat

Includes the Windows system installation script.

install.xml

Includes the Ant installation script.

package

Includes the directory of updated files.

tools

Includes the directory of supporting files.

Follow these steps:

1. Open the command prompt and execute the following command:

   For Windows:

   ```
   jar -xvf filename
   ```

   For UNIX system:

   ```
   jar -xvf filename
   ```

   These commands extract the contents of the .jar file to the same location where the .jar file resides.

2. (UNIX environment) Execute the following command:

   ```
   chmod +x install.sh
   ```

   This command grants execution privileges for the install script.

Stop the CA Clarity PPM Services

You must stop the CA Clarity PPM Application (app) and CA Clarity PPM Background (bg) services before applying add-ins. Restart the services after you have applied the add-in to CA Clarity PPM from CA Clarity PPM System Administration. The following sections explain how to stop the services in different server configurations.

Important! If the CA Clarity PPM System Administration (nsa), Database (db), Beacon, and Reports (reports) services are deployed on the server, do *not* stop them.

Follow these steps:

1. Log in to CA Clarity PPM System Administration.

   The Overview page appears.

2. Select All Services from the Home menu.

   The All Services page appears.

3. Select the CA Clarity PPM Application (app) and the CA Clarity PPM Background (bg) service check boxes and click Stop.

   The services are stopped.

Note: See the *Clarity Connector for CA Service Desk Manager & CA Software Change Manager for Distributed Product Guide* for additional information about stopping or starting the required CA Clarity PPM services based on the application server you use (for example, Tomcat).

Install the Add-In

The following procedure installs the updates to objects, reports, and the database.

Important! Back up your CA Clarity PPM installation before installing this add-in so that you can restore the application to the prior version, if necessary. After you install the add-in, you cannot uninstall it.

Follow these steps:

1. Open the command prompt, navigate to the folder where you extracted the .jar files, and execute the following command:

   ```
   install
   ```

   The installation process begins.

2. Follow the instructions in the wizard to complete the add-in installation.

   The following example shows the installation of the add-in to the C:\Clarity directory, which is the NIKU_HOME of the CA Clarity PPM server.

```
-------------------------------------------------------------
This program will install package cai:
See the included README.txt for more information.
-------------------------------------------------------------
_install:
init:
install:
---------------------------------------------------------------------------
This program will install the CA Service Desk - Harvest Integration (CAI)
---------------------------------------------------------------------------
init:
files:
    [copy] Copying 89 files to C:\clarity
deploy:
    [exec] Installing content... cai
    [exec] - Initializing: pma.init...
    [exec] SYS  2011-06-27 23:07:30,424 [main] niku.union Initializing: pma.init...
    [exec] Content Pack Installation Complete....
languages:
upgrade:
_install:
    [java] ==========================================
    [java] DBTools Log - Mon Jun 27 23:10:11 EDT 2011
    [java] ==========================================
    [java]
    [java] Total time: 0H:0M:1S
    [echo] Package Installation Successful - 27-June-2011 23:10:13
BUILD SUCCESSFUL
```

Start CA Clarity PPM Services

After you install the add-in, start the CA Clarity PPM Application (app) and CA Clarity PPM Background (bg) services. Use a configuration that has the Apache Tomcat as the application server, with all services running on a single server.

Follow these steps:

1. Log in to CA Clarity PPM System Administration.

   The Overview page appears.

2. Select All Services from the Home menu.

   The All Services page appears.

3. Select the CA Clarity PPM Application (app) and the CA Clarity PPM Background (bg) service check boxes and click Start.

   The services are started.

Upgrade an Existing Add-In

If you already have installed the add-in and you are upgrading to a current add-in version, apply the new or modified items that you need.

When you upgrade to the current add-in version, only those items that are new or modified are selected by default. You can select or clear the items that you want to apply.

New items are listed with a status of Not Installed. Modified items are listed with a status of Needs Update. You can select or clear the items that you want to apply.

Important! Before you apply modified items, verify that the existing items have not been configured. If the existing items have been configured, you may not want to apply these items. Applying modified items to existing items overwrites the existing configurations.

Follow these steps:

1. Log in to CA Clarity PPM and open the Administration Tool.

   The Administration Home page appears.

2. Select Add-Ins from the CA Clarity PPM Studio menu.

   The Add-Ins page appears.

3. Click the name of the add-in from which you want to apply items.

   The Add-In Details page appears.

4. Review each selected item and accept only those changes that you want. Only those items with selected check boxes are updated. Click Apply.

   Note: If a selected item has dependencies on other items, the dependencies are also updated.

   A list of updated items displays in the Confirm Add-In Update or Install page.

5. Do one of the following actions:

   - Click Yes to update or install the items.

     The add-in items are applied to CA Clarity PPM.

   - Click No to cancel the process.

   The Add-In Details page appears.

Publish the Applied Add-in Items

If the applied add-in items contain existing items that are configured, publish the items so that the user can see the changes.

Note: For more information about publishing configured items (such as portlets, pages, and views), see the *Studio Developer's Guide*.

Install the Add-In on Niku Application Service

Stop the Niku Application (app) service before you deploy the add-in. Restart the service after the add-in is deployed.

Follow these steps:

1. Log in to Niku System Administration (NSA) as an Administrator.

2. Click All Services from the Overview menu.

   The All Services page appears.

3. Select the Niku Application check box and click Stop.

4. Install the Connector: Unicenter Service Desk/Harvest add-in from NSA using the following steps:

    a. Select Install and Upgrade from the Installation menu.

    The Install and Upgrade: Pre-Upgrade page appears.

    b. Select Add-Ins under Installation Tasks from the content menu.

    The Install: Add-Ins page appears.

    c. Select the Connector: Unicenter Service Desk/Harvest check box.

    d. Click Install.

5. Start the Niku Application service using the following steps:

    a. Select All Services from the Home menu.

    The All Services page appears.

    b. Select the Niku Application check box and click Start.

    The add-in is successfully installed.

How to Configure the Connector

After you install the connector add-ins, configure the connector to specify resource names that need access rights.

Change the Password for the CAIAdmin User

After you install the add-in from CA Clarity PPM System Administration, change the CAIAdmin user password. The CAIAdmin user is the CA Clarity PPM resource that is used by the CAI processes included with the Connector: CA Service Desk/Harvest add-in. This user is not the CA Clarity PPM administrator user.

Note: If you change the password to something other than caiadmin, verify that you use the changed password throughout the connector configuration and setup.

Follow these steps:

1. Log in to CA Clarity PPM and open the Administration Tool.

   The Administration Home page appears.

2. Select Resources from the Organization and Access menu.

   The Resources page appears.

3. In the Resource Filter, enter cai and click Filter.

4. Select the name of the CAIAdmin user.

   The Resource: Properties page for that resource appears.

5. Complete the following fields:

   Password

   Enter caiadmin.

   Confirm Password

   Enter caiadmin.

   Force Password

   Clear the check box.

   Note: If you change the password to something other than caiadmin, verify that you use the same password in the Test.properties file in the CA SDM configuration section.

6. Click Save and Exit.

   The Resources page appears.

Grant Harvest Project Access Rights to CA Clarity PPM Resources

If you are integrating CA Clarity PPM with CA SCM, grant Harvest Project global access rights to each CA Clarity PPM resource that will be creating Harvest Projects in CA Clarity PPM. You must grant four global access rights to CA Clarity PPM resources. These access rights let the resources view the Harvest Project custom object in CA Clarity PPM and create Harvest Projects in CA Clarity PPM.

Note: If the CA Clarity PPM user is not associated to a CA Clarity PPM resource, create the resource first. See your CA Clarity PPM administrator or the *CA Clarity PPM Administration Guide* for more information.

Follow these steps:

1. Log in to CA Clarity PPM and open the Administration Tool.
2. Click Resources from the Organization and Access menu.

   The Resources page appears.
3. Click the name of the resource to which you want to grant Harvest Project global access rights.

   The Resource: Properties page appears.
4. From the content menu, under Resource Access Rights, select Global.

   The Resource: Global Access Rights page appears.
5. Click Add.

   The Select Access Rights page appears.
6. Filter the global access rights by entering Harvest at Access Right in the Access Right Filter section and click Filter.
7. Click the Select All icon to select all four access rights in the list and click Add.

   The Resource: Global Access Rights page appears.
8. Click Exit.

   The Resources page appears.

Note: If you are integrating CA Clarity PPM with CA SCM, see the *Connector for CA Unicenter Service Desk & CA Software Change Manager for Distributed Product Guide* in the CA Clarity PPM documentation bookshelf.

Edit the GEL Script Custom Parameters

Several CA Clarity PPM processes are included with the Connector: CA Service Desk Manager/Harvest add-in. These processes are the connection processes included with the connector.

Note: See your CA Clarity PPM administrator or the *CA Clarity PPM Administration Guide* for more information about the CA Clarity PPM processes.

Edit the GEL Script Custom Parameters for each of the process steps to set the values for user names, passwords, and URLs. Edit the process step scripts, and not the custom script parameters that are listed on the Custom Script Parameters page. The Custom Script page contains a text box where you can configure the parameters.

After editing the GEL Custom Parameters for each of the process steps, validate and activate the CAI processes. Do *not* edit the GEL scripts directly using the Custom Scripts page. Use the Custom Scripts Parameters page, unless you are instructed otherwise by CA Technologies Support.

Follow these steps:

1. Open the CA Clarity PPM Administration Tool. The tool icon is at the top right on the Harvest Project List page.

   The Administration Home page appears.

2. Select Processes from the Data Administration menu.

   The Available Processes page appears.

3. Filter the list by entering cai in the Process Name field and clicking Filter.

   You can now view the CAI processes that are related to the connector.

4. Select the name of the process that you want to edit from the list of processes.

   The Process Definition: Properties page appears.

5. Configure the process steps based on the products that you have installed for your integrated systems. Use the following table to determine which process step you need to configure.

   Note: You only need to activate the processes that are associated with the products that you installed and connected. This example covers the third column in the following table, "Configure and Activate CA Clarity PPM – CA SDM only".

Process	Step	Configure and Activate CA Clarity PPM - CA SDM only	Configure and Activate CA Clarity PPM - Harvest only	Configure and Activate all
CAI Harvest	Create	No	Yes	Yes
CAI Harvest Status	Update Status	No	Yes	Yes
CAI Project Post Create	Create	Yes	No	Yes
CAI Project Update	Update	Yes	No	Yes
CAI SDCO Task Update	Update	Yes	No	Yes
CAI Service Desk Create	Create	Yes	No	Yes
CAI Service Desk Task Create Post	Create Post	Activate Only	No	Activate Only
CAI Harvest Status ED	ED	No	No	No

6. Select Steps from the content menu.

   The Process Definition: Steps page appears.

7. Click the name of the step that you want to edit. See the process-step table to determine which step to edit.

8. Click the Name of the Action in the Actions section.

   The Custom Script Properties page appears.

9. Click the Custom Script Parameters option from the content menu.

10. Provide the values of attributes that are relevant to your integration. See Variable Settings (see page 114) for information about variable changes that are required for the process steps.

11. Click Save.

12. Click Validate to verify that the process contains no errors and click Cancel.

13. Click Cancel to return to the Processes list page.

Variable Settings

The following table lists the variables and their default settings and descriptions for the CAI Harvest Feature Create process for the Create Harvest Feature step.

Variable Name	Default Setting	Description/Action
pbroker	harvest	Enter the name of the Harvest broker.
pusername	harvest	Enter the name of the Harvest user.
ppassword	harvest	Enter the password of the Harvest user.
pcreatePkgProc	Create RFC	Enter the name of the Harvest process that is associated to the CA SDM Clarity Connector lifecycle template. **Note:** The default process is Create RFC. If the name of this process is changed in Harvest, this parameter must be changed to match the new name.
pdevState	Plan	Enter the first default state of the Harvest package. The default state should be Plan.
clarity_dbId	niku	Enter the CA Clarity PPM data source.
SDURL	http://localhost:8080/axis/services/USD_R11_WebService	Enter your CA SDM server name and port.
SDUserName	ServiceDesk	Enter the name of the CA SDM user. CA Technologies recommends entering a CA SDM user other than ServiceDesk, because this user is typically the administrator.
SDPassword	ServiceDesk	Enter your CA SDM password.
locale	en	Enter the locale value of your CA SDM server.
csvWeights	0.25, 0.5, 0.75, 1.0	Enter the values of the weights that are associated with the four Harvest lifecycle states that are included with CA Clarity PPM out of the box. The weights that you assign to each state are the weights used to calculate the Overall % Complete field.
dateFormat	yyyy-MM-dd HH:mm:ss	Enter the format for the date and timestamp. This format should be the default.
pbroker	harvest	Enter the name of the Harvest broker.
pusername	harvest	Enter the name of the Harvest user.
ppassword	harvest	Enter the password for the Harvest user.

The following table lists the variables and their default settings for the CAI Project Post Create process for the Set SD CO InProgress Status step:

Variable Name	Default Setting	Description/Action
clarity_dbId	niku	Enter the CA Clarity PPM data source.
SDURL	http://localhost:8080/axis/services/USD_R11_WebService	Enter the URL, including the name and port, of the CA SDM server.
SDUserName	ServiceDesk	Enter the name of the CA SDM user. CA Technologies recommends entering a CA SDM user other than ServiceDesk, because this user is typically the administrator.
SDPassword	ServiceDesk	Enter the password for the CA SDM user.
locale	en	Enter the locale for the CA SDM server.

The following table lists the variables and their default settings for the CAI Project Update process for Send Project Complete Message step:

Variable Name	Default Setting	Description/Action
clarity_dbId	niku	Enter the CA Clarity PPM data source.
SDURL	http://localhost:8080/axis/services/USD_R11_WebService	Enter the URL, including the name and port, of the CA SDM server.
SDUserName	ServiceDesk	Enter the name of the CA SDM user. CA Technologies recommends entering a CA SDM user other than ServiceDesk, because this user is typically the administrator.
SDPassword	ServiceDesk	Enter the password for the CA SDM user.
locale	en	Enter the locale for the CA SDM server.

The following table lists the variables and their default settings for the CAI CA SDM Create process for Create Object step:

Variable Name	Default Setting	Description/Action
XOGUsername	caiadmin	Enter the CAI administrator user name, or the user name of a user with XOG rights.
XOGPassword	caiadmin	Enter the CAI administrator password or the password of a user with XOG rights.
XOGURL	http://localhost:80	Enter the URL, including the name and port, of the CA Clarity PPM server.

Variable Name	Default Setting	Description/Action
clarity_dbId	niku	Enter the CA Clarity PPM data source.
clarity_sd_resource	caiadmin	Enter the ID of the CA SDM user who can create or update an idea, incident, or project.
SDURL	http://localhost:8080/axis/services/USD_R11_WebService	Enter the URL, including the name and port, of the CA SDM server.
sDUserName	ServiceDesk	Enter the name of the CA SDM user. CA Technologies recommends entering a CA SDM user other than ServiceDesk, because this user is typically the administrator.
sDPassword	ServiceDesk	Enter the password for the CA SDM user.
locale	en	Enter the locale for the CA SDM server.

Validate and Activate the Processes

After you edit the GEL Script custom parameters for the processes included with the Connector: CA SDM/CA Software Change Manager add-in, validate and activate all of the processes. These processes are the processes that you plan to use, and not just the ones that you configured.

Note: See your CA Clarity PPM administrator or the *CA Clarity PPM Administration Guide* for more information about working with processes.

Follow these steps:

1. Select the name of the process that you want to validate from the list of processes.

   The Process Definition: Properties page appears.

2. Click Validation from the content menu.

   The Process Definition: Validation page appears.

3. Click Validate All and Activate.

   Note: If errors are displayed, correct them and validate the process again.

4. Click Properties on the content menu.

   The Process Definition: Properties page appears.

5. Click Exit.

6. Repeat these steps for all the processes that you want to use.

   Note: See the *Clarity Connector for CA SDM & CA Software Change Manager for Distributed Product Guide* for more information about scheduling Clarity processes for CA SCM connectivity.

Configure the Integration from CA SDM

Configuring the integration from CA SDM requires installing and configuring the XML Open Gateway (XOG) client on CA SDM application servers. XML Open Gateway is the CA Clarity PPM web service interface. Using XOG, you can read and write data objects from CA Clarity PPM. You can also use this interface to import data from external systems into CA Clarity PPM. Since the integration uses web services, install and configure the XOG Client on the CA SDM application server.

This section provides the instructions for installing and configuring the XOG client on different operating systems. If the XOG client is not installed on the CA SDM servers, the integration between CA Clarity PPM and CA SDM does not work.

Note: See your CA Clarity PPM administrator or the *CA Clarity PPM Integration Guide* for more information about XOG.

Download the XOG Client from CA Clarity PPM

For Windows, UNIX system, and LINUX servers, download the XOG client from CA Clarity PPM before setting up XOG on the CA SDM application server. You must download the XOG client even if CA SDM is installed on the same server as CA Clarity PPM.

Follow these steps:

1. From the CA SDM application server, log in to CA Clarity PPM as the Administrator and open the Administration Tool.

   The Administration Home page appears.

2. Click Client Downloads from the General Settings menu.

   The Client Downloads page appears.

   Note: To see the General Settings section, use the scroll bar to navigate to this area.

3. Click the Download link next to Cross-platform ZIP.

   The File Download window opens. The cross-platform ZIP file contains the XOG client.

4. Click Save.

   The xogclient.zip file is saved to a local folder on the CA SDM application server.

How to Set Up XOG Client on Windows CA SDM Application Servers

The following sections describe how to set up the XOG client when CA SDM is installed on a Windows application server.

Extract the ZIP file

After you download the XOG client from CA Clarity PPM, extract the XOG files on the Windows CA SDM application server. To extract the ZIP file, open any file compression utility and extract the xogclient.zip file to a folder (for example, C:\CA_Clarity\XOG) on the CA SDM application server.

Copy Files to the XOG Client

If you are setting up the add-in on CA Clarity PPM, copy the following files to the XOG client:

- Copy all the files under *cai add-in*\package\xogclient\bin\ to *xogclient_path*\bin
- Copy the *cai add-in*\package\xogclient\lib\cai-client.jar file to *xogclient_path*\lib\

Note: The *cai add-in* refers to the location of the extracted Clarity Connector: CA Service Desk Manager/Harvest add-in files. The c:\temp directory contains the Clarity Connector add-in that you extracted on the CA Clarity PPM server.

Edit the test.properties File

Edit the test.properties file to specify the CA Clarity PPM server name, port number, CAIAdmin user, and password information. This information must be defined for each CA SDM server that will be connecting to a CA Clarity PPM server instance. The XOG client uses this information to send the CA SDM change order information to the predefined CAIAdmin user on the CA Clarity PPM server.

Follow these steps:

1. Using a text editor, open the test.properties file located in the folder that contains the extracted XOG files (for example, C:\Clarity\XOG \bin\test.properties file).
2. Change the following settings:
   - Set the server name to the CA Clarity PPM server name.
   - Set the port to the CA Clarity PPM server port number.
   - Set the user name to caiadmin.
   - Set the password to caiadmin.

   Note: If you changed the default caiadmin password to something other than caiadmin, set this value to the new password setting.
3. Save and close the test.properties file.

Create System Environment Variables

Create a Windows operating system environment variable named XOG_HOME and define it to point to the home directory of the XOG client. Create the JAVA_HOME environment variable also, if you do not already have it. JAVA_HOME should point to the JAVA Runtime Installation directory.

Follow these steps:

1. Open the Windows Control Panel and click System.

   The System Properties dialog opens.
2. Select the Advanced tab and click Environment Variables.

   The Environment Variables dialog appears.
3. Click New in the System Variables section of the dialog.

   The New System Variable dialog appears.

4. Provide the following information:
   - Enter XOG_HOME as the variable name.
   - Enter the full path pointing to the XOG folder (for example, C:\Clarity\XOG) as the variable value.
5. Click OK.

   The new variable is saved.
6. Click New in the System Variables section of the window.

   The New System Variable window appears.
7. Provide the following information:
   - Enter JAVA_HOME as the variable name.
   - Enter the full path pointing to the JAVA JRE folder (for example, C:\Progra~2\CA\SC\JRE\1.6.0_23) as the variable value.
8. Click OK.

   The new variable is saved.
9. Identify the system variable PATH and click Edit.
10. Prepend %JAVA_HOME%\bin to the PATH variable value.
11. Save the changes and reboot the CA SDM server.

How to Set Up the XOG Client on UNIX CA SDM Application Servers

The following sections describe how to set up the XOG client on UNIX, Sun Solaris, and IBM AIX CA SDM application servers.

Extract the ZIP file

Download the XOG client from CA Clarity PPM before extracting XOG on the UNIX CA SDM application server. For more information about downloading the XOG client, see Download the XOG Client from CA Clarity PPM (see page 117).

Follow these steps:

1. Log in as the root user in the UNIX system.
2. Create the /*path*/Clarity/XOG folder structure.

   Example:

   /opt/CA/Clarity/XOG
3. Copy the xogclient.zip file to /*path*/Clarity/XOG.
4. Unzip the contents to /*path*/Clarity/XOG.
5. Change directory to /*path*/Clarity/XOG/bin.
6. Grant read and execute rights for the cai.sh file by executing the following command at the command prompt:

   ```
   chmod 555 cai.sh
   ```

Copy Files to the XOG Client

Perform this procedure only if you are integrating with CA Clarity PPM Release 12.0 or 8.1.

Follow these steps:

1. Copy all the files under *cai add-in*/package/xogclient/bin/ to the *xogclient_path/*bin folder.
2. Copy the *cai add-in/*package/xogclient/lib/cai-client.jar file to the *xogclient_path*/lib/ folder.

Note: The *cai add-in* refers to the location of the extracted Clarity Connector: CA SDM/CA Software Change Manager add-in files.

Edit the test.properties File

Edit the test.properties file to specify the CA Clarity PPM server name, port number, CAIAdmin user, and password information. This information needs to be defined for each CA SDM server that will connect to a CA Clarity PPM server instance. The XOG client uses this information to send the change order information to the predefined CAIAdmin user on the CA Clarity PPM server.

Follow these steps:

1. Log in as the root user in the UNIX system.
2. Open the test.properties file located in the folder that contains the extracted XOG files.

   Example:

   ```
   /path/Clarity/XOG/bin/test.properties
   ```
3. Change the following settings:

   - Set the server name to the CA Clarity PPM server name.
   - Set the port to the CA Clarity PPM server port number.
   - Set the user name to caiadmin.
   - Set the password to caiadmin.

   Note: If you changed the default caiadmin password to something other than caiadmin, set this value to your new password setting.
4. Save and close the test.properties file.

Create System Environment Variables

Create a UNIX operating system environment variable named XOG_HOME and define it to point to the home directory of the XOG client. Also, create the JAVA_HOME environment variable, if you do not already have it.

Follow these steps:

1. Log in as the root user in the UNIX system.
2. Execute the following command to stop CA SDM daemons:

   ```
   pdm_halt
   ```

3. Edit the shell running on the UNIX system.

   - For Solaris, edit the /etc/profile and the /etc/.login.
   - For AIX, edit the /etc/profile and the /etc/csh.login.

4. Add the following lines to the beginning of the identified file:

   - For /etc/profile:

     ```
     XOG_HOME =/path/Clarity/XOG
     export XOG_HOME
     JAVA_HOME=java installed path (up to but not including the bin directory)
     export JAVA_HOME
     ```

   - For /etc/.login or /etc/csh.login:

     ```
     setenv XOG_HOME path/Clarity/XOG
     setenv JAVA_HOME java installed path (up to but not including the bin directory)
     ```

5. If the CA SDM privileged user is running the C or Trusted C shells, add the following line to the /etc/.login:

   ```
   setenv XOG_HOME path/Clarity/XOG
   ```

6. Exit the UNIX session.

7. Log in to the UNIX system again as the CA SDM privileged user.

8. Execute the following command to verify that the XOG_HOME environment variable and JAVA_HOME are set correctly:

   ```
   env
   ```

9. Execute the following command to restart the CA SDM daemons:

   ```
   pdm_init
   ```

How to Set Up the XOG Client on LINUX CA SDM Application Servers

The following sections describe how to set up the XOG client on LINUX CA SDM application servers.

Extract the ZIP file

Download the XOG client from CA Clarity PPM before extracting XOG on the Linux CA SDM application server. For more information about downloading the XOG client, see Download the XOG Client from CA Clarity PPM (see page 117).

Follow these steps:

1. Log in as the root user in LINUX.
2. Create the /*path*/Clarity/XOG folder structure.

   Example:

   ```
   /opt/CA/Clarity/XOG
   ```
3. Copy the xogclient.zip file to /*path*/Clarity/XOG.
4. Unzip the contents of the zip file to /*path*/Clarity/XOG.
5. Change directory to /*path*/Clarity/XOG/bin.
6. Assign read and execute rights for the cai.sh file by executing the following command at the command prompt:

   ```
   chmod 555 cai.sh
   ```

Copy Files to the XOG Client

Perform this procedure only if you are integrating with CA Clarity PPM Release 12.0 or 8.1.

Follow these steps:

1. Copy all the files under *cai add-in*/package/xogclient/bin/ to: *xogclient_path/*bin
2. Copy the *cai add-in/*package/xogclient/lib/cai-client.jar file to: *xogclient_path*/lib/

Note: The *cai add-in* refers to the location of the extracted Clarity Connector: CA SDM/CA Software Change Manager add-in files.

Edit the test.properties File

Edit the test.properties file to specify the CA Clarity PPM server name, port number, CAIAdmin user, and password information. This information needs to be defined for each CA SDM server that will be connecting to a CA Clarity PPM server instance. The XOG client uses this information to send the CA SDM change order information to the predefined CAIAdmin user on the CA Clarity PPM server.

Follow these steps:

1. Log in as the root user in LINUX.
2. Open the test.properties file located in the folder that contains the extracted XOG files.

   Example:

   ```
   /path/Clarity/XOG/bin/test.properties
   ```
3. Change the following settings:

   - Set the server name to the CA Clarity PPM server name.
   - Set the port to the CA Clarity PPM server port number.
   - Set the user name to caiadmin.
   - Set the password to caiadmin.

   Note: If you changed the default caiadmin password to something other than caiadmin, set this value to your new password.
4. Save and close the test.properties file.

Create System Environment Variables

Create a LINUX operating system environment variable named XOG_HOME and define it to point to the home directory of the XOG client. Also, create the JAVA_HOME environment variable, if you do not already have it.

Follow these steps:

1. Log in as the root user in LINUX.
2. Execute the following command to stop CA SDM daemons:

   ```
   pdm_halt
   ```

3. Add the following lines to the beginning of /etc/profile:

   ```
   XOG_HOME=/path/Clarity/XOG;
   export XOG_HOME;
   JAVA_HOME=java_install_path (up to but not including the bin directory);
   export JAVA_HOME;
   ```

4. If the CA SDM privileged user is running the C or Trusted C shells, add the following line to the /etc/.login:

   ```
   setenv XOG_HOME /path/Clarity/XOG
   ```

5. Exit your LINUX session.

6. Log in to LINUX again as the CA SDM privileged user.

7. Execute the following command to verify if the XOG_HOME environment variable and JAVA_HOME are set correctly:

   ```
   env
   ```

8. Execute the following command to restart the CA SDM daemons:

   ```
   pdm_init
   ```

Load Data on CA SDM Server

As part of the integration configuration, load the necessary CA SDM data on the CA SDM server.

Follow these steps:

1. Log in to the CA SDM server.

2. Open a command prompt window and specify the location of the \data directory within the CA SDM installation files.

   Example:

   ```
   C:\Program Files (x86)\CA\Service Desk Manager\data
   ```

3. Execute the following command:

   ```
   pdm_load –f projex.dat
   ```

4. If there are any errors during the load, review the errors and rerun the load.

   If the load is successful, no message is displayed.

5. Log in to CA SDM using CA SDM Administrator credentials and click the Administration tab.

6. Select Service Desk on the left and expand it.

7. Expand Change Orders on the left and select Categories.

8. On the right of the Change Category List page, verify that categories such as Project.Maint CA Clarity PPM Only appear.

   Note: If you see categories, the data probably was loaded successfully.

Integration Example

This section describes the functional integration between CA SDM and CA Clarity PPM. The example describes how to perform the following actions:

- Create CA Clarity PPM change order tasks using CA SDM.
- Create CA Clarity PPM incidents and ideas.
- Monitor the integration progress using the CA SDM Change Order Activity Log.

Create CA Clarity PPM Change Order Tasks

Use this procedure to create CA Clarity PPM change order tasks.

Follow these steps:

1. Open a CA SDM change order.

2. In the Category field, select Project.Maint Clarity Only from the drop-down list.

3. Complete the following fields:

   Description

   Specifies the order description from the original change order that created the CA Clarity PPM task.

   Need By Date

   Specifies the date and time when you want the CA SDM change order to be resolved and closed.

Project

Specifies the CA SDM asset or project CI that was set up to reference the project in the external system, such as CA SCM for Distributed or CA Clarity PPM.

You must define the external project to CA SDM before you can initialize integration with the external project. This field is then used in the change order that you create to link it to the project in the external system.

Requester

Specifies the name of the person initiating the change order. This person must be a defined contact in CA SDM.

Affected End User

Specifies the name of the person affected by the change order. This user can be the same person as the requester. This user must be a defined contact in CA SDM.

4. Click Save.

5. Change the CA SDM change order Evaluate Clarity Task workflow task status from Pending to Evaluate.

   The workflow invokes the integration process between CA SDM and CA Clarity PPM. The CA Clarity PPM change order task is created on an existing CA Clarity PPM project.

   Note: Changes to workflow tasks do not display until the ticket is saved.

6. Click Save.

Create CA Clarity PPM Incidents from CA SDM

CA SDM Analysts typically initiate CA Clarity PPM incidents after the change order that represents the demand has been analyzed and it has been determined that the change order needs to be managed in CA Clarity PPM. The CA Clarity PPM incident can remain as an incident, or the Change Manager can convert the incident to a project.

Note: For information about incidents and how to convert them to projects, see the *CA Clarity PPM Using Demand Management Guide*. For information about CA SDM workflows, see the *CA SDM Administrator Guide* or CA SDM online help.

Follow these steps:

1. Open a change order in CA SDM and click Category.
2. Select the Project.Other Maint Work from the drop-down list.
3. Complete the following fields:

   Order Description

   Specifies a detailed description of the change order or request.

   Category

   Displays the type of change order to which this task is associated.

   Description

   Specifies the order description from the original CA SDM change order that created the CA Clarity PPM task.

   Need By Date

   Specifies the date and time from the CA SDM change order when you want the ticket to be closed and resolved.

   Requester

   Specifies the name of the person initiating the change order. This person must be a defined contact in CA SDM.

   Affected End User

   Specifies the name of the person affected by the change order. This user can be the same person as the requester. This user must be a defined contact in CA SDM.

4. Click Save.
5. From the Workflow Tasks tab, click the sequence number associated with the Create Clarity Work Request workflow.

   The Change Workflow Detail window appears.

6. Change the CA SDM change order Create Clarity Work Request workflow task status from Pending to Complete.

   The workflow invokes the connection between CA SDM and CA Clarity PPM, and the incident is created.

   Note: The changes you make to workflow tasks do not display until you save the ticket.

7. Click Save.

Note: See the *Demand Management User Guide* for more information about CA Clarity PPM ideas and how to convert them to projects.

Create CA Clarity PPM Ideas from CA SDM

Use this procedure to create CA Clarity PPM ideas from CA SDM.

Follow these steps:

1. Open a change order in CA SDM and click Category.

2. Select Project.New System Development from the drop-down list.

3. Complete the following fields:

   Order Description

   Specifies a detailed description of the change order or request.

   Category

   Displays the type of change order to which this task is associated.

   Description

   Specifies the order description from the original CA SDM change order that created the CA Clarity PPM task.

   Need By Date

   Specifies the date and time from the CA SDM change order when you want the ticket to be closed and resolved.

Requester

Specifies the name of the person initiating the change order. This person must be a defined contact in CA SDM.

Affected End User

Specifies the name of the person affected by the change order. This user may be the same person as the requester. This user must be a defined contact in CA SDM.

4. Click Save.
5. From the Workflow Tasks tab, click the sequence number associated with the Create Clarity Idea workflow.

   The Change Workflow Detail window opens.
6. Change the CA SDM change order Create Clarity Idea workflow task status from Pending to Complete.

   Note: Changes to workflow tasks do not display until the ticket is saved.
7. Click Save.

Converting CA Clarity PPM Incidents to Projects

CA Clarity PPM incidents that originate as CA SDM change orders represent the request for maintenance work and contain the details from that change order. To view a list of the fields that are mapped from CA SDM change orders to CA Clarity PPM incidents, see the Field Mappings appendix in the *CA Clarity PPM Connector Guide*.

The CA Clarity PPM Change Manager considers the scope of the new incident and determines that the incident must be managed as a project. The Change Manager then converts the incident to a project.

Each time a CA Clarity PPM incident that originated as a CA SDM change order is converted to a project, CA Clarity PPM sends an update to CA SDM. The log comment is entered in the CA SDM Change Order Activity Log List. The conversion process also triggers CA Clarity PPM to set the CA SDM change order Monitor Clarity Work Request workflow task status from Pending to In Progress.

Note: See the *Demand Management User Guide* for more information about incidents and converting them to projects.

Converting CA Clarity PPM Ideas to Projects

The CA Clarity PPM Change Manager is responsible for reviewing CA Clarity PPM ideas that originate in CA SDM. The CA Clarity PPM Demand Manager considers the scope of the new idea and determines that the idea must be managed as a CA Clarity PPM project. The Change Manager then converts the CA Clarity PPM idea to a project.

Each time a CA Clarity PPM idea that originated as a CA SDM change order is converted to a project, an update is sent to CA SDM. The log comment is entered in the CA SDM Change Order Activity Log List. The conversion process also triggers CA Clarity PPM to set the CA SDM change order Monitor Clarity Project workflow task status from Pending to In Progress.

Converting CA Clarity PPM ideas to projects is a basic Demand Management function.

Note: See the *Demand Management User Guide* for more information about CA Clarity PPM ideas and converting them to projects.

Evaluating and Scheduling CA Clarity PPM Change Order Tasks

The initial status of CA Clarity PPM change order tasks that originate from CA SDM is Evaluate. You can view this status on the Task Properties: Change Order Details page in CA Clarity PPM.

During the evaluation period, the CA Clarity PPM project manager can begin to scope the task and evaluate resource capacity by assigning staff and identifying the estimated time to complete (ETC) and the start and finish dates for the task. Evaluating and scheduling tasks are basic project management functions.

Note: See the *Project Management User Guide* for more information about how to build project teams using CA Clarity PPM.

After the task is evaluated, the CA Clarity PPM project manager can change the CA Clarity PPM change order task status from Evaluate to Scheduled. To do this, from the Task Properties: Change Order Details page, select Scheduled in the Change Order Status field and click Submit.

When you mark a CA Clarity PPM change order task as Scheduled, CA Clarity PPM sends an update to CA SDM. The log comment is entered in the CA SDM Change Order Activity Log List and details the name of the task, resource assigned, ETC, and start and finish dates. The scheduling process also triggers CA Clarity PPM to set the CA SDM change order Evaluate Clarity Task workflow task status from Evaluate to Complete.

Note: If you have only CA SDM and CA Clarity PPM connected, setting the change order task status to Scheduled triggers a CA SDM status change. CA Clarity PPM updates the CA SDM change order Notify Assignee workflow task status from Wait to Pending.

If CA SCM is integrated with CA SDM and CA Clarity PPM and is being used to manage the change order development, setting the change order task status to Scheduled triggers CA Clarity PPM to update the CA SDM change order Monitor Harvest Package workflow task status from Wait to Pending.

Complete CA Clarity PPM Tasks and Projects

The following sections describe how to mark CA Clarity PPM tasks and projects as complete.

Mark Tasks as Complete

When all the CA SCM packages for a task have been promoted to the production lifecycle state, the CA Clarity PPM project manager can mark the CA Clarity PPM task as complete. This action triggers CA Clarity PPM to send an update to CA SDM. The update is entered as a log comment in the CA SDM Change Order Activity Log List and details the task completion.

When the task is complete, the CA SDM assignee must update and close the CA SDM change order and notify the CA SDM end user.

Note: See the *Project Management User Guide* for more information about how to mark tasks as complete.

How Projects are Marked as Complete

After all the project tasks are complete, the CA Clarity PPM project manager must mark the project as complete. This is a basic project management function.

Note: See the *Project Management User Guide* for more information about how to mark projects as complete.

When you complete a CA Clarity PPM project that originated in CA SDM, the following events take place:

- CA Clarity PPM sends an update to CA SDM.
- The log comment is entered in the CA SDM Change Order Activity Log List and details the CA Clarity PPM project completion.

- In CA Clarity PPM, the CA SDM change order Monitor Clarity Project workflow task status is set from In Progress to Complete.
- In CA Clarity PPM, the change order Notify Assignee workflow task status is set from Wait to Pending.

Note: When the project is complete, the CA SDM assignee must update and close the CA SDM change order and notify the CA SDM end user.

Fault Handling: CA SDM to CA Clarity PPM

CA SDM change orders have unique internal (hidden) IDs and reference numbers that are passed to CA Clarity PPM. The reference number is used to determine the type of CA Clarity PPM object that is created, such as project, task, incident, or idea.

The following table contains errors that you may see during the integration of CA SDM and CA Clarity PPM and describes how CA Clarity PPM handles them.

Fault	Action	Resolution
Duplicate CA Clarity PPM Task ID	A log comment is entered in CA SDM Change Order Activity Log List.	One of the following actions should occur: ■ Create a CA SDM change order. ■ Change the duplicate CA Clarity PPM Task ID.
Project ID does not exist	A log comment is entered in CA SDM Change Order Activity Log List.	One of the following actions should occur: ■ If the CA Clarity PPM project exists, edit the CA SDM project CI to match the CA Clarity PPM Project ID. ■ If the CA Clarity PPM project does not exist, create the project. ■ Create a CA SDM change order.

Fault	Action	Resolution
Resource ID not found	A default resource ID is used for the Idea Owner (for CA Clarity PPM ideas) and Primary Contact (for incidents).	The CA Clarity PPM administrator user named CAIAdmin is used by default.
Duplicate Incident ID	A log comment is entered in CA SDM Change Order Activity Log List.	Create a CA SDM change order.
Duplicate Idea ID	A log comment is entered in CA SDM Change Order Activity Log List.	Create a CA SDM change order.

Consideration for Communicating Over SSL

Consider the following points when either the CA SDM server or the CA Clarity PPM server is configured to use secure socket layer (SSL) for communication:

- The SSL certificate must be trusted by the other server. For example, if CA SDM is configured to use SSL, the SSL certificate must be imported into the cacerts file or the keystore file that CA Clarity PPM uses on the CA Clarity PPM server. Similarly, if CA Clarity PPM is configured to use SSL, the CA Clarity PPM SSL certificate must be imported on the CA SDM server.

- If the CA Clarity PPM server is using SSL, the XOG Client install on the CA SDM server requires the following additional configuration:

  - Edit the test.properties file to change the sslenabled option to True.

  - Change the port number to the correct SSL port.

  Note: For more information about the .properties file, see the *XML Open Gateway Developer Guide for CA Clarity PPM*.

- If the CA SDM server uses SSL, you must edit the GEL Script Custom Parameters pages for all the CAI processes and verify that the correct SSL-based CA SDM URL is used.

Troubleshooting the Integration

You can try the following options to troubleshoot the issues with the integration:

- Verify CA SDM logs for any traces of errors invoking the Remote Reference script cai.bat (or cai.sh). Normally these files have the name stdlog.* in the $NX_ROOT/log directory (where $NX_ROOT represents the CA SDM installation directory). These logs normally provide clues about issues with granting permission to execute the script or attributes on the change order that the CA SDM Analyst may have missed.

- Verify that the test.properties file has the correct parameters for CA Clarity PPM (for example, URL, login/password). You can manually log in to the CA Clarity PPM URL with the same user name and password that is specified in the test.properties file. Verify that the login is successful.

- Verify that the CA SDM user name and password in the GEL Custom Script Parameters are valid. You can manually log in to the CA SDM URL with the same user name and password that is specified in the GEL Custom Script parameters for the CA Clarity PPM process that has errors.

- Try providing the complete host name of the CA Clarity PPM server. Use the complete host name instead of localhost or a vanity URL when you specify the CA Clarity PPM URL references to the attributes on the GEL Custom Parameters pages.

- Verify that JAVA_HOME is set properly, especially when it is installed to a directory with embedded spaces in the directory name (for example, Program Files). We recommend using the DOS 8.3 file naming convention in such a case. For example, Progra~1 usually refers to Program Files and progra~2 usually refers to Program Files (x86).

- If you are unable to edit the cai.bat file in the %XOG_HOME%\bin directory on the CA SDM server, edit the program and provide a hard code reference to JAVA_HOME and PATH as follows:

  ```
  set JAVA_HOME=C:\Progra~2\CA\SC\JRE\1.6.0_23
  set PATH=%JAVA_HOME%\bin;%PATH%
  echo cai.bat invoked
  and remove below string that does the JAVA_HOME check:
  if "%1" == "-javaHome" (
   set JAVA_HOME=%2
   shift
   shift
  )
  if "%JAVA_HOME%" == "" (
   echo.
   echo Warning: JAVA_HOME environment variable is not set.
   echo.
  ) else (
   set PATH=%JAVA_HOME%\bin;%PATH%
  )
  ```

  Save the file and retest now.

- If a CA Clarity PPM process is not working or results in errors, you can refer to the Initiated processes list in the CA Clarity PPM Administration tool. Click the Error icon in the Messages column for the failing process instance. Identify the step that caused the error. A brief message is displayed in the Exceptions column. To obtain more details, select the check box to the left of the step and click the Show Details button.

- Additional details can also be obtained from the bg-niku.log.

- CA Technologies Support can provide further help to troubleshoot the issues, if necessary.

Expanding the Solution to Include CA SCM

For details on expanding the CA Clarity PPM and CA SDM integration to include CA SCM, see the *Clarity Connector for CA Service Desk Manager & CA Software Change Manager for Distributed Product Guide.* You can find this guide in the CA Clarity PPM documentation bookshelf.

Chapter 5: CA Business Service Insight

CA Business Service Insight Integration

This chapter discusses how CA SDM Release 12.6 and CA Business Service Insight (CA BSI) Releases 7 and 8 can be configured to work together. The following key topics are covered:

- Integration from CA SDM to CA BSI
- Integration from CA BSI to CA SDM
- How the integration works
- Integration instructions

Overview of CA BSI

CA BSI, which was formerly known as CA Oblicore Guarantee, provides a top-down, contract-based approach to Service Level Management (SLM). The top-down approach is ideal for managing business value compared to the traditional bottom-up approach of aggregating technical metrics that can be virtually meaningless to the business. CA BSI lets you author, modify, and measure service level agreements, operational level agreements, and underpinning contracts. With CA BSI, you can improve service performance by creating accountability for the services that are provided and aligning them to contractual obligations. CA BSI provides a collaborative environment for monitoring and reporting service performance. CA BSI provides the following advantages:

- Improved productivity with automatic performance reporting
- Performance aligned with contracted obligations
- Reduced costs
- Increased customer satisfaction and corporate governance

Integration Details

CA BSI Event Generation from CA SDM

CA BSI interfaces with various data sources to collect real-time data about the service levels being provided to contract parties. These interfaces, which sit between the data sources and CA BSI, are called adapters. Adapters are modules that collect and format data into unified event structure. The adapters enable a full separation between the data sources layer and the contracts, business logic and reporting layers. This separation means that a data source can be changed without affecting the business logic in use.

CA BSI adapter technology is based on a high-performance XML engine. Each data source is accessed by a specified adapter. Two types of adapters exist, Text File adapters and SQL ODBC-based adapters. These adapter types allow accessibility to information that originates in various types of data sources, including the following sources:

- Databases
- Log files
- XML source files
- Excel files
- TCP/IP, SNMP and SMTP streams
- APIs and Web Services
- LDAP and IMS repositories
- Homegrown tools, and other utilities

Using a well-defined XML configuration, the adapter knows how to read all types of data forms, formats and structures, and passes only the relevant information to CA BSI.

The adapter modules are separate modules of CA BSI and can be deployed in a distributed fashion in the organization. The adapter communicates using the TCP/IP safe protocol. The adapter includes a restart/recovery mechanism and can handle problems such as network disruptions, missing data, duplicate data, corrupt data, data gaps, and data validation. Each adapter provides full data integrity and complete tracking and logging of all adapter messages.

Adapters contain two components:

- Generic component

  This component is the executable that runs the adapter. The generic component can be either a Text File adapter component or an ODBC-based, SQL adapter component. These components enable connecting to a data source and parsing it as a text file or executing various SQL queries against the component.

- Adapter configuration

  The adapter configuration can be created and managed using the Adapter Wizard interface. The wizard is a step-by-step GUI-based interface that takes the user through a series of forms. The forms specify and capture all relevant settings that are required for configuring and managing an adapter. Adapters that are created and managed by the wizard are known as configuration-managed adapters. Adapters with configurations that are created and maintained manually are known as configuration-unmanaged adapters.

  The adapter configuration is required to know where and how to connect, what to retrieve, and how to transform and translate the data into generic CA BSI transactions and events. The configuration file is an XML file that is organized into the following sections:

  - Connect and interface the data source.
  - Structure the input.
  - Structure the output.
  - Communicate with CA BSI to send and receive information.

CA SDM has data that the CA BSI adapters can use to generate events from the CA SDM service operation processes, such as request fulfillment, incident, and problem management. CA SDM also generates data from its service transition processes such as change, release, and service asset and configuration management. CA BSI uses this data to create events, which are then used as measures to determine service levels.

Before you configure the integration, you must understand the structure of the event:

- CA BSI is event-driven.
- Events are generated by the adapter.
- Events are driven by business logic requirements.

  Which events are necessary to be able to do the calculations?

- Extra data to be contained within events.

  What is necessary for calculations?

  Provide hints to the managed data repository (MDR) for further research (for example, a CA SDM ticket ID).

  Do not replicate MDR in CA BSI (for performance reasons).

- When designing Adapters, consider the following factors:

  Determine load and performance impact.

  Properly prefilter data.

  Implement event singularity.

  Allow for data changes to happen through the MDR and update CA BSI.

  Use translation tables for both event and resource model.

Configure the Integration from CA SDM

You can collect CA SDM data that CA BSI will analyze using a text file or SQL queries. This section provides the instructions to generate events using both methods.

Configure a Text Adapter

A text adapter uses CSV files as inputs from CA SDM. You can generate a CSV file from CA SDM using one of the following methods:

- CA Business Intelligence report
- pdm_extract utility

Extract Data to CSV Files Using CA Business Intelligence

CA Business Intelligence is a powerful reporting tool that is provided with CA SDM. You can create a report in CA Business Intelligence, schedule the report to collect data at regular intervals, and save the data to the CSV format.

Follow these steps:

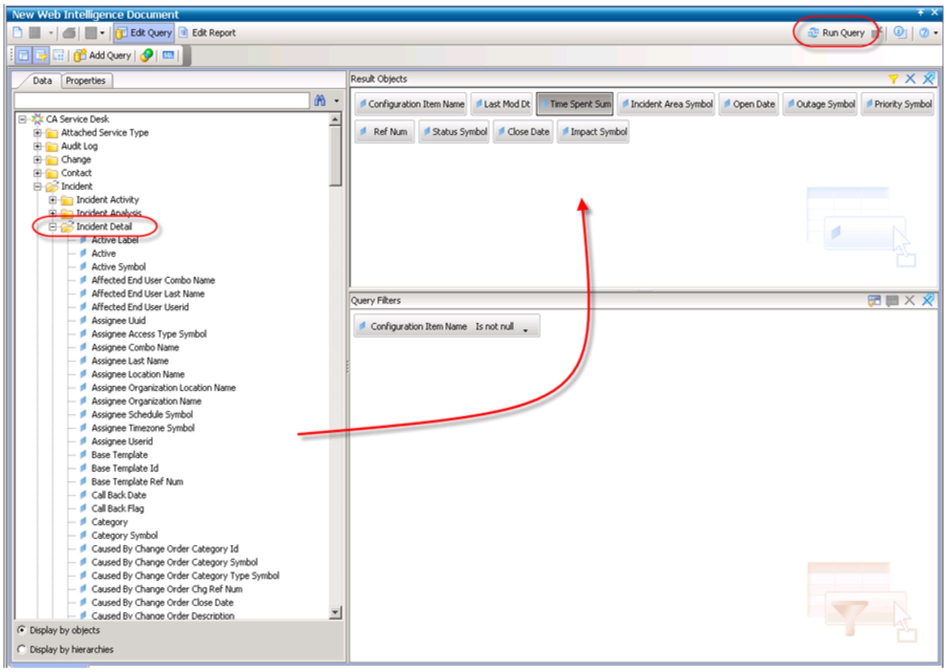
1. Open CA Business Intelligence Infoview and create a web intelligence report containing CA SDM fields that you need to use in CA BSI. You can use any CA SDM record, such as incident, request, problem, changes, issues, or knowledge.

2. Include a resource, timestamp, and the required values for SLM calculation in the report.

3. Select the fields and drag them to the report area.

   Note: This method does not require a thorough knowledge of CA SDM schema because it deals with the object layer.

   The following example includes a filter to help ensure that the extracted data has a CI associated with it:



Result Objects

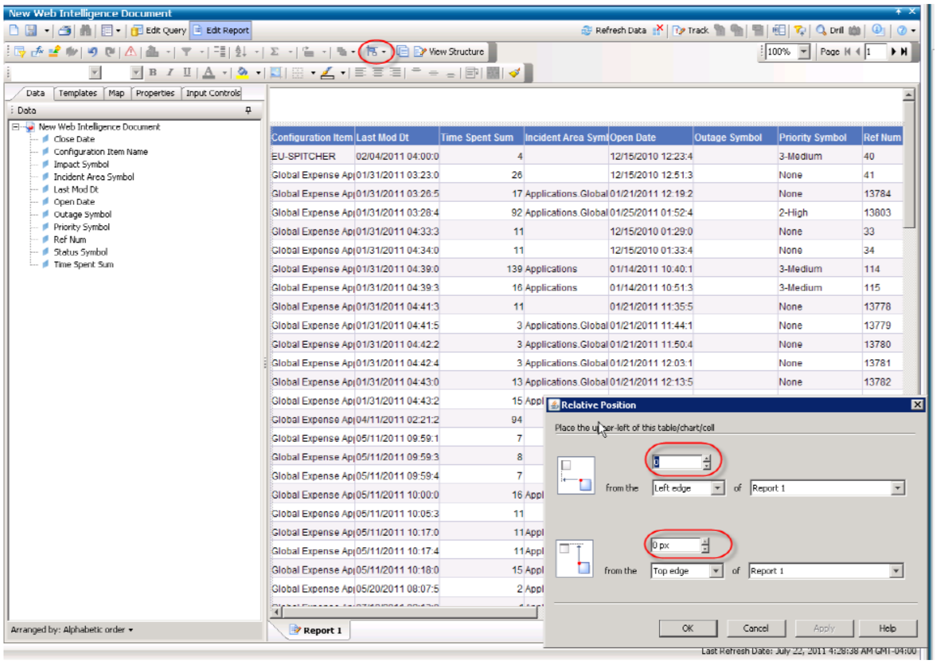
Configuration Item Name | Last Mod Dt | Time Spent Sum | Incident Area Symbol | Open Date | Outage Symbol | Priority Symbol | Ref Num | Status Symbol | Close Date | Impact Symbol

Query Filters

Configuration Item Name Is not null

4. Click Run Query.

5. Suppress the report title and verify that the relative position of the report screen is set to 0.



Configuration Item	Last Mod Dt	Time Spent Sum	Incident Area Syml	Open Date	Outage Symbol	Priority Symbol	Ref Num
EU-SPITCHER	02/04/2011 04:00:0	4		12/15/2010 12:23:4		3-Medium	40
Global Expense Ap	01/31/2011 03:23:0	26		12/15/2010 12:51:3		None	41
Global Expense Ap	01/31/2011 03:26:5	17	Applications.Global	01/21/2011 12:19:2		None	13784
Global Expense Ap	01/31/2011 03:28:4	92	Applications.Global	01/25/2011 01:52:4		2-High	13803
Global Expense Ap	01/31/2011 04:33:3	11		12/15/2010 01:29:0		None	33
Global Expense Ap	01/31/2011 04:34:0	11		12/15/2010 01:33:4		None	34
Global Expense Ap	01/31/2011 04:39:0	139	Applications	01/14/2011 10:40:1		3-Medium	114
Global Expense Ap	01/31/2011 04:39:3	16	Applications	01/14/2011 10:51:3		3-Medium	115
Global Expense Ap	01/31/2011 04:41:3	11		01/21/2011 11:35:5		None	13778
Global Expense Ap	01/31/2011 04:41:5	3	Applications.Global	01/21/2011 11:44:1		None	13779
Global Expense Ap	01/31/2011 04:42:2	3	Applications.Global	01/21/2011 11:50:4		None	13780
Global Expense Ap	01/31/2011 04:42:4	3	Applications.Global	01/21/2011 12:03:1		None	13781
Global Expense Ap	01/31/2011 04:43:0	13	Applications.Global	01/21/2011 12:13:5		None	13782
Global Expense Ap	01/31/2011 04:43:2	15	Appl				
Global Expense Ap	04/11/2011 02:21:2	94					
Global Expense Ap	05/11/2011 09:59:1	7					
Global Expense Ap	05/11/2011 09:59:3	8					
Global Expense Ap	05/11/2011 09:59:4	7					
Global Expense Ap	05/11/2011 10:00:0	16	Appl				
Global Expense Ap	05/11/2011 10:05:3	11					
Global Expense Ap	05/11/2011 10:17:0	11	Appl				
Global Expense Ap	05/11/2011 10:17:4	11	Appl				
Global Expense Ap	05/11/2011 10:18:0	15	Appl				
Global Expense Ap	05/20/2011 08:07:5	2	Appl				

Relative Position

Place the upper-left of this table/chart/cell

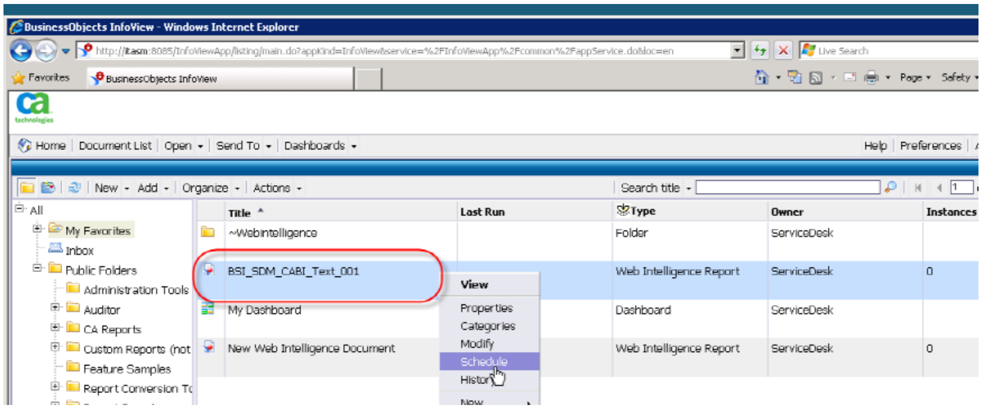
0 from the Left edge of Report 1

0 px from the Top edge of Report 1

Last Refresh Date: July 22, 2011 4:28:38 AM GMT-04:00

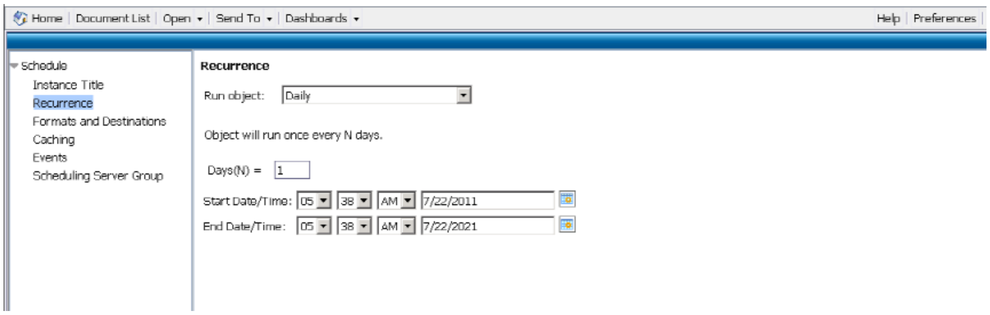
6. Save the report and use the CA Business Intelligence Scheduler to schedule the report to run as needed using the following steps:

   a. Right-click the report and select Schedule.



Title	Last Run	Type	Owner	Instances
~Webintelligence		Folder	ServiceDesk	
BSI_SDM_CABI_Text_001		Web Intelligence Report	ServiceDesk	0
My Dashboard		Dashboard	ServiceDesk	
New Web Intelligence Document		Web Intelligence Report	ServiceDesk	0

b. Specify the Recurrence.



Recurrence

Run object: Daily

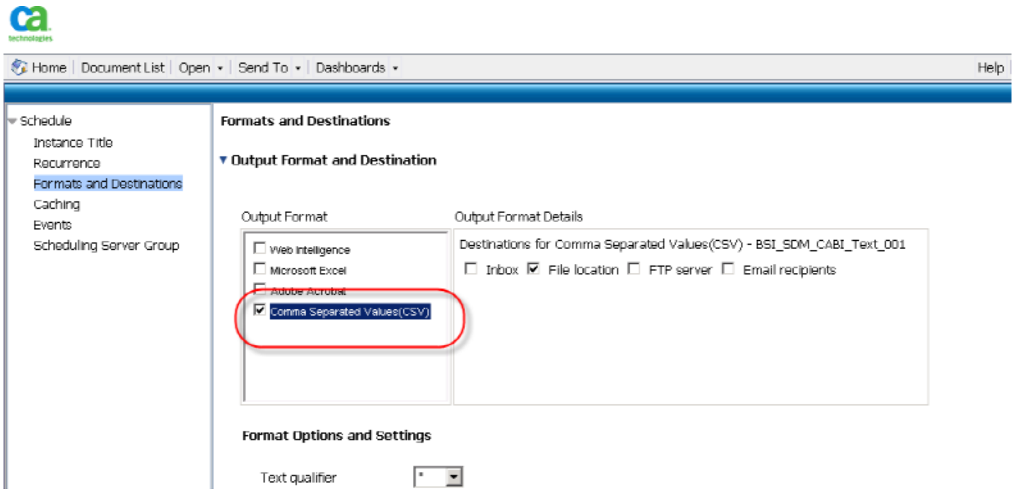
Object will run once every N days.

Days(N) = 1

Start Date/Time: 05 38 AM 7/22/2011

End Date/Time: 05 38 AM 7/22/2021

c. Select the output format as Comma Separated Values (CSV) and select the destination as shown in the following example.



Formats and Destinations

Output Format and Destination

Output Format

☐ Web Intelligence
☐ Microsoft Excel
☐ Adobe Acrobat
☑ Comma Separated Values(CSV)

Output Format Details

Destinations for Comma Separated Values(CSV) - BSI_SDM_CABI_Text_001

☐ Inbox ☑ File location ☐ FTP server ☐ Email recipients

Format Options and Settings

Text qualifier "

The report runs at the scheduled time and saves the report to CSV format.

Extract Data to CSV Files Using pdm_extract

Use the pdm_extract utility to extract data at the schema level. The utility lets you save the data to a CSV file. The CSV file is then passed to the adapter.

Note: You must have a thorough knowledge of the data model to use the pdm_extract utility.

Follow these steps:

1. Open a text editor and type the following command:

   ```
   pdm_extract -f SQL_Query -c -u > filename.csv
   ```

   SQL_Query

   Defines the SQL query with the exact fields that you want to extract.

   -c

   Saves the data in a CSV file.

   -u

   Indicates no headers.

   The following command example shows how you can extract CI event data, such as timestamp, CI name, and time that is spent on resolving the CI.

   ```
   pdm_extract -f "SELECT Call_Req.last_mod_dt ca_owned_resource.resource_name,
   Call_Req.time_spent_sum FROM Call_Req, ca_owned_resource WHERE (Call_Req.affected_rc =
   ca_owned_resource.id)" -c -u > SDM_pdm_extract_file.csv
   ```

   Note: You can include additional fields, if necessary.

2. Save the file as a batch file.

3. Schedule the batch file to run at a specific interval.

   You can schedule it to run every day, week, or month depending on the Service Level Management requirements.

The following excerpt shows an example of the generated CSV file:

```
"07/19/2011 13:41:18","USNYAPP01","0"
"07/19/2011 13:41:18","Global Expense System","0"
"07/19/2011 11:41:16","USCAX10_NetApp","0"
"07/19/2011 15:41:15","Quoting Service","0"
"07/19/2011 13:41:13","USCAX10 Router1","0"
"07/19/2011 13:41:11","USCAX10_Switch1","0"
"07/19/2011 22:31:46","Global Expense System","1"
"07/19/2011 11:57:41","USNYAPP01","0"
"07/19/2011 22:32:59","Global Expense System","17"
"07/19/2011 09:57:34","USCAX10_NetApp","0"
"07/19/2011 13:57:34","Quoting Service","0"
"07/19/2011 11:57:31","USCAX10 Router1","0"
"07/19/2011 11:57:31","USCAX10_Switch1","0"
"07/19/2011 11:57:29","Global Expense System","0"
"07/18/2011 14:13:04","Global Expense Application","1"
"07/06/2011 10:06:34","Global Expense System","251"
…
```

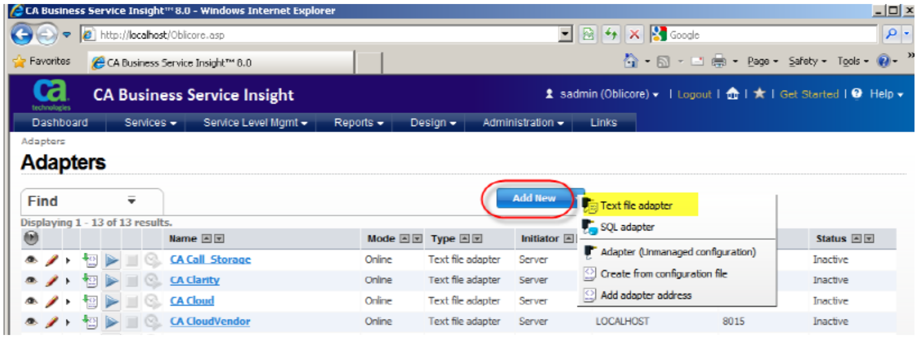
The first column or timestamp contains the date when the ticket was last modified. The second column contains the name of the CI associated with the ticket. The third column indicates the total time that was spent on the ticket. The resulting data is stored in a CSV-formatted file when the batch file is run.

Create a Text Adapter Event

Follow these steps:

1. Copy the CSV file to the C:\data folder on the CA BSI server and also on the computer where the adapter is stored.
2. Verify that both of the Adapter Services are started.
3. Log in to the CA BSI console and click Design, Data Acquisition, Adapter Time Format.
4. Verify that the time format matches the timestamp format in the CSV file.
5. Click Design, Data Acquisition, Adapters.

6. Click Add New and select Text file Adapter.


CA Business Service Insight™ 8.0 - Windows Internet Explorer
http://localhost/Oblicore.asp
CA Business Service Insight
sadmin (Oblicore) | Logout | Get Started | Help
Dashboard
Services
Service Level Mgmt
Reports
Design
Administration
Links
Adapters
Find
Add New
Text file adapter
SQL adapter
Adapter (Unmanaged configuration)
Create from configuration file
Add adapter address

Adapters

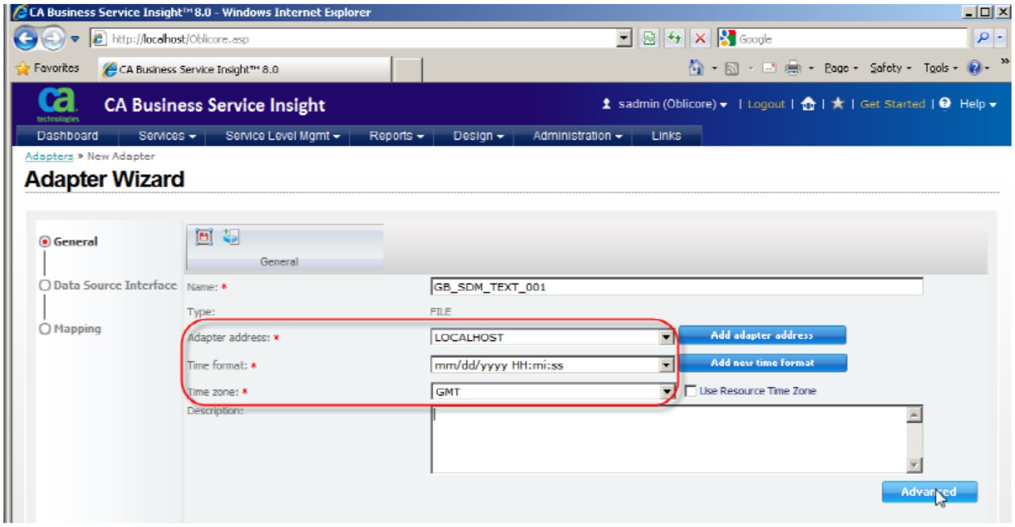
Displaying 1 - 13 of 13 results.

Name	Mode	Type	Initiator			Status
CA Call_Storage	Online	Text file adapter	Server			Inactive
CA Clarity	Online	Text file adapter	Server			Inactive
CA Cloud	Online	Text file adapter	Server			Inactive
CA CloudVendor	Online	Text file adapter	Server	LOCALHOST	8015	Inactive

The Adapter Wizard opens.

7. Provide the following information in the General section.

   - Name of the adapter.
   - Adapter address. The address must point to the server where the adapter is running. Depending on where the adapter is running, you either specify the address of the CA SDM server or the address of the BSI server.
   - Time format that matches the time format of your time stamp (the time_spent_sum field).

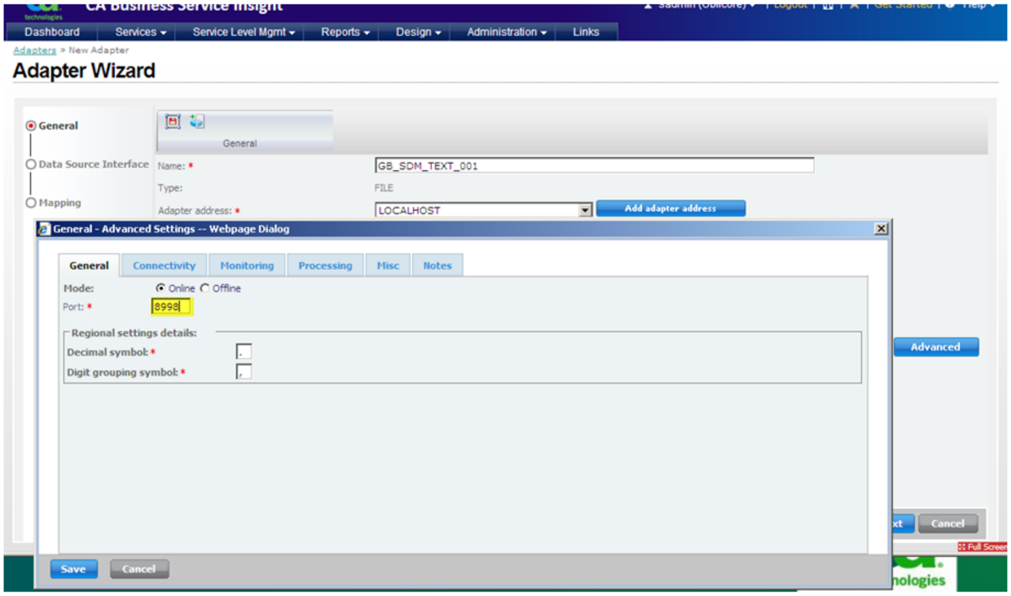


Adapter Wizard

Name: *	GB_SDM_TEXT_001
Type:	FILE
Adapter address: *	LOCALHOST
Time format: *	mm/dd/yyyy HH:mi:ss
Time zone: *	GMT ☐ Use Resource Time Zone
Description:	

8. Click Advanced and complete the details on each tab, based on your requirements.

   Note: On the General tab, verify that the TCP port that is used by the adapter is not used by any other process.



Adapter Wizard

Name: * GB_SDM_TEXT_001

Type: FILE

Adapter address: * LOCALHOST

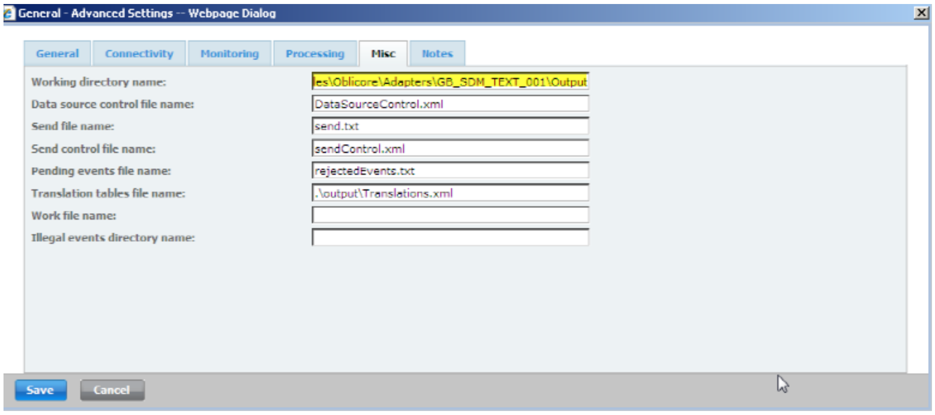
Mode: ● Online ○ Offline

Port: * 8998

Regional settings details:

Decimal symbol: * .

Digit grouping symbol: * ,



Working directory name: es\Oblicore\Adapters\GB_SDM_TEXT_001\Output

Data source control file name: DataSourceControl.xml

Send file name: send.txt

Send control file name: sendControl.xml

Pending events file name: rejectedEvents.txt

Translation tables file name: .\output\Translations.xml

Work file name:

Illegal events directory name:

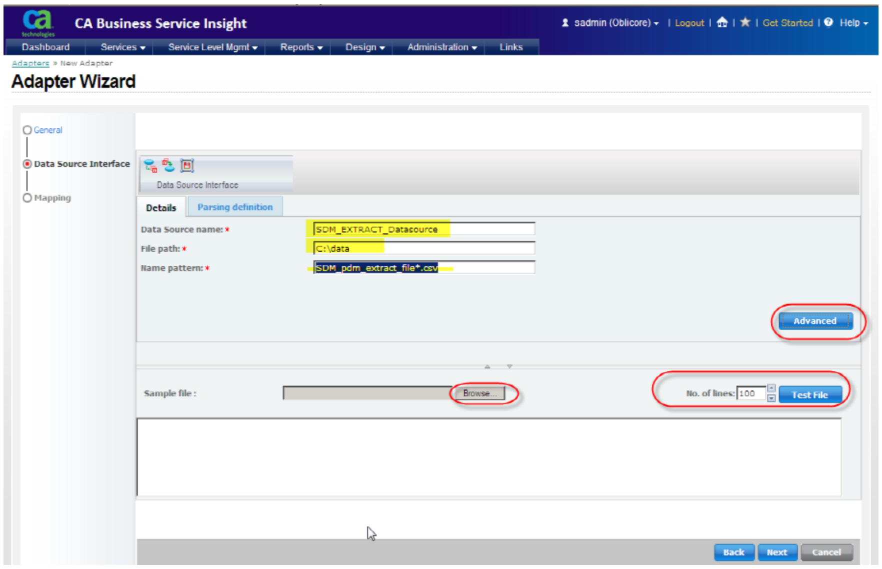
9. Click Save after you complete all tabs.

10. Click Next on the Adapter Wizard.

    The Data Source Interface definition page opens.

11. Specify the name of your data source, the path to the file you copied, and the name pattern.

12. Click Advanced to specify parameters, such as initial file name, and parsing definitions.


CA Business Service Insight
sadmin (Oblicore) | Logout | Get Started | Help
Dashboard | Services | Service Level Mgmt | Reports | Design | Administration | Links
Adapters » New Adapter
General
Data Source Interface
Mapping
Data Source Interface
Details
Parsing definition
Advanced
Browse...
Test File
Back
Next
Cancel

Adapter Wizard

Data Source name: * SDM_EXTRACT_Datasource

File path: * C:\data

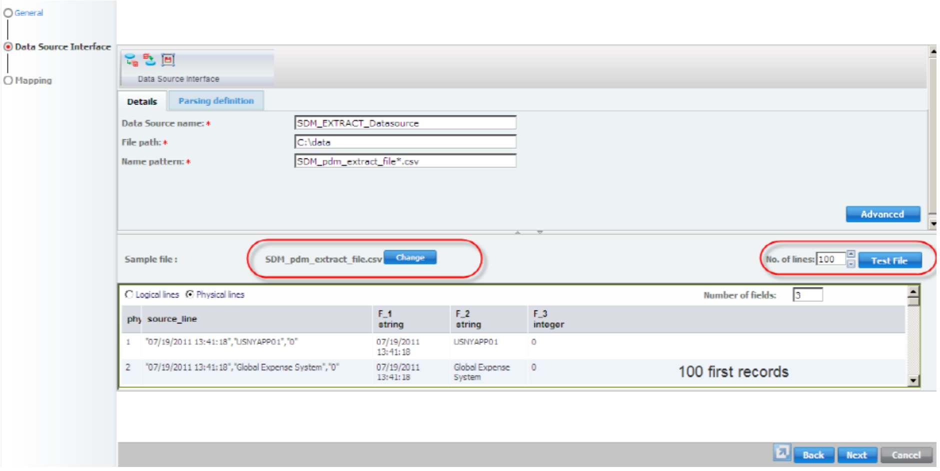
Name pattern: * SDM_pdm_extract_file*.csv

Sample file :

No. of lines: 100

13. Click Save to save the changes and return to the Adapter Wizard.

14. In the bottom pane of the Data Source Interface page, select the file and click Test File.



Data Source name: * SDM_EXTRACT_Datasource

File path: * C:\data

Name pattern: * SDM_pdm_extract_file*.csv

Sample file : SDM_pdm_extract_file.csv

No. of lines: 100

○ Logical lines ● Physical lines

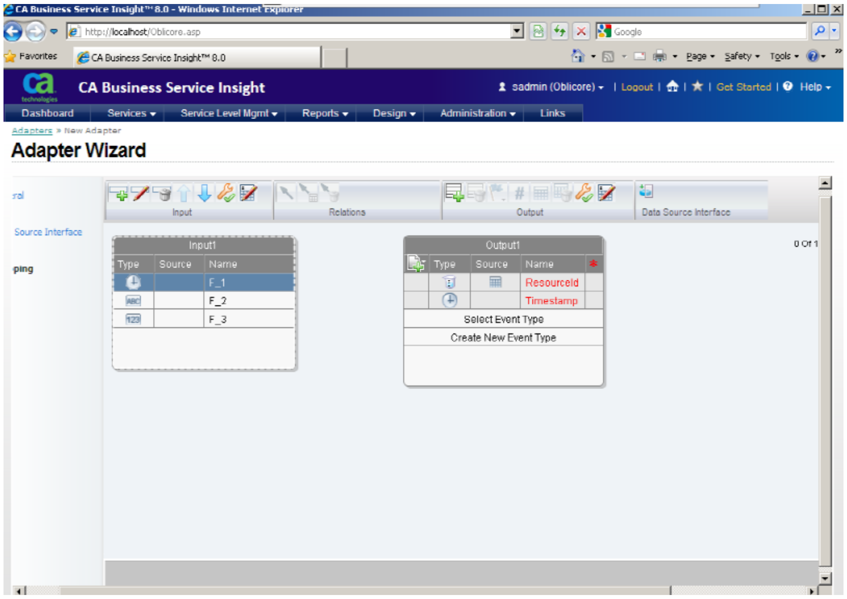
Number of fields: 3

phy	source_line	F_1 string	F_2 string	F_3 integer
1	"07/19/2011 13:41:18","USNYAPP01","0"	07/19/2011 13:41:18	USNYAPP01	0
2	"07/19/2011 13:41:18","Global Expense System","0"	07/19/2011 13:41:18	Global Expense System	0

100 first records

15. If the test is successful, click Next.

    The Mapping page opens.



Adapter Wizard

Input1

Type	Source	Name
		F_1
ABC		F_2
123		F_3

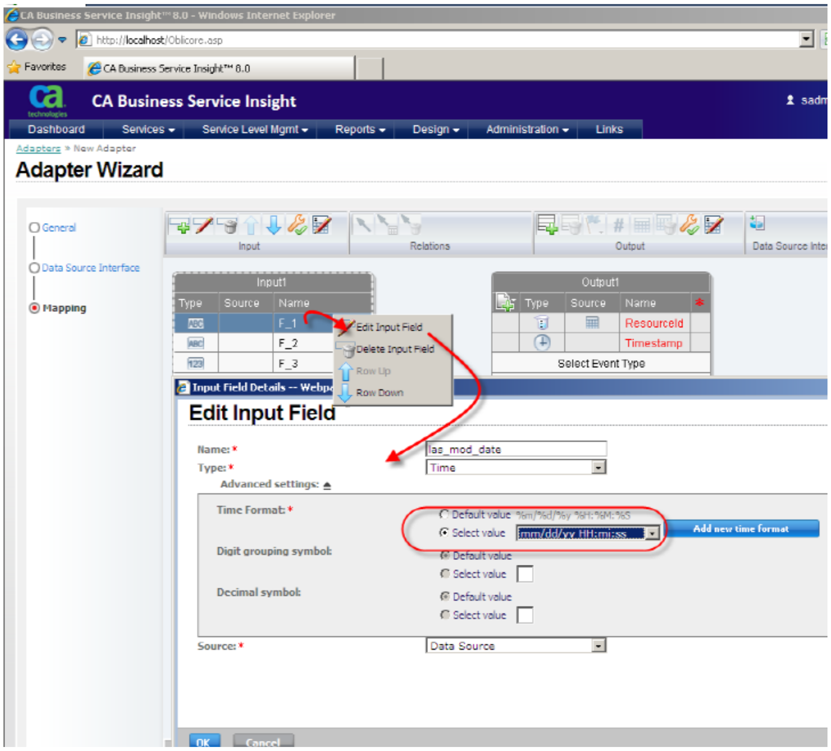
Output1

Type	Source	Name	*
		ResourceId	
		Timestamp	

Select Event Type

Create New Event Type

16. Right-click the input fields and provide the name and format, as shown in the following example:



Edit Input Field

Name: * las_mod_date

Type: * Time

Advanced settings:

Time Format: * ○ Default value %m/%d/%y %H:%M:%S ● Select value mm/dd/yy HH:mi:ss

Digit grouping symbol: ● Default value ○ Select value □

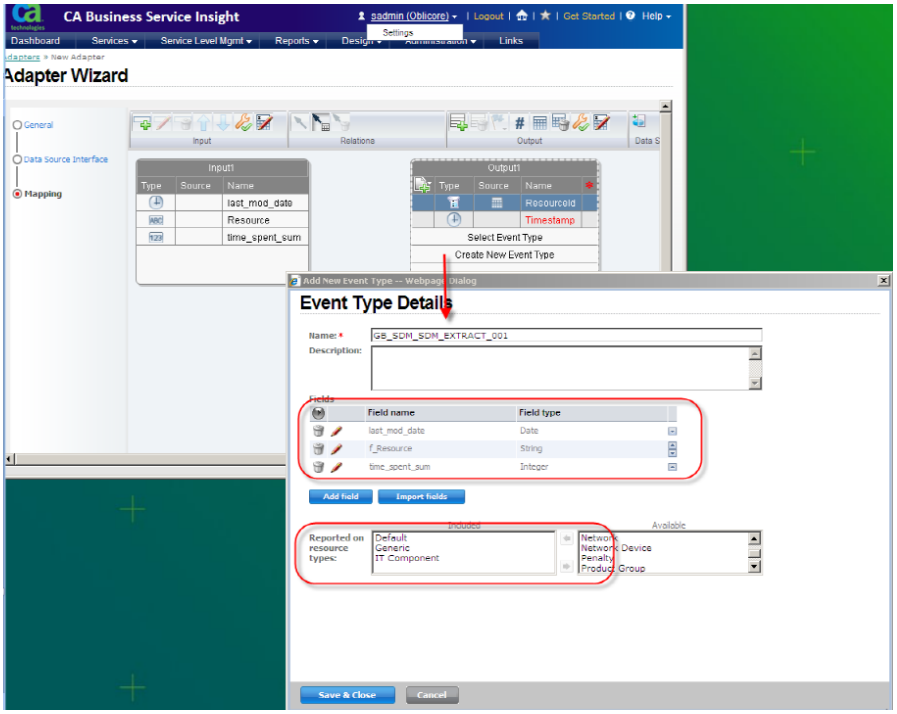
Decimal symbol: ● Default value ○ Select value □

Source: * Data Source

Note: If you want to modify the time format, double-click the Advanced settings arrow to select the time format.

17. On the output table, click Create New Event Type to create an event type as shown in the following example.

    The Event Type Details dialog opens with the default values.



Type	Source	Name
		last_mod_date
		Resource
		time_spent_sum

Type	Source	Name
		ResourceId
		Timestamp

Event Type Details

Name: * GB_SDM_SDM_EXTRACT_001

Description:

Fields

Field name	Field type
last_mod_date	Date
f_Resource	String
time_spent_sum	Integer

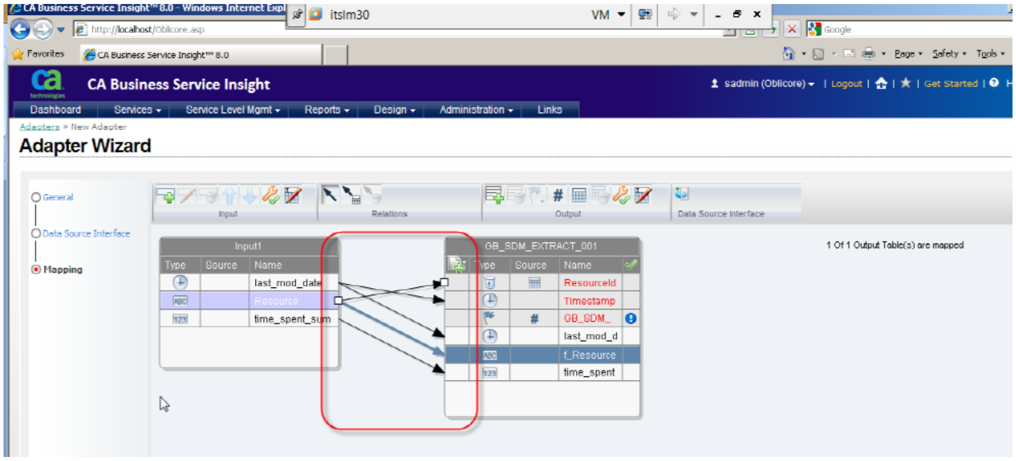
Reported on resource types:

Included: Default, Generic, IT Component

Available: Network, Network Device, Penalty, Product Group

18. Click Save and then Close.

19. On the Mapping page, drag the input fields to the appropriate output fields and click Finish when you are done.


CA Business Service Insight™ 8.0 - Windows Internet Expl
itslm30
VM
http://localhost/Oblicore.asp
Google
Favorites
CA Business Service Insight™ 8.0
Page
Safety
Tools
CA Business Service Insight
sadmin (Oblicore) | Logout | Get Started
Dashboard | Services | Service Level Mgmt | Reports | Design | Administration | Links
Adapters » New Adapter
Adapter Wizard
General
Data Source Interface
Mapping
Input
Relations
Output
Data Source Interface
1 Of 1 Output Table(s) are mapped

Input1

Type	Source	Name
		last_mod_date
		Resource
		time_spent_sum

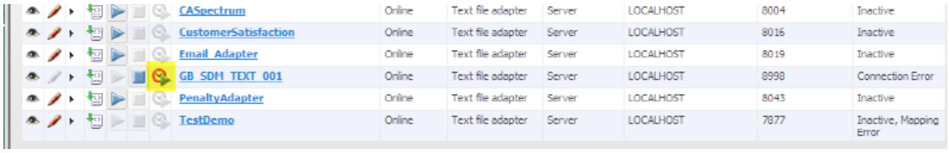
GB_SDM_EXTRACT_001

Type	Source	Name
		ResourceId
		Timestamp
	#	GB_SDM_
		last_mod_d
		f_Resource
		time_spent

The new adapter is now added to the Adapter list.

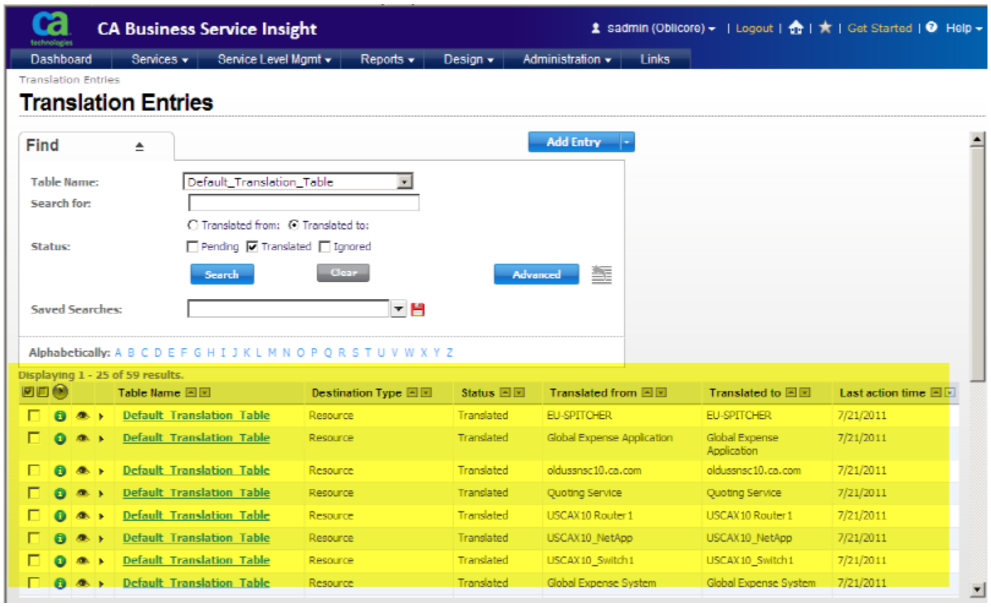
20. Click the blue triangle icon to start the adapter.

21. Click Refresh in the bottom left of the page and click the watch-and-triangle icon, as highlighted in the following example:



CASpectrum	Online	Text file adapter	Server	LOCALHOST	8004	Inactive
CustomerSatisfaction	Online	Text file adapter	Server	LOCALHOST	8016	Inactive
Email_Adapter	Online	Text file adapter	Server	LOCALHOST	8019	Inactive
GB_SDM_TEXT_001	Online	Text file adapter	Server	LOCALHOST	8998	Connection Error
PenaltyAdapter	Online	Text file adapter	Server	LOCALHOST	8043	Inactive
TestDemo	Online	Text file adapter	Server	LOCALHOST	7877	Inactive, Mapping Error

This example uses the default translation table, which automatically creates resources in CA BSI. You can use your translation table. The following example shows the resources from CA SDM translated as resources in CA BSI.


CA Business Service Insight
sadmin (Oblicore) | Logout | Get Started | Help
Dashboard
Services
Service Level Mgmt
Reports
Design
Administration
Links
Translation Entries
Find
Add Entry
Search
Clear
Advanced
Alphabetically: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Translation Entries

Table Name: Default_Translation_Table

Search for:

○ Translated from: ● Translated to:

Status: ☐ Pending ☑ Translated ☐ Ignored

Saved Searches:

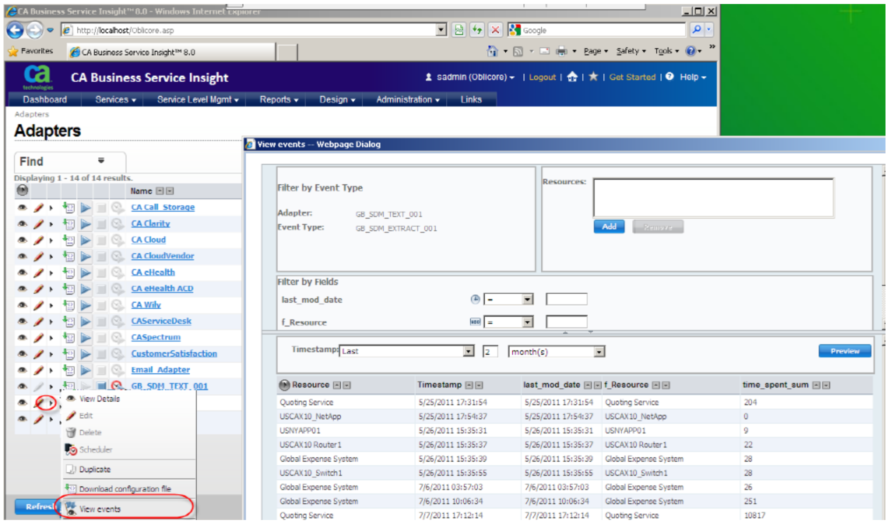
Displaying 1 - 25 of 59 results.

Table Name	Destination Type	Status	Translated from	Translated to	Last action time
Default_Translation_Table	Resource	Translated	EU-SPITCHER	EU-SPITCHER	7/21/2011
Default_Translation_Table	Resource	Translated	Global Expense Application	Global Expense Application	7/21/2011
Default_Translation_Table	Resource	Translated	oldussnsc10.ca.com	oldussnsc10.ca.com	7/21/2011
Default_Translation_Table	Resource	Translated	Quoting Service	Quoting Service	7/21/2011
Default_Translation_Table	Resource	Translated	USCAX10 Router1	USCAX10 Router1	7/21/2011
Default_Translation_Table	Resource	Translated	USCAX10_NetApp	USCAX10_NetApp	7/21/2011
Default_Translation_Table	Resource	Translated	USCAX10_Switch1	USCAX10_Switch1	7/21/2011
Default_Translation_Table	Resource	Translated	Global Expense System	Global Expense System	7/21/2011

View Events Generated by the Adapter

You can view the events using one of the following methods:

- Click the black triangle and select View events.



Filter by Event Type

Adapter: GB_SDM_TEXT_001
Event Type: GB_SDM_EXTRACT_001

Resources:

Filter by Fields

last_mod_date =

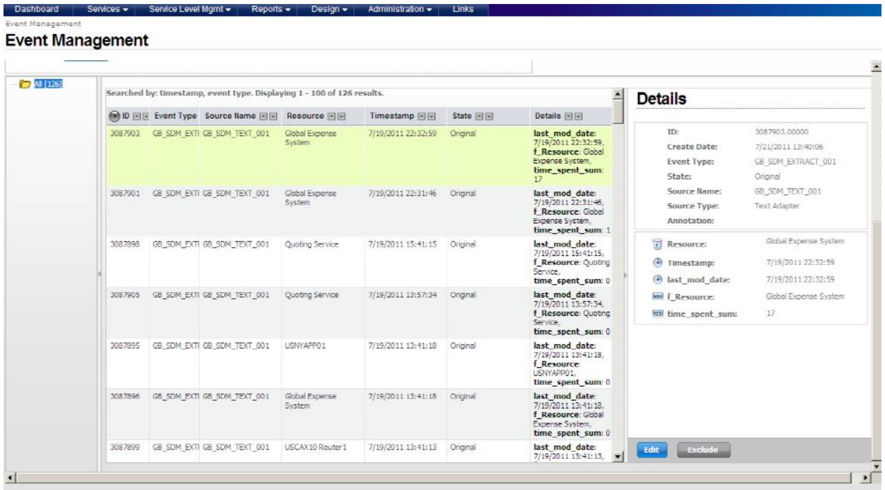
f_Resource =

Timestamp: Last 2 month(s)

Resource	Timestamp	last_mod_date	f_Resource	time_spent_sum
Quoting Service	5/25/2011 17:31:54	5/25/2011 17:31:54	Quoting Service	204
USCAX10_NetApp	5/25/2011 17:54:37	5/25/2011 17:54:37	USCAX10_NetApp	0
USNYAPP01	5/26/2011 15:35:31	5/26/2011 15:35:31	USNYAPP01	9
USCAX10 Router1	5/26/2011 15:35:37	5/26/2011 15:35:37	USCAX10 Router1	22
Global Expense System	5/26/2011 15:35:39	5/26/2011 15:35:39	Global Expense System	28
USCAX10_Switch1	5/26/2011 15:35:55	5/26/2011 15:35:55	USCAX10_Switch1	28
Global Expense System	7/6/2011 03:57:03	7/6/2011 03:57:03	Global Expense System	26
Global Expense System	7/6/2011 10:06:34	7/6/2011 10:06:34	Global Expense System	251
Quoting Service	7/7/2011 17:12:14	7/7/2011 17:12:14	Quoting Service	10817

The event list is displayed. You can filter the events based on event type criteria.

- Click Design, Data Acquisition, Event Management.

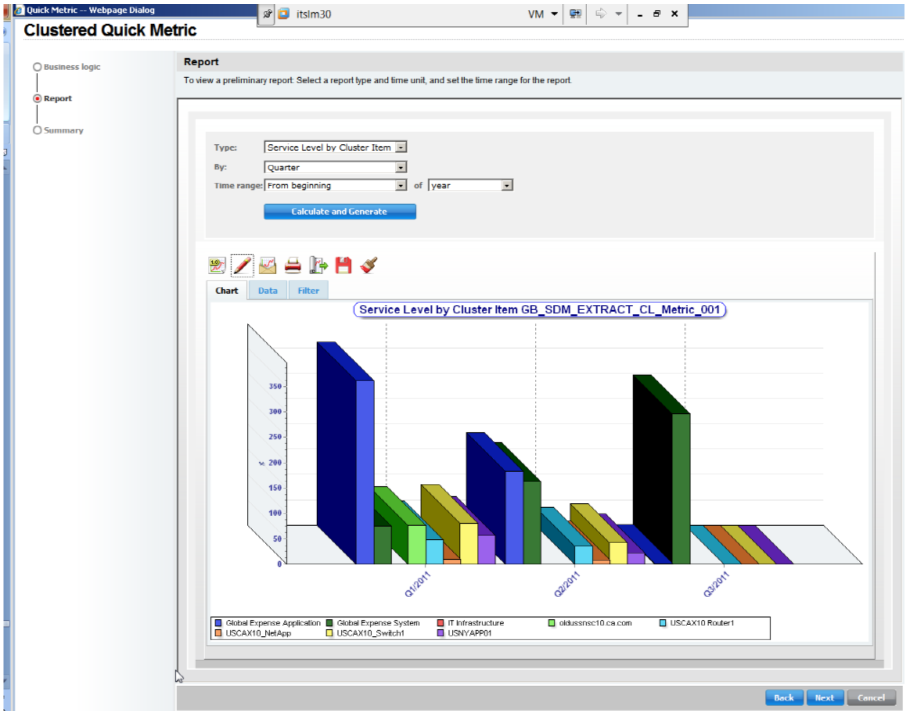


Searched by: timestamp, event type. Displaying 1 - 100 of 126 results.

ID	Event Type	Source Name	Resource	Timestamp	State	Details
3087903	GB_SDM_EXTI	GB_SDM_TEXT_001	Global Expense System	7/19/2011 22:32:59	Original	**last_mod_date**: 7/19/2011 22:32:59, **f_Resource**: Global Expense System, **time_spent_sum**: 17
3087901	GB_SDM_EXTI	GB_SDM_TEXT_001	Global Expense System	7/19/2011 22:31:46	Original	**last_mod_date**: 7/19/2011 22:31:46, **f_Resource**: Global Expense System, **time_spent_sum**: 1
3087898	GB_SDM_EXTI	GB_SDM_TEXT_001	Quoting Service	7/19/2011 15:41:15	Original	**last_mod_date**: 7/19/2011 15:41:15, **f_Resource**: Quoting Service, **time_spent_sum**: 0
3087905	GB_SDM_EXTI	GB_SDM_TEXT_001	Quoting Service	7/19/2011 13:57:34	Original	**last_mod_date**: 7/19/2011 13:57:34, **f_Resource**: Quoting Service, **time_spent_sum**: 0
3087895	GB_SDM_EXTI	GB_SDM_TEXT_001	USNYAPP01	7/19/2011 13:41:18	Original	**last_mod_date**: 7/19/2011 13:41:18, **f_Resource**: USNYAPP01, **time_spent_sum**: 0
3087896	GB_SDM_EXTI	GB_SDM_TEXT_001	Global Expense System	7/19/2011 13:41:18	Original	**last_mod_date**: 7/19/2011 13:41:18, **f_Resource**: Global Expense System, **time_spent_sum**: 0
3087899	GB_SDM_EXTI	GB_SDM_TEXT_001	USCAX10 Router1	7/19/2011 13:41:13	Original	**last_mod_date**: 7/19/2011 13:41:13,

ID:	3087903.00000
Create Date:	7/21/2011 13:40:06
Event Type:	GB_SDM_EXTRACT_001
State:	Original
Source Name:	GB_SDM_TEXT_001
Source Type:	Text Adapter
Annotation:	
Resource:	Global Expense System
Timestamp:	7/19/2011 22:32:59
last_mod_date:	7/19/2011 22:32:59
f_Resource:	Global Expense System
time_spent_sum:	17

Note: You can also create a quick metric or quick clustered metric from the adapter list. The following example shows a clustered metric.



Clustered Quick Metric

Report

To view a preliminary report: Select a report type and time unit, and set the time range for the report.

Type: Service Level by Cluster Item

By: Quarter

Time range: From beginning of year

Configure a SQL Adapter

You can use a SQL adapter to collect data directly from the CA SDM MDB, instead of using CA Business Intelligence or the pdm_extract utility. If you use this method, you must have a thorough knowledge of the CA SDM schema.

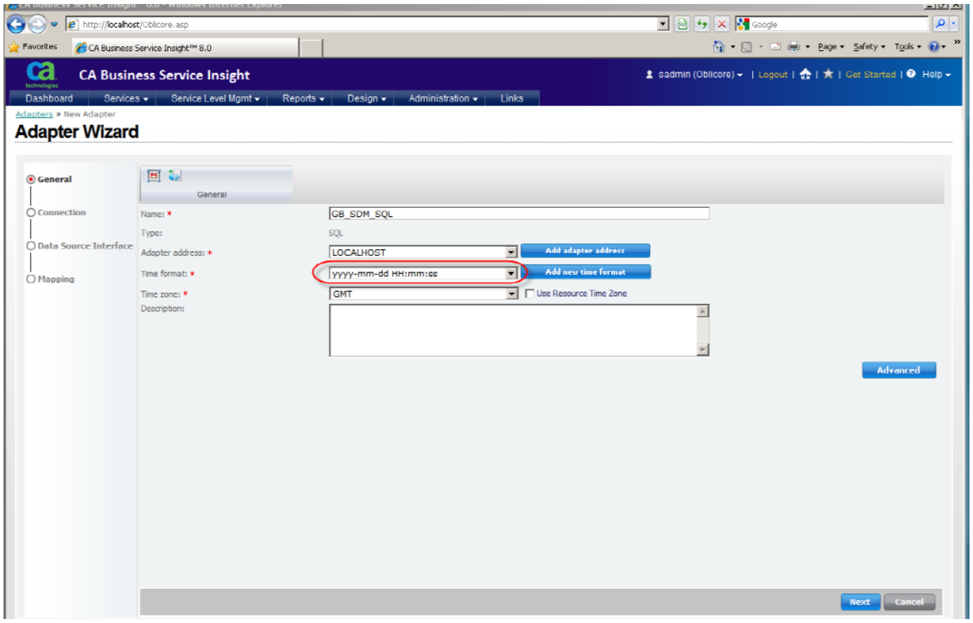
Follow these steps:

1. Log in to CA BSI and click Design, Data Acquisition, Adapters.
2. Click Add New and select SQL Adapter.

   The Adapter Wizard opens.

3. On the General page, specify a name for the adapter and the correct time format.

4. Click Advanced and specify the connectivity and monitoring parameters for this adapter.



Adapter Wizard

Name: * GB_SDM_SQL

Type: SQL

Adapter address: * LOCALHOST

Time format: * yyyy-mm-dd HH:mm:ss

Time zone: * GMT ☐ Use Resource Time Zone

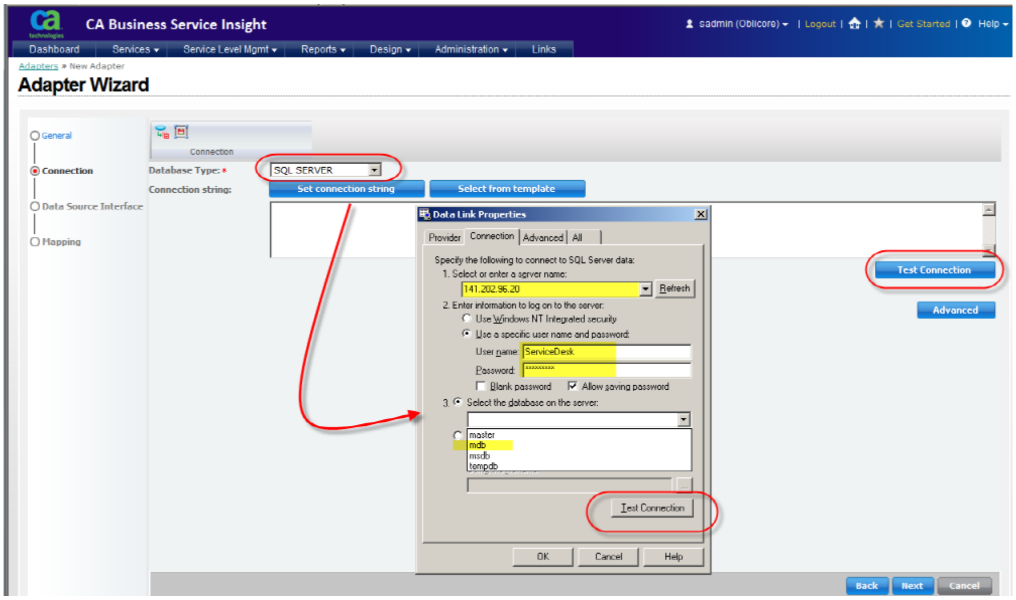
Description:

5. Click Next and specify the following details:

   a. Select CA SDM for the database type.

   b. Click Set connection String, and specify connection parameters, such as server address, username and password, and database in the Data Link Properties dialog.

c. Click Test Connection to test the connection to the server.



Adapter Wizard

Connection

Database Type: * SQL SERVER

Connection string:

Data Link Properties

Provider | Connection | Advanced | All

Specify the following to connect to SQL Server data:

1. Select or enter a server name: 141.202.96.20

2. Enter information to log on to the server:

○ Use Windows NT Integrated security

● Use a specific user name and password:

User name: ServiceDesk

Password: **********

□ Blank password ☑ Allow saving password

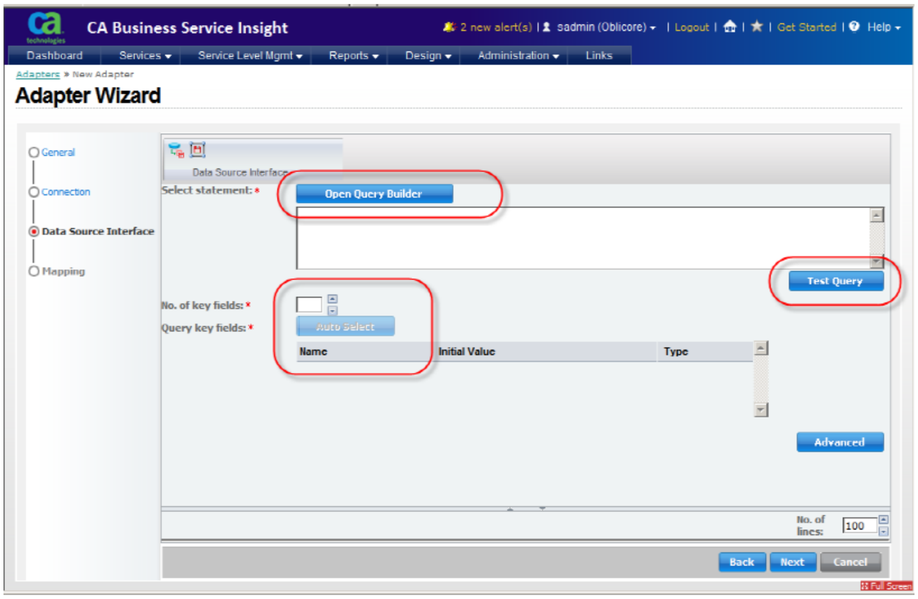
3. ● Select the database on the server:

master
mdb
msdb
tempdb

Note: You can use the adapter templates to avoid specifying these parameters each time.

6. Click Next.

7. Click Open Query Builder to specify the data that you want the adapter to collect.



Adapter Wizard

Data Source Interface

Select statement: *

No. of key fields: *

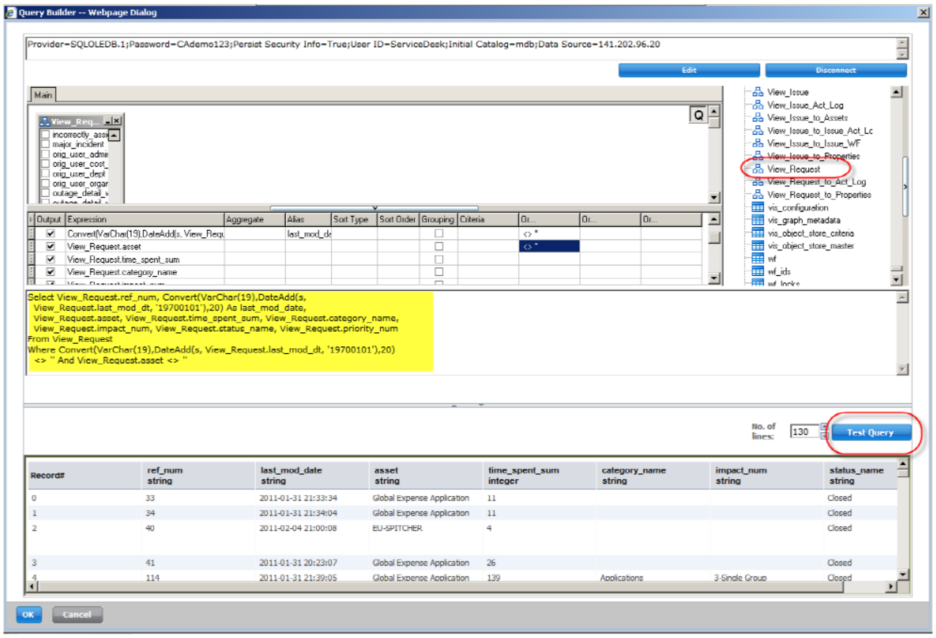
Query key fields: *

Name	Initial Value	Type

No. of lines: 100

The Query Builder dialog opens.

In the following example, the View_Request view is used. All CA SDM tables are accessible by the query builder. The highlighted part in the middle of the example represents the query that was generated by the query builder. The bottom pane shows the result of the Test Query operation.



```
Provider=SQLOLEDB.1;Password=CAdemo123;Persist Security Info=True;User ID=ServiceDesk;Initial Catalog=mdb;Data Source=141.202.96.20
```

Output	Expression	Aggregate	Alias	Sort Type	Sort Order	Grouping	Criteria	Or...	Or...	Or...
☑	Convert(VarChar(19),DateAdd(s, View_Requ		last_mod_d			□		<> ''		
☑	View_Request.asset					□		<> ''		
☑	View_Request.time_spent_sum					□				
☑	View_Request.category_name					□				

```
Select View_Request.ref_num, Convert(VarChar(19),DateAdd(s,
  View_Request.last_mod_dt, '19700101'),20) As last_mod_date,
  View_Request.asset, View_Request.time_spent_sum, View_Request.category_name,
  View_Request.impact_num, View_Request.status_name, View_Request.priority_num
From View_Request
Where Convert(VarChar(19),DateAdd(s, View_Request.last_mod_dt, '19700101'),20)
  <> '' And View_Request.asset <> ''
```

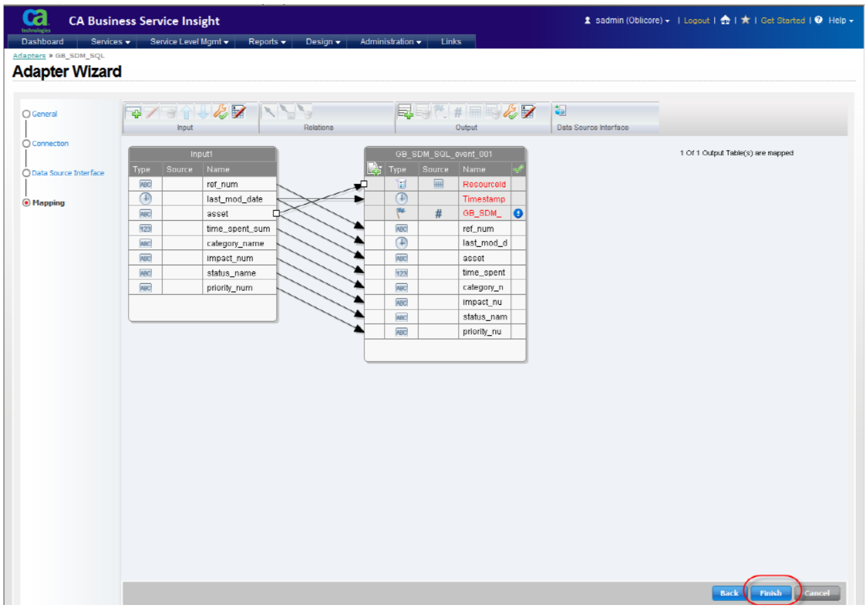
No. of lines: 130

Record#	ref_num string	last_mod_date string	asset string	time_spent_sum integer	category_name string	impact_num string	status_name string
0	33	2011-01-31 21:33:34	Global Expense Application	11			Closed
1	34	2011-01-31 21:34:04	Global Expense Application	11			Closed
2	40	2011-02-04 21:00:08	EU-SPITCHER	4			Closed
3	41	2011-01-31 20:23:07	Global Expense Application	26			Closed
4	114	2011-01-31 21:39:05	Global Expense Application	139	Applications	3-Single Group	Closed

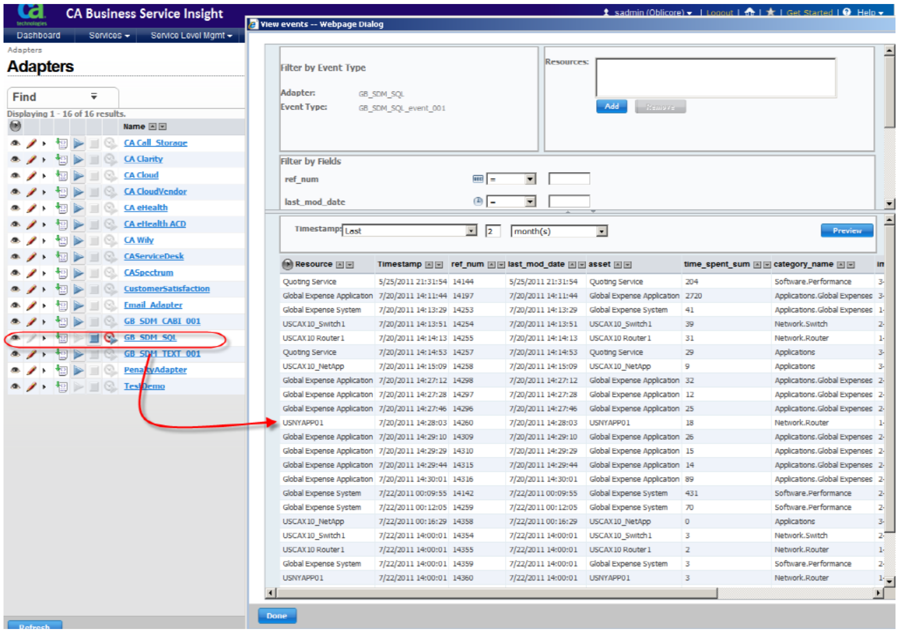
8. Click OK to return to the Data Source Interface page and specify the query key fields for the adapter.

9. Click Next to move to the Mapping page. Create the event types and map the fields.

10. Click Finish after you have mapped all the fields.



The SQL Adapter is ready to start and run. You can view the events that were generated by the adapter. For more information about viewing the events, see View Events Generated by the Adapter (see page 155). The following example shows the events that were generated by the SQL adapter.



Adapters

Displaying 1 - 16 of 16 results.

Name
CA Call_Storage
CA Clarity
CA Cloud
CA CloudVendor
CA eHealth
CA eHealth ACD
CA Wily
CAServiceDesk
CASpectrum
CustomerSatisfaction
Email_Adapter
GB_SDM_CABI_001
GB_SDM_SQL
GB_SDM_TEXT_001
PenaltyAdapter
TestDemo

Filter by Event Type

Adapter: GB_SDM_SQL
Event Type: GB_SDM_SQL_event_001

Resources:

Filter by Fields

ref_num =
last_mod_date -

Timestamp: Last 2 month(s)

Resource	Timestamp	ref_num	last_mod_date	asset	time_spent_sum	category_name	in
Quoting Service	5/25/2011 21:31:54	14144	5/25/2011 21:31:54	Quoting Service	204	Software.Performance	3-
Global Expense Application	7/20/2011 14:11:44	14197	7/20/2011 14:11:44	Global Expense Application	2720	Applications.Global Expenses	3-
Global Expense System	7/20/2011 14:13:29	14253	7/20/2011 14:13:29	Global Expense System	41	Applications.Global Expenses	1-
USCAX10_Switch1	7/20/2011 14:13:51	14254	7/20/2011 14:13:51	USCAX10_Switch1	39	Network.Switch	2-
USCAX10 Router1	7/20/2011 14:14:13	14255	7/20/2011 14:14:13	USCAX10 Router1	31	Network.Router	1-
Quoting Service	7/20/2011 14:14:53	14257	7/20/2011 14:14:53	Quoting Service	29	Applications	3-
USCAX10_NetApp	7/20/2011 14:15:09	14258	7/20/2011 14:15:09	USCAX10_NetApp	9	Applications	3-
Global Expense Application	7/20/2011 14:27:12	14298	7/20/2011 14:27:12	Global Expense Application	32	Applications.Global Expenses	2-
Global Expense Application	7/20/2011 14:27:28	14297	7/20/2011 14:27:28	Global Expense Application	12	Applications.Global Expenses	2-
Global Expense Application	7/20/2011 14:27:46	14296	7/20/2011 14:27:46	Global Expense Application	25	Applications.Global Expenses	2-
USNYAPP01	7/20/2011 14:28:03	14260	7/20/2011 14:28:03	USNYAPP01	18	Network.Router	1-
Global Expense Application	7/20/2011 14:29:10	14309	7/20/2011 14:29:10	Global Expense Application	26	Applications.Global Expenses	2-
Global Expense Application	7/20/2011 14:29:29	14310	7/20/2011 14:29:29	Global Expense Application	15	Applications.Global Expenses	2-
Global Expense Application	7/20/2011 14:29:44	14315	7/20/2011 14:29:44	Global Expense Application	14	Applications.Global Expenses	2-
Global Expense Application	7/20/2011 14:30:01	14316	7/20/2011 14:30:01	Global Expense Application	89	Applications.Global Expenses	2-
Global Expense System	7/22/2011 00:09:55	14142	7/22/2011 00:09:55	Global Expense System	431	Software.Performance	2-
Global Expense System	7/22/2011 00:12:05	14259	7/22/2011 00:12:05	Global Expense System	70	Software.Performance	2-
USCAX10_NetApp	7/22/2011 00:16:29	14358	7/22/2011 00:16:29	USCAX10_NetApp	0	Applications	3-
USCAX10_Switch1	7/22/2011 14:00:01	14354	7/22/2011 14:00:01	USCAX10_Switch1	3	Network.Switch	2-
USCAX10 Router1	7/22/2011 14:00:01	14355	7/22/2011 14:00:01	USCAX10 Router1	2	Network.Router	1-
Global Expense System	7/22/2011 14:00:01	14359	7/22/2011 14:00:01	Global Expense System	3	Software.Performance	2-
USNYAPP01	7/22/2011 14:00:01	14360	7/22/2011 14:00:01	USNYAPP01	3	Network.Router	1-

How to Use ETL to Integrate CA SDM with CA BSI

Several methods have been discussed to integrate CA SDM with CA BSI. The final, and preferred, method is to use an extract transform load (ETL) approach. While any ETL tool can be used, the community version of Pentaho is recommended and is discussed in this section.

The basic approach to leveraging the ETL approach uses the following process:

1. Download the Pentaho Community Edition tool at sourceforge.com.

   Important! Do not use the version from the Pentaho site.

2. Configure the Spoon tool, which is part of the Pentaho suite, to run correctly.

3. Create the ETL transformation with Spoon to extract data into the desired CSV format.

4. Create an adapter to read the CSV file. See Configure a Text Adapter (see page 142) for more information about creating adapters.

The approach that is used here leverages the CA SDM data abstraction layer known as Majic. Also, this approach uses the CA Business Intelligence Business Objects CA SDM ODBC driver. You could use the ETL tool directly on the CA SDM tables. However, this method is not recommended because of security violation concerns that are defined in the CA SDM role entitlements.

Using an ETL approach provides the following advantages:

- Allows much better control of the way in which data is received by CA BSI.
- Provides the ability to build a library of ETL jobs to handle a wide variety of applications.
- Focuses the effort to understand MDR data on the customer (or CA Technologies if it is a CA Technologies application).
- Supports the Community model more easily.
- Provides flexibility to use an ETL tool that is preferred by the customer.

Get Started with the Spoon Tool

Follow these steps:

1. Download the Spoon tool from sourceforge.com.

   Note: The Spoon tool is a part of the Pentaho Business Intelligence Suite. You cannot access the Spoon tool separately. You must download the entire suite to get access to Spoon.

2. Install the file.

   Note: You must have at least a newer version of Java running. However, running the latest version is highly recommended.

3. Locate the kettle.properties file that is installed and back it up because you will be changing it.

   Note: The kettle.properties file is the primary tool that you use to configure Spoon. You also use two batch files: spoon.bat and set-pentaho-env.bat.

4. Run the spoon.bat file and verify that it loads.

   The spoon.bat file may pause when you first run it because it runs from the command line. Wait at least 15 seconds before deciding that the application is not responding. If spoon.bat does not run, there may be a problem with finding the appropriate Java environment.

5. If the spoon.bat file does not run, edit the set-pentaho-env.bat file. Follow the instructions in the set-pentaho-env.bat file. This file is used to configure the Java environment so that Spoon runs correctly.

Configure the Spoon ETL Tool

If you are planning to leverage the predefined ETL transformations available through CA Technologies Support, the following additional configuration is required. If you are not using the CA Technologies Support ETL transformations, you will need to create your own similar structures.

Follow these steps:

1. Locate the kettle.properties file and back up the file.

   Note: This file is the master Spoon configuration file and is loaded each time that you run the Spoon tool. If you change this configuration file, the Spoon environment is not affected until you shut down Spoon and reopen it.

2. Create a directory structure where all of your various files and output can be created and saved.

   Note: These instructions apply to the Windows environment and need to be modified slightly in a Linux environment.

3. Create a directory named C:\etl and create the following subdirectories:

   - C:/etl/filters
   - C:/etl/jobs
   - C:/etl/logs
   - C:/etl/results
   - C:/etl/tracking
   - C:/etl/transformations
   - C:/etl/enumerations
   - C:/etl/usminfo
   - C:/etl/mdrimport

4. Modify the kettle.properties file to include the parameters in the following list:

   Note: You can modify the file directly or open the Spoon GUI and select Edit, Edit the kettle.properties file. The Spoon GUI method is recommended.

   - ETL_DIR=c:/etl
   - ETL_Filters_DIR=c/etl/filters
   - ETL_Jobs_DIR=c:/etl/jobs
   - ETL_LOGS_DIR=c:/etl/logs
   - ETL_RESULTS_DIR=c:/etl/results
   - ETL_TRACKING_DIR=c:/etl/tracking
   - ETL_TRANSFORMATIONS_DIR=c:/etl/transformations
   - ETL_ENUMERATIONS_DIR=c:/etl/enumerations
   - ETL_USMINFO_DIR=c:/etl/usminfo
   - ETL_MDR_IMPORT_DIR=c:/etl/mdrimport

   You can change these directories at any time. If you do so, verify that the directory structure and the parameters match. Also, it is highly recommended that you use the forward slash to specify directories.

5. (Optional) If you are using the predefined content, add the following additional parameters to the kettle.properties file. These parameters are used in the transformations as filters.

   - STARTDATE=2001-01-01
   - STARTTIME=00:00:00
   - ENDDATE=2019-12-31
   - ENDTIME=23-59:59

Download the CA SDM-Specific Content

Two kinds of content are available. One type of content, a set of CA SDM transformations, is used with the SMI functionality of CA BSI. The other type of content is a straight ISO20000 content pack. Both types are available on CA Technologies Support. Both content packs are provided as zip structures and set up with the directory structure defined in Configure the Spoon ETL Tool (see page 162).

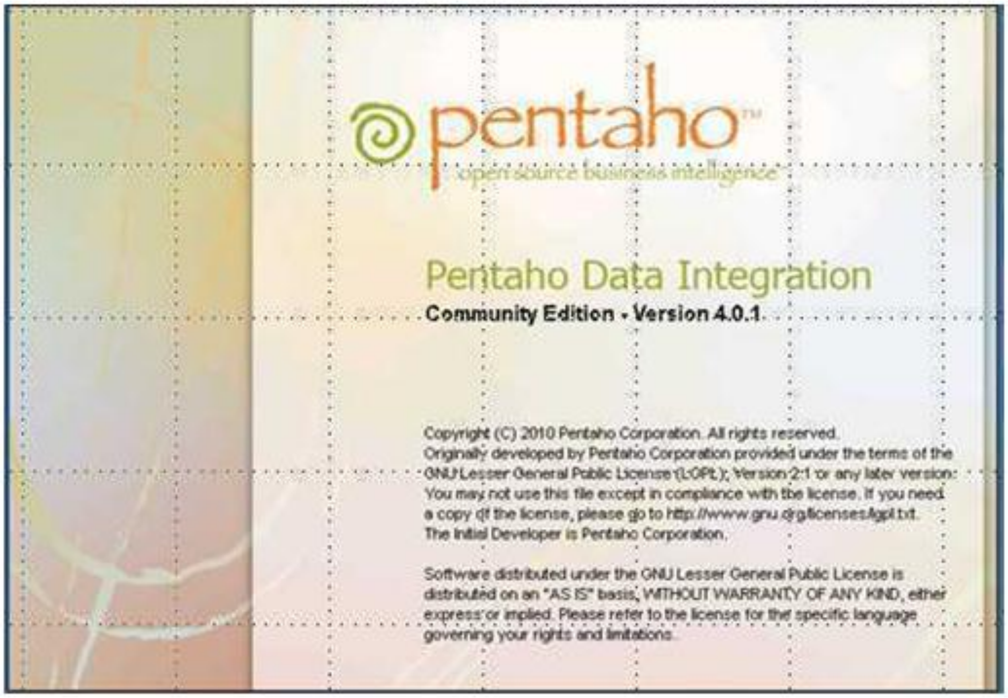
Download the content that applies to your environment.

Create Transformations with Spoon

The Spoon ETL tool is generally easy to use. Several books are available on this tool (you can run web searches for "Pentaho"). The instructions provided in this section guide you through creating a simple transformation. We recommend, however, that you leverage the predefined content, if possible, as a basis. If you use the predefined content, verify that the CA SDM CA Business Intelligence ODBC (SDM BI ODBC) service is running.

Follow these steps:

1. Load the Spoon ETL tool.



Pentaho Data Integration
Community Edition - Version 4.0.1

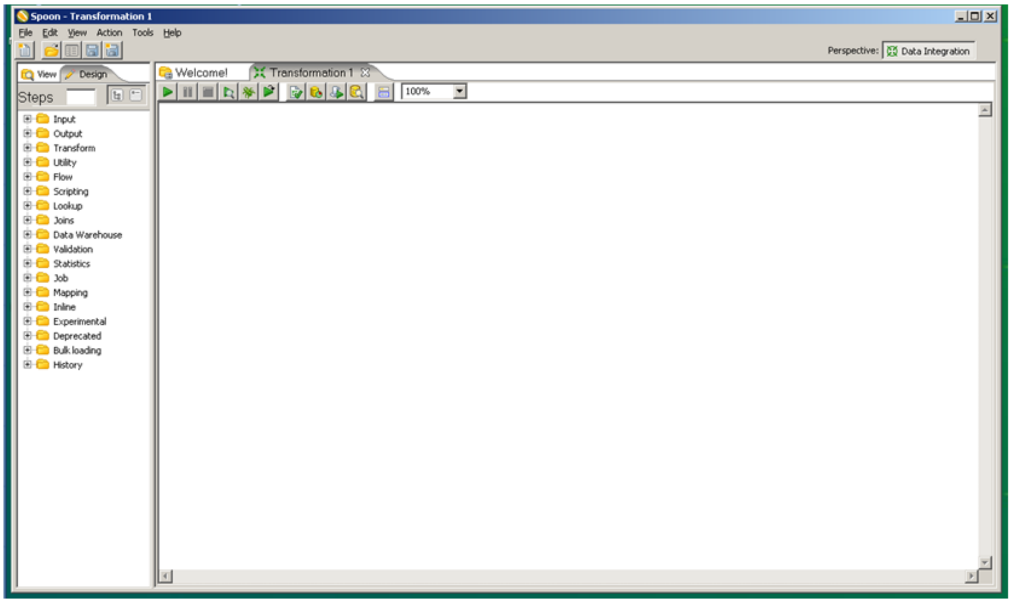
Copyright (C) 2010 Pentaho Corporation. All rights reserved.
Originally developed by Pentaho Corporation provided under the terms of the GNU Lesser General Public License (LGPL), Version 2.1 or any later version. You may not use this file except in compliance with the license. If you need a copy of the license, please go to http://www.gnu.org/licenses/lgpl.txt. The Initial Developer is Pentaho Corporation.

Software distributed under the GNU Lesser General Public License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. Please refer to the license for the specific language governing your rights and limitations.

You may have a different (more updated) version.

2. Select File, New, Transformation.

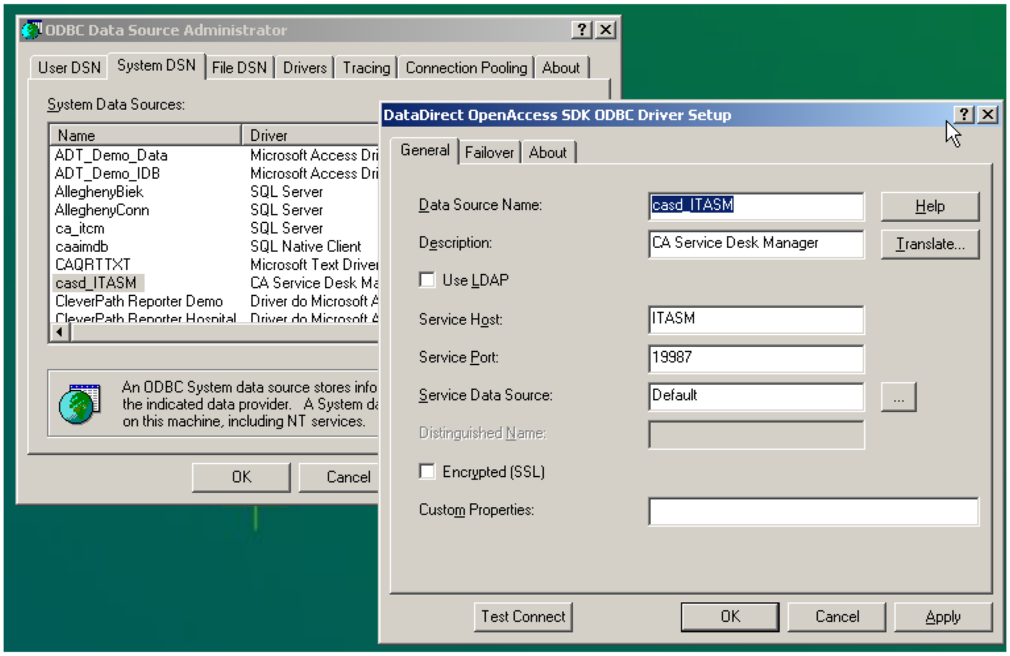
   You will see the page shown in the following example.



Note: The difference between a transformation and a job is that a transformation is an individual ETL task and a job consists of multiple transformations that are assembled together.

3. Define a connection to the CA SDM MDB.

   As we are leveraging the ODBC driver, verify that an ODBC DSN is defined that points to the CA SDM MDB. Use the ODBC Administration tool (ODBC Data Source Administrator) from the server Control Panel (or Administration Tools) to create a DSN. Test the connection. The following example shows the DSN that we defined in this section.



System Data Sources:

Name	Driver
ADT_Demo_Data	Microsoft Access Dri
ADT_Demo_IDB	Microsoft Access Dri
AlleghenyBiek	SQL Server
AlleghenyConn	SQL Server
ca_itcm	SQL Server
caaimdb	SQL Native Client
CAQRTTXT	Microsoft Text Driver
casd_ITASM	CA Service Desk Ma
CleverPath Reporter Demo	Driver do Microsoft A
CleverPath Reporter Hospital	Driver do Microsoft A

An ODBC System data source stores info
the indicated data provider. A System da
on this machine, including NT services.

Data Source Name: casd_ITASM
Description: CA Service Desk Manager
□ Use LDAP
Service Host: ITASM
Service Port: 19987
Service Data Source: Default
Distinguished Name:
□ Encrypted (SSL)
Custom Properties:

4. Click the View tab and double-click the Database connections.

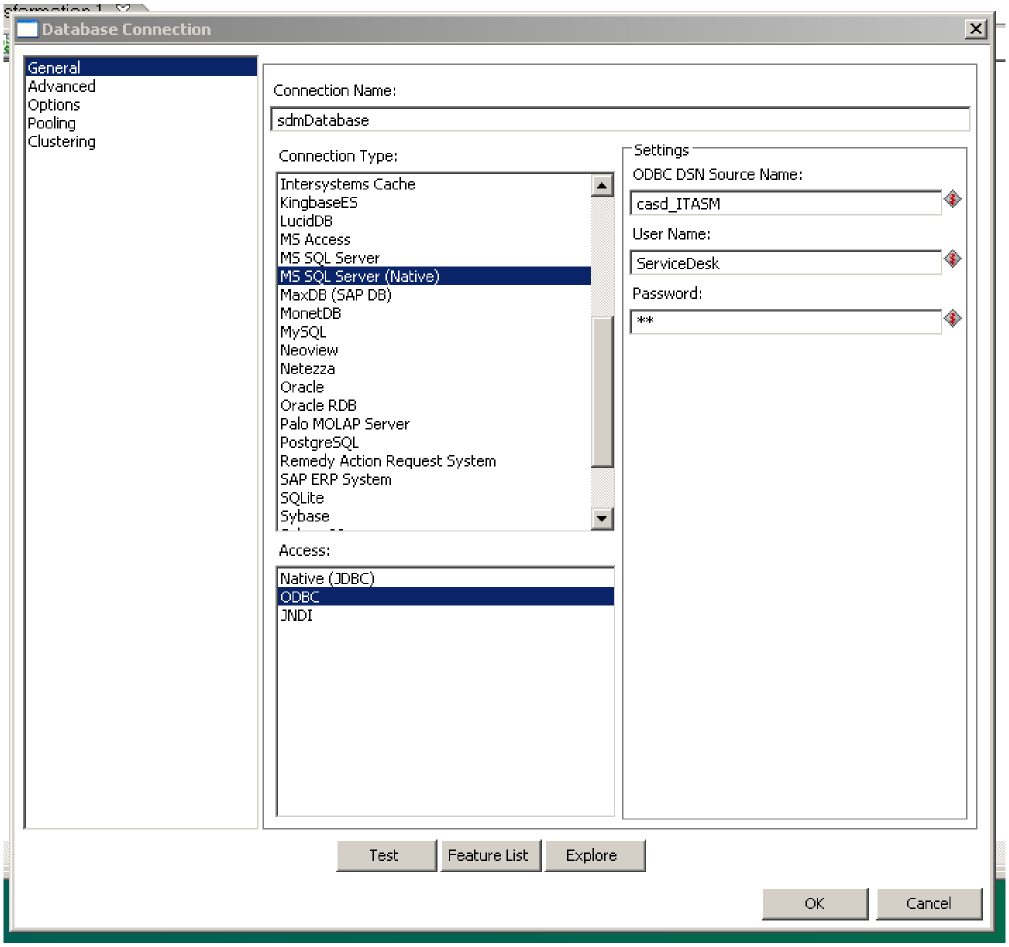
5. Provide the following information: connection name, connection type, and access information.

   If you are creating many jobs, add this information to the kettle.properties file so that this information can be used as run-time parameters. This approach is used by the predefined content. For this example, the following information is assumed:

   - Database connection name: sdmDatabase
   - Database type: SQL Server
   - Database access: JDBC
   - Database ODBC_DSN: casd_ITASM
   - Database Name: ServiceDesk

- Database Password: ca

The completed form appears as in the following example:


Database Connection

Connection Name: sdmDatabase

Connection Type: MS SQL Server (Native)

Access: ODBC

Settings

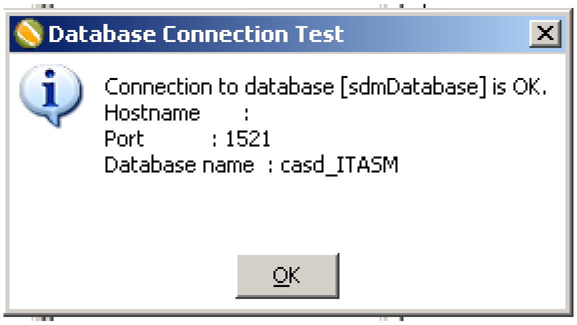
ODBC DSN Source Name: casd_ITASM

User Name: ServiceDesk

Password: **

6. Click Test.

The following confirmation message appears:


Database Connection Test

```
Connection to database [sdmDatabase] is OK.
Hostname       :
Port           : 1521
Database name  : casd_ITASM
```

If you get an error message, verify that the parameters are correct. Also verify that the CA SDM ODBC Driver services are running.

7. Click the View tab and select Database Connections.

   The sdmDatabase connection displays.

8. Drag and drop the sdmDatabase connection onto the transformation breadboard.

   The Table Input window appears.

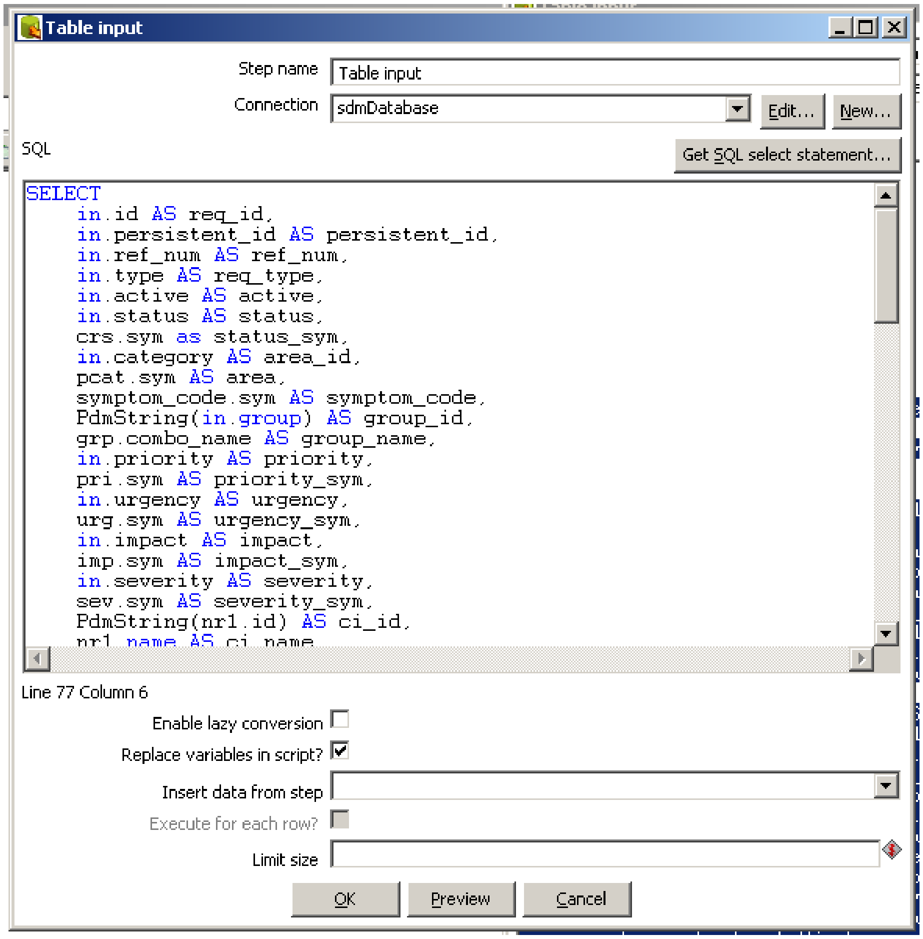
9. Enter the SQL statement that will return the fields that you want to process.

   In this example, the statement returns information about incidents:

```
SELECT
    in.id AS req_id,
    in.persistent_id AS persistent_id,
    in.ref_num AS ref_num,
    in.type AS req_type,
    in.active AS active,
    in.status AS status,
    crs.sym as status_sym,
    in.category AS area_id,
    pcat.sym AS area,
    symptom_code.sym AS symptom_code,
    PdmString(in.group) AS group_id,
    grp.combo_name AS group_name,
    in.priority AS priority,
    pri.sym AS priority_sym,
    in.urgency AS urgency,
    urg.sym AS urgency_sym,
    in.impact AS impact,
    imp.sym AS impact_sym,
    in.severity AS severity,
    sev.sym AS severity_sym,
    PdmString(nr1.id) AS ci_id,
    nr1.name AS ci_name,
    nr1.family AS ci_family,
    nr1.class AS ci_class,
    PdmString(nr2.id) AS service_id,
    nr2.name AS service_name,
    nr2.family AS service_family,
    nr2.class AS service_class,
    in.open_date AS open_date,
    in.resolve_date AS resolve_date,
    in.close_date AS close_date,
    PdmSeconds(in.time_spent_sum) AS time_spent,
    in.resolution_code AS res_code,
    resocode.sym AS res_code_sym,
    in.resolution_method AS res_method,
    resomethod.sym AS res_method_sym,
    in.sla_violation AS sla_violation,
    PdmString(in.tenant) as tenant_id,
    tenant.name AS tenant_name,
    in.external_system_ticket AS ext_ticket,
    in.last_mod_dt AS last_mod_dt,
    in.major_incident AS major_incident,
    in.ticket_avoided AS ticket_avoided,
    in.caused_by_chg AS caused_by_change,
    in.incorrectly_assigned AS incorrectly_assigned,
    in.outage_start_time AS outage_start_time,
    in.outage_end_time AS outage_end_time,
    in.outage_type AS outage_type,
    outage_type.sym AS outage_type_sym,
    sdsc.violation_cost AS violation_cost,
    in.charge_back_id AS charge_back_id
FROM
    in
INNER JOIN cnt ON cnt.id = in.customer
LEFT JOIN tenant ON in.tenant = tenant.id
LEFT JOIN sdsc ON sdsc.code = pcat.service_type
LEFT JOIN nr nr1 ON in.affected_resource = nr1.id
LEFT JOIN nr nr2 ON in.affected_service = nr2.id
LEFT JOIN pcat ON in.category=pcat.persistent_id
LEFT JOIN grp ON in.group=grp.id
LEFT JOIN chg ON in.change=chg.id
LEFT JOIN symptom_code ON in.symptom_code = symptom_code.id
LEFT JOIN resocode ON in.resolution_code = resocode.id
LEFT JOIN resomethod ON in.resolution_method  = resomethod.id
LEFT JOIN rc ON in.rootcause  = rc.id
LEFT JOIN chg_tpl ON chg.template_name=chg_tpl.id
LEFT JOIN pri ON in.priority = pri.enum
LEFT JOIN urg ON in.urgency = urg.enum
LEFT JOIN imp ON in.impact = imp.enum
LEFT JOIN sev ON in.severity = sev.enum
LEFT JOIN crs ON in.status = crs.code
LEFT JOIN outage_type ON in.outage_type = outage_type.id
WHERE
in.last_mod_dt >= {ts '${STARTDATE} ${STARTTIME}'}
AND in.last_mod_dt <= {ts '${ENDDATE} ${ENDTIME}'}
```

10. Verify that the following check box is selected: Replace variables in script?

    This option allows you to use the parameters in the kettle.properties file. The following example displays this check box.



Step name: Table input

Connection: sdmDatabase

```
SELECT
    in.id AS req_id,
    in.persistent_id AS persistent_id,
    in.ref_num AS ref_num,
    in.type AS req_type,
    in.active AS active,
    in.status AS status,
    crs.sym as status_sym,
    in.category AS area_id,
    pcat.sym AS area,
    symptom_code.sym AS symptom_code,
    PdmString(in.group) AS group_id,
    grp.combo_name AS group_name,
    in.priority AS priority,
    pri.sym AS priority_sym,
    in.urgency AS urgency,
    urg.sym AS urgency_sym,
    in.impact AS impact,
    imp.sym AS impact_sym,
    in.severity AS severity,
    sev.sym AS severity_sym,
    PdmString(nr1.id) AS ci_id,
    nr1.name AS ci_name
```

Line 77 Column 6

Enable lazy conversion ☐

Replace variables in script? ☑

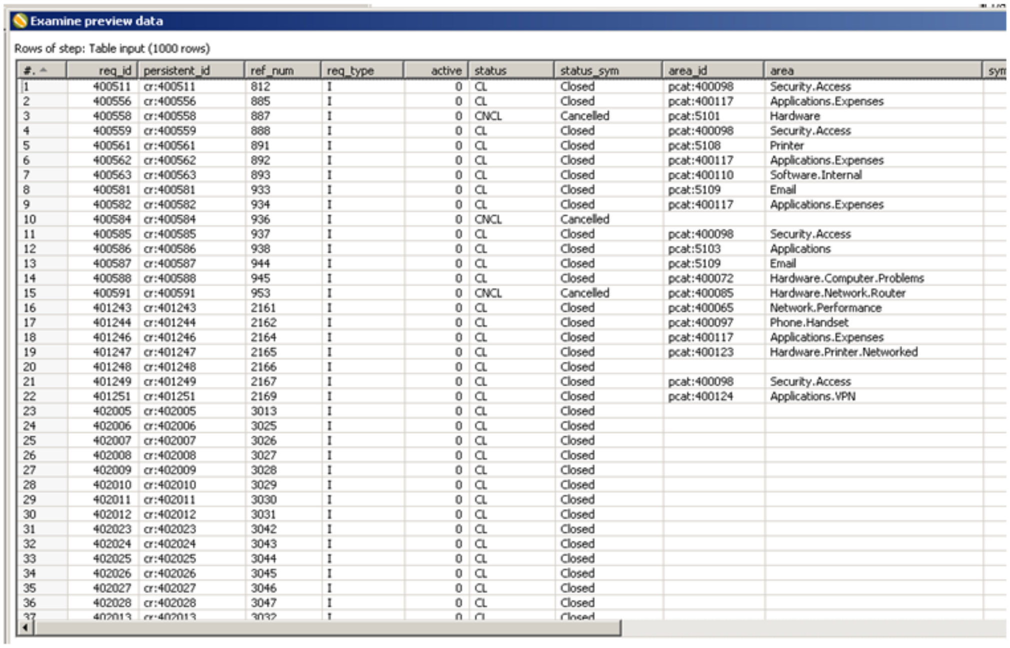
Insert data from step

Execute for each row? ☐

Limit size

11. Click the Preview tab to see the requests of this query.

    You will see a page that is similar to the following example.



Examine preview data

Rows of step: Table input (1000 rows)

#.	req_id	persistent_id	ref_num	req_type	active	status	status_sym	area_id	area	sym
1	400511	cr:400511	812	I	0	CL	Closed	pcat:400098	Security.Access	
2	400556	cr:400556	885	I	0	CL	Closed	pcat:400117	Applications.Expenses	
3	400558	cr:400558	887	I	0	CNCL	Cancelled	pcat:5101	Hardware	
4	400559	cr:400559	888	I	0	CL	Closed	pcat:400098	Security.Access	
5	400561	cr:400561	891	I	0	CL	Closed	pcat:5108	Printer	
6	400562	cr:400562	892	I	0	CL	Closed	pcat:400117	Applications.Expenses	
7	400563	cr:400563	893	I	0	CL	Closed	pcat:400110	Software.Internal	
8	400581	cr:400581	933	I	0	CL	Closed	pcat:5109	Email	
9	400582	cr:400582	934	I	0	CL	Closed	pcat:400117	Applications.Expenses	
10	400584	cr:400584	936	I	0	CNCL	Cancelled			
11	400585	cr:400585	937	I	0	CL	Closed	pcat:400098	Security.Access	
12	400586	cr:400586	938	I	0	CL	Closed	pcat:5103	Applications	
13	400587	cr:400587	944	I	0	CL	Closed	pcat:5109	Email	
14	400588	cr:400588	945	I	0	CL	Closed	pcat:400072	Hardware.Computer.Problems	
15	400591	cr:400591	953	I	0	CNCL	Cancelled	pcat:400085	Hardware.Network.Router	
16	401243	cr:401243	2161	I	0	CL	Closed	pcat:400065	Network.Performance	
17	401244	cr:401244	2162	I	0	CL	Closed	pcat:400097	Phone.Handset	
18	401246	cr:401246	2164	I	0	CL	Closed	pcat:400117	Applications.Expenses	
19	401247	cr:401247	2165	I	0	CL	Closed	pcat:400123	Hardware.Printer.Networked	
20	401248	cr:401248	2166	I	0	CL	Closed			
21	401249	cr:401249	2167	I	0	CL	Closed	pcat:400098	Security.Access	
22	401251	cr:401251	2169	I	0	CL	Closed	pcat:400124	Applications.VPN	
23	402005	cr:402005	3013	I	0	CL	Closed			
24	402006	cr:402006	3025	I	0	CL	Closed			
25	402007	cr:402007	3026	I	0	CL	Closed			
26	402008	cr:402008	3027	I	0	CL	Closed			
27	402009	cr:402009	3028	I	0	CL	Closed			
28	402010	cr:402010	3029	I	0	CL	Closed			
29	402011	cr:402011	3030	I	0	CL	Closed			
30	402012	cr:402012	3031	I	0	CL	Closed			
31	402023	cr:402023	3042	I	0	CL	Closed			
32	402024	cr:402024	3043	I	0	CL	Closed			
33	402025	cr:402025	3044	I	0	CL	Closed			
34	402026	cr:402026	3045	I	0	CL	Closed			
35	402027	cr:402027	3046	I	0	CL	Closed			
36	402028	cr:402028	3047	I	0	CL	Closed			
37	402013	cr:402013	3032	I	0	CL	Closed			

Export a CSV File for the CA BSI Adapter

After you have created the transformations, you need to export a CSV file that will be processed by the CA BSI adapter.

Follow these steps:

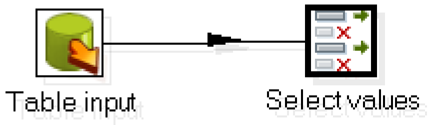
1. Click the Design tab and expand Transform.
2. Select the Select Values icon and drag it to the transformation breadboard.

3. Place the mouse cursor over the table input and click.

   Four symbols appear below the icon.

4. Select the symbol on the right (right arrow) and drag it to the Select Values icon.

   A line connecting the two appears as shown in the following example.



5. Click Select values.

   Three tabs are displayed.

6. Click the Select & Alter tab.

7. On the right, click Get fields to select.

   The rows from the SQL statement that you created previously are selected.

8. Click the Remove tab and click Get fields to remove.

9. Remove the following fields:

   - ref_num
   - req_type
   - active
   - status_sym
   - open_date
   - close_date
   - last_mod_dt

   Note: You are removing the fields that you actually want to keep. That is, you are removing from this list the fields that you want to keep in the ETL job.

10. Click the Meta-data tab and click Get fields to change.

11. Select each entry that is *not* a field that you just removed and delete the entry.

12. For the remaining fields, enter the following information in the Rename to field:

    - ref_num: Ticket_ReferenceNum
    - req_type: Ticket_Type
    - active: Ticket_State
    - status_sym: Ticket Status
    - open_date: Ticket_OpenDate
    - close_date: Ticket_CloseDate
    - last_mod_dt: Ticket_LastModifiedDate

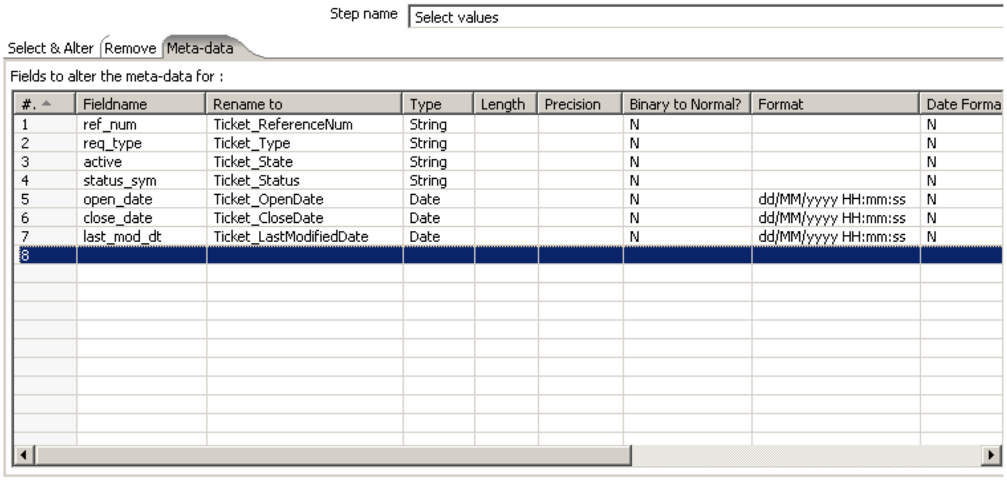
13. For each field, change the Type as follows:

    - ref_num: String
    - req_type: String
    - active: String
    - status_sym: String
    - open_date: Date
    - close_date: Date
    - last_mod_dt: Date

14. Change the format of the three date fields to match the following format:

    dd/MM/yyyy HH:mm:ss

The data for the fields should appear as in the following example.



Step name: Select values

Fields to alter the meta-data for :

#.	Fieldname	Rename to	Type	Length	Precision	Binary to Normal?	Format	Date Forma
1	ref_num	Ticket_ReferenceNum	String			N		N
2	req_type	Ticket_Type	String			N		N
3	active	Ticket_State	String			N		N
4	status_sym	Ticket_Status	String			N		N
5	open_date	Ticket_OpenDate	Date			N	dd/MM/yyyy HH:mm:ss	N
6	close_date	Ticket_CloseDate	Date			N	dd/MM/yyyy HH:mm:ss	N
7	last_mod_dt	Ticket_LastModifiedDate	Date			N	dd/MM/yyyy HH:mm:ss	N
8								

Export Data into a CSV File

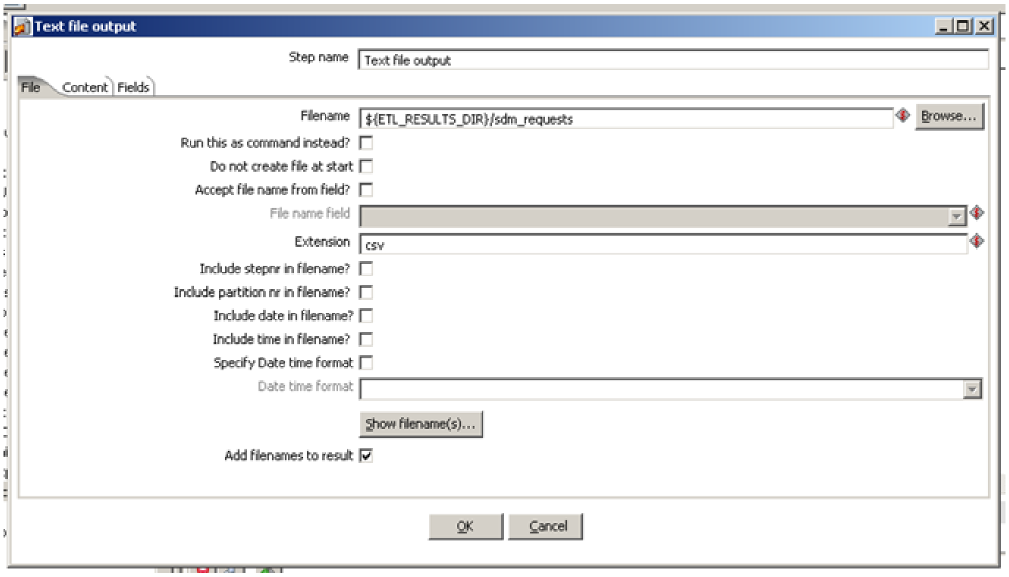
Export the data into a CSV file that will be processed by the CA BSI adapter.

Follow these steps:

1. On the Design tab, click the Output icon.
2. Expand and select Text file output.
3. Drag and drop Text file output onto the transformation breadboard.
4. Connect the Select Value icon to the Text file output.
5. Double-click Text file out.

   Three tabs are displayed.

6. Select the File tab and enter the information as shown in the following example.



Step name: Text file output

Filename: ${ETL_RESULTS_DIR}/sdm_requests

Run this as command instead? □

Do not create file at start □

Accept file name from field? □

File name field:

Extension: csv

Include stepnr in filename? □

Include partition nr in filename? □

Include date in filename? □

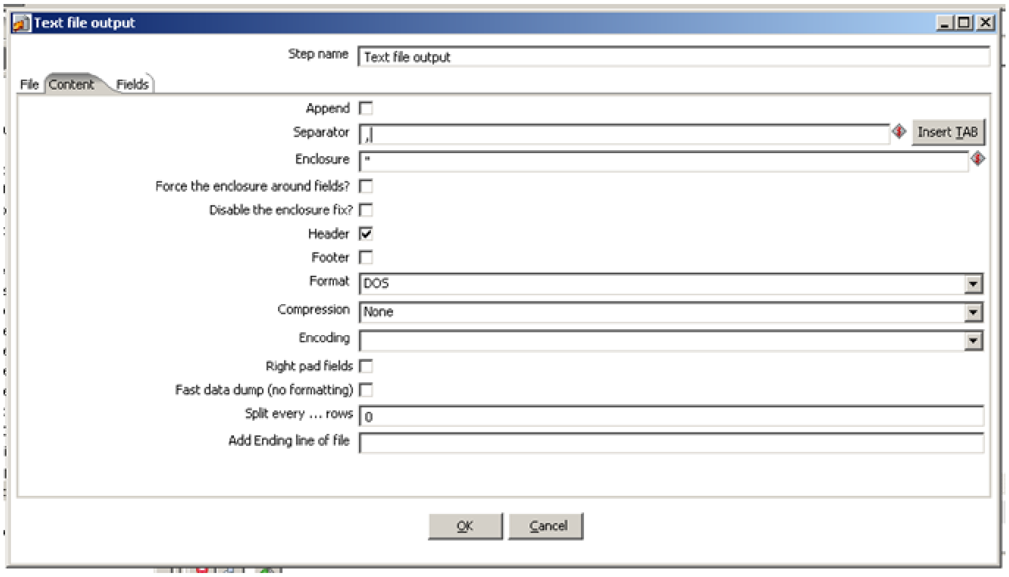
Include time in filename? □

Specify Date time format □

Date time format:

Add filenames to result ☑

7. Click the Content tab and enter the information as shown on the following example.



Step name: Text file output

Append □

Separator: ,

Enclosure: "

Force the enclosure around fields? □

Disable the enclosure fix? □

Header ☑

Footer □

Format: DOS

Compression: None

Encoding:

Right pad fields □

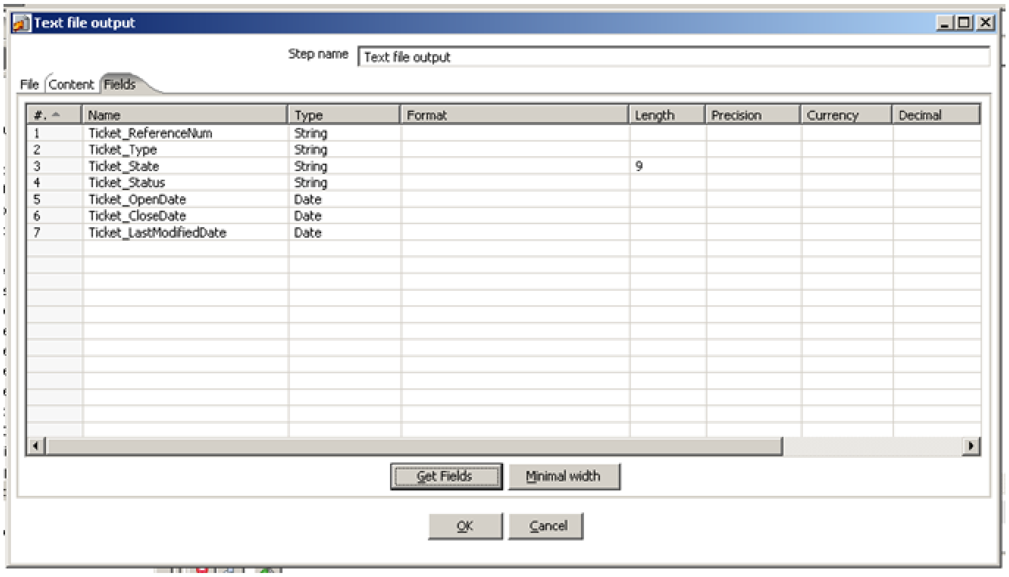
Fast data dump (no formatting) □

Split every ... rows: 0

Add Ending line of file:

8. Click the Fields tab and click Get Fields.

   The data that is displayed on your window should be similar to the following example.

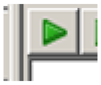


Step name: Text file output

#.	Name	Type	Format	Length	Precision	Currency	Decimal
1	Ticket_ReferenceNum	String					
2	Ticket_Type	String					
3	Ticket_State	String		9			
4	Ticket_Status	String					
5	Ticket_OpenDate	Date					
6	Ticket_CloseDate	Date					
7	Ticket_LastModifiedDate	Date					

9. Click Okay.

10. Click the right arrow button on the left to run the actual transformation.



   You are prompted to enter run-time parameters.

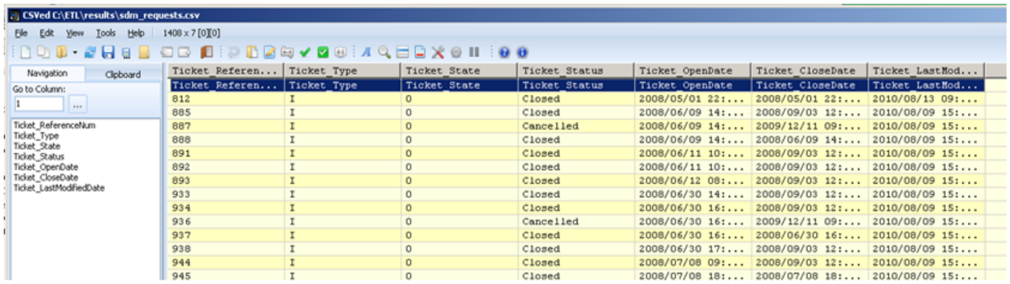
11. Click Launch.

   You are prompted to save the transformation.

12. Enter a name for the transformation.

   Note: Verify that the dialog is set to save the transformation in the C:\etl\transformation subdirectory, or any directory where you decide to save these types of files.

When the transformation is saved, you can navigate to the C:\etl\results directory and you can view the sdm_requests.csv file. The following example shows a transformation file.



Ticket_Referen...	Ticket_Type	Ticket_State	Ticket_Status	Ticket_OpenDate	Ticket_CloseDate	Ticket_LastMod...
Ticket_Referen...	Ticket_Type	Ticket_State	Ticket_Status	Ticket_OpenDate	Ticket_CloseDate	Ticket_LastMod...
812	I	0	Closed	2008/05/01 22:...	2008/05/01 22:...	2010/08/13 09:...
885	I	0	Closed	2008/06/09 14:...	2008/09/03 12:...	2010/08/09 15:...
887	I	0	Cancelled	2008/06/09 14:...	2009/12/11 09:...	2010/08/09 15:...
888	I	0	Closed	2008/06/09 14:...	2008/06/09 14:...	2010/08/09 15:...
891	I	0	Closed	2008/06/11 10:...	2008/09/03 12:...	2010/08/09 15:...
892	I	0	Closed	2008/06/11 10:...	2008/09/03 12:...	2010/08/09 15:...
893	I	0	Closed	2008/06/12 08:...	2008/09/03 12:...	2010/08/09 15:...
933	I	0	Closed	2008/06/30 14:...	2008/09/03 12:...	2010/08/09 15:...
934	I	0	Closed	2008/06/30 16:...	2008/09/03 12:...	2010/08/09 15:...
936	I	0	Cancelled	2008/06/30 16:...	2009/12/11 09:...	2010/08/09 15:...
937	I	0	Closed	2008/06/30 16:...	2008/06/30 16:...	2010/08/09 15:...
938	I	0	Closed	2008/06/30 17:...	2008/09/03 12:...	2010/08/09 15:...
944	I	0	Closed	2008/07/08 09:...	2008/09/03 12:...	2010/08/09 15:...
945	I	0	Closed	2008/07/08 18:...	2008/07/08 18:...	2010/08/09 15:...

You can now process this file through the CA BSI adapter.

Integration Points from CA BSI to CA SDM

CA BSI can generate alerts for contract deviations, service level violations, or any other events that you want to track. An alert is a notification sent to one or more users about events that are taking place in the system, according to predefined conditions defined in alert profiles. You can configure alert profiles for events in general or for events that apply to specific contracts. You can configure such alerts in CA BSI to create a ticket automatically in CA SDM.

Configure the CA BSI Mail Interface

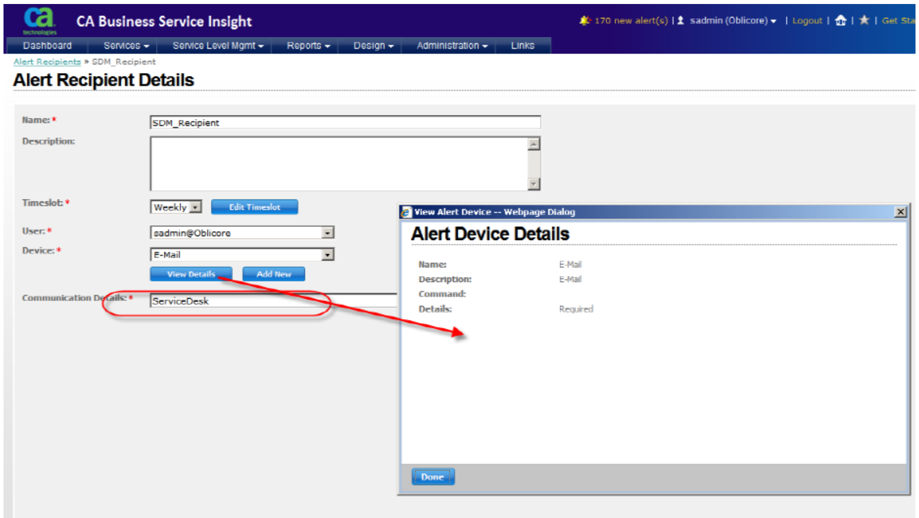
The simplest way for CA BSI to create a CA SDM ticket is to use the mail interface of both products.

Follow these steps:

1. Log in to CA BSI and, from the main menu bar, click Reports, Alerts, Alert Recipient.
2. Click Add New.

   The Alert Recipient Details page opens.

3. Specify the recipient name, select the Device as E-mail, and specify the CA SDM mailbox name in the Communication Details field. The following example shows the completed page.


CA Business Service Insight
170 new alert(s) | sadmin (Oblicore) | Logout | Get Sta
Dashboard
Services
Service Level Mgmt
Reports
Design
Administration
Links
Alert Recipients » SDM_Recipient
Edit Timeslot
View Details
Add New
Done

Alert Recipient Details

Name: * SDM_Recipient
Description:
Timeslot: * Weekly
User: * sadmin@Oblicore
Device: * E-Mail
Communication Details: * ServiceDesk

View Alert Device -- Webpage Dialog

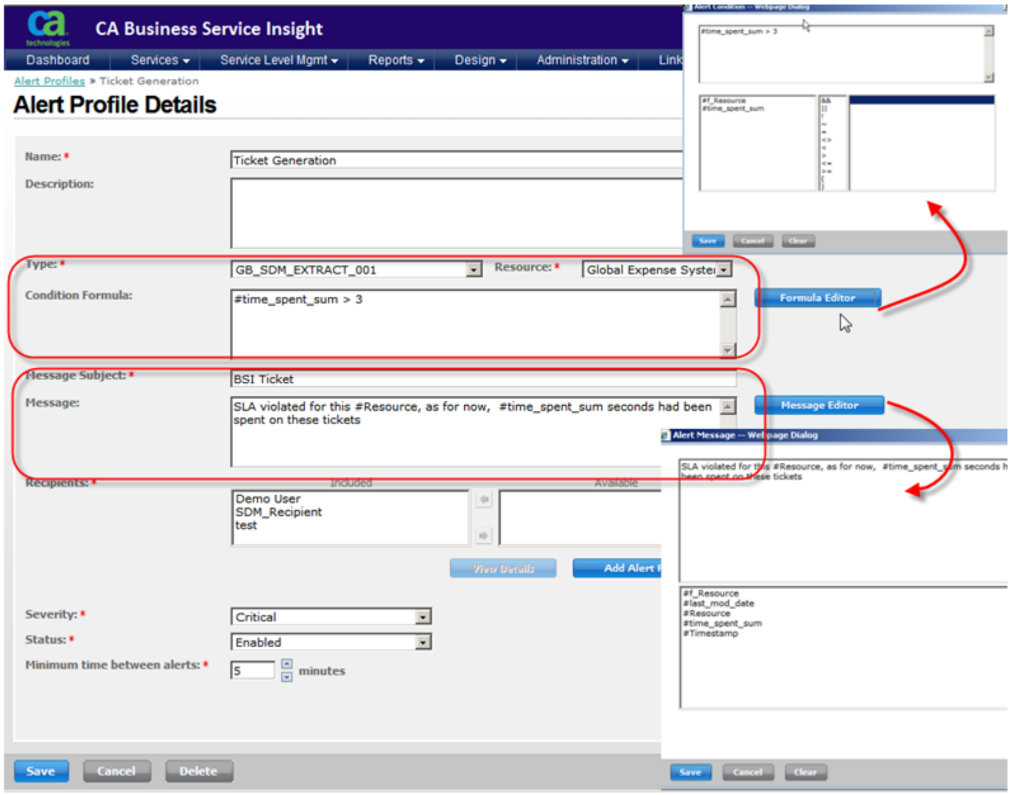
Alert Device Details

Name: E-Mail
Description: E-Mail
Command:
Details: Required

Next you configure an Alert Profile to specify what needs to be included in the ticket and when.

4. From the menu bar, click Reports, Alerts, Alert Profile and click Add New.

   The Alert Profile Details page appears, as shown in the following example.



Alert Profile Details

Name: * Ticket Generation
Description:
Type: * GB_SDM_EXTRACT_001 Resource: * Global Expense Syste
Condition Formula: #time_spent_sum > 3
Message Subject: * BSI Ticket
Message: SLA violated for this #Resource, as for now, #time_spent_sum seconds had been spent on these tickets
Recipients: * Demo User
SDM_Recipient
test
Severity: * Critical
Status: * Enabled
Minimum time between alerts: * 5 minutes

#time_spent_sum > 3

#f_Resource
#time_spent_sum

SLA violated for this #Resource, as for now, #time_spent_sum seconds h
been spent on these tickets

#f_Resource
#last_mod_date
#Resource
#time_spent_sum
#Timestamp

An alert Profile could be divided into at least three main parts:

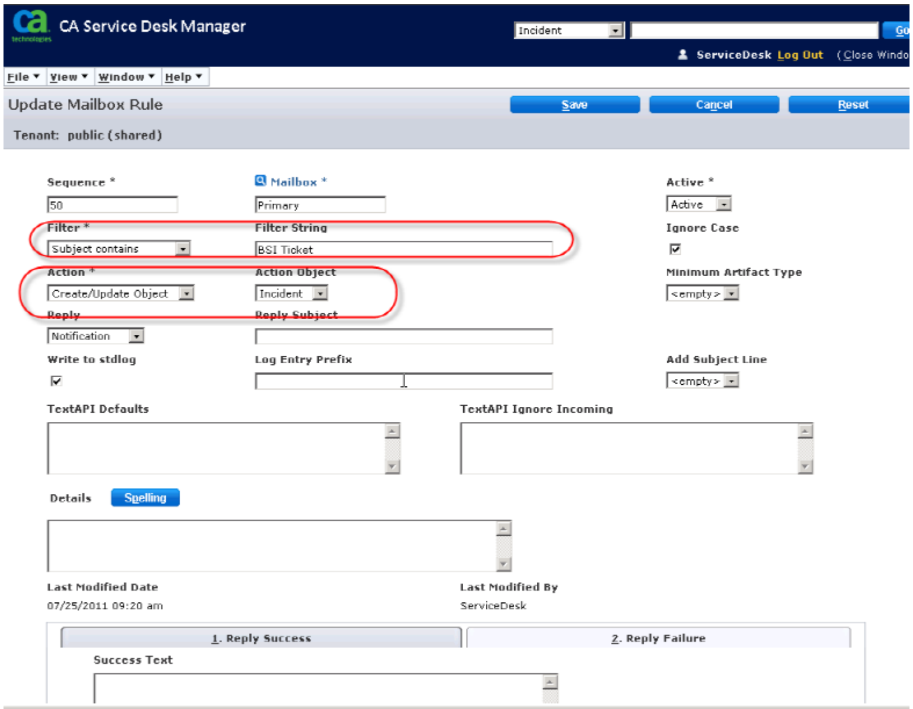
- Identification of the alert: name and description
- Trigger for the ticket creation (event type or CA BSI event, resource, and condition formula). Specify the condition using the Condition Formula Editor.
- Definition of the information that needs to be sent to the ticket. Any variables from the event itself can be used.

Configure the CA SDM Mail Interface

Configure CA SDM to create a mailbox rule that opens a ticket when it receives an email from CA BSI.

Follow these steps:

1. Click the Administration tab and select Email, Mailbox Rules.
2. Click Add New and specify the details as shown in the following example.



Update Mailbox Rule

Tenant: public (shared)

Sequence *: 50

Mailbox *: Primary

Active *: Active

Filter *: Subject contains

Filter String: BSI Ticket

Ignore Case: ☑

Action *: Create/Update Object

Action Object: Incident

Minimum Artifact Type: <empty>

Reply: Notification

Reply Subject:

Write to stdlog: ☑

Log Entry Prefix:

Add Subject Line: <empty>

TextAPI Defaults:

TextAPI Ignore Incoming:

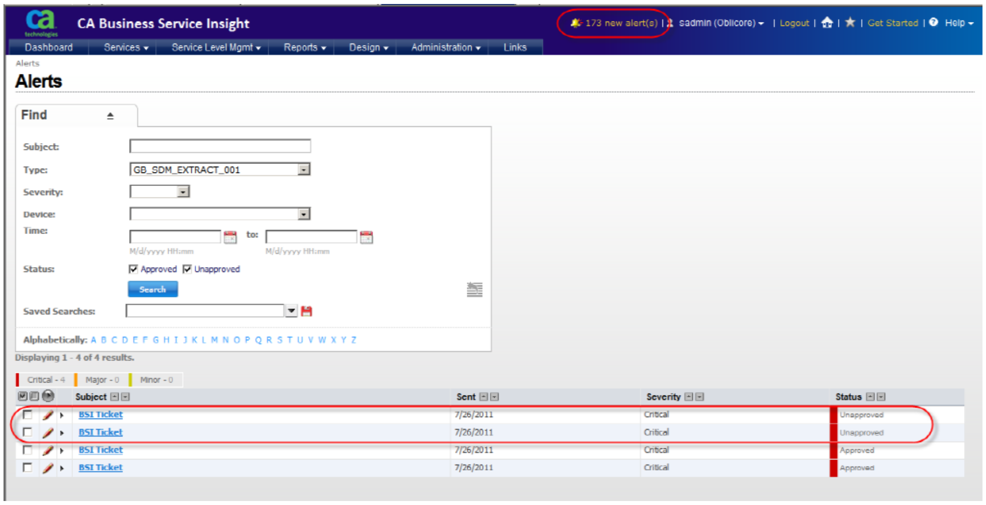
Details:

Last Modified Date: 07/25/2011 09:20 am

Last Modified By: ServiceDesk

Success Text:

When the conditions specified in the alert profile are met, an alert is triggered. The alert appears in the Alerts list in CA BSI.



Alerts

Subject:

Type: GB_SDM_EXTRACT_001

Severity:

Device:

Time: M/d/yyyy HH:mm to: M/d/yyyy HH:mm

Status: ☑ Approved ☑ Unapproved

Saved Searches:

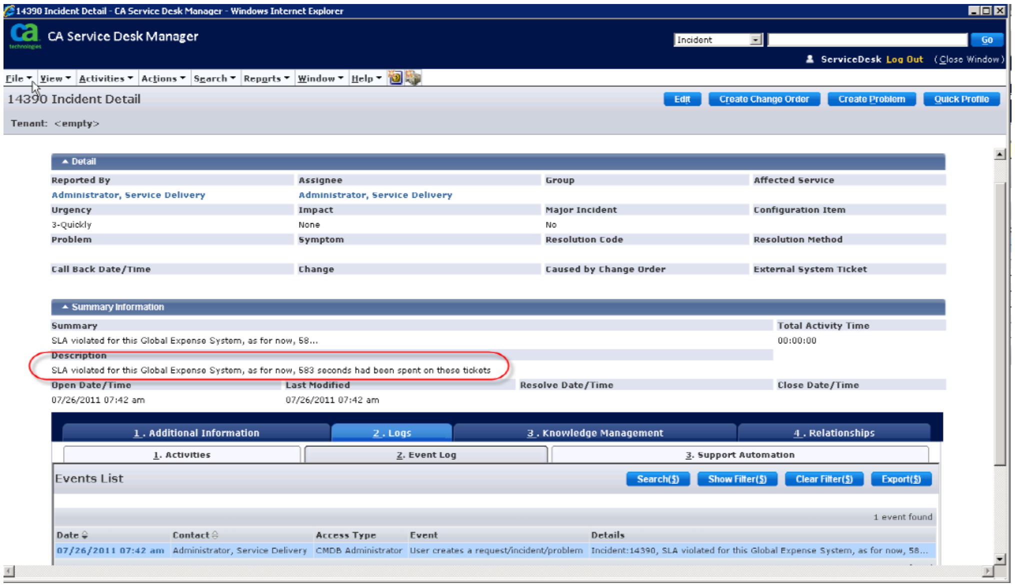
Alphabetically: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Displaying 1 - 4 of 4 results.

Critical - 4 | Major - 0 | Minor - 0

	Subject	Sent	Severity	Status
□	BSI Ticket	7/26/2011	Critical	Unapproved
□	BSI Ticket	7/26/2011	Critical	Unapproved
□	BSI Ticket	7/26/2011	Critical	Approved
□	BSI Ticket	7/26/2011	Critical	Approved

The alert sends an email to CA SDM, which creates a ticket as shown in the following example.



14390 Incident Detail

Tenant: <empty>

Reported By	Assignee	Group	Affected Service
Administrator, Service Delivery	Administrator, Service Delivery		
Urgency	**Impact**	**Major Incident**	**Configuration Item**
3-Quickly	None	No	
Problem	**Symptom**	**Resolution Code**	**Resolution Method**
Call Back Date/Time	**Change**	**Caused by Change Order**	**External System Ticket**

Summary: SLA violated for this Global Expense System, as for now, 58...

Total Activity Time: 00:00:00

Description: SLA violated for this Global Expense System, as for now, 583 seconds had been spent on these tickets

Open Date/Time	Last Modified	Resolve Date/Time	Close Date/Time
07/26/2011 07:42 am	07/26/2011 07:42 am		

Events List

1 event found

Date	Contact	Access Type	Event	Details
07/26/2011 07:42 am	Administrator, Service Delivery	CMDB Administrator	User creates a request/incident/problem	Incident:14390, SLA violated for this Global Expense System, as for now, 58...

Chapter 6: CA Identity Manager

CA Identity Manager Integration

This chapter discusses how CA SDM Release 12.6 and CA Identity Manager can be configured to work together. The following key topics are discussed:

- Integration points and functionality from CA SDM
- Integration points and value from CA Identity Manager to CA SDM
- How the integration works
- Integration instructions

Overview of CA Identity Manager

CA Identity Manager helps improve the operational efficiency and effectiveness of IT organizations. CA Identity Manager provides a scalable and configurable identity management foundation that can organize your identity information within the context of your unique business roles and processes. CA Identity Manager helps streamline the on-boarding and off-boarding of users, enables the business to manage access requests, and automates identity compliance processes proactively.

CA Identity Manager is a comprehensive solution that manages all types of identities across all IT systems, from the web to the mainframe, throughout the identity lifecycle. CA Identity Manager also provides an authoritative point of identity administration, enforces consistent identity policies, and audits identity-related actions.

CA Identity Manager provides an integrated identity administration solution. The solution serves as the foundation for user provisioning, self-service requests, identity governance, and other key processes. This solution enables your organization to reap the following benefits:

- Automate the processes of on-boarding, modifying, and off-boarding users and their associated access.
- Enable end users to initiate provisioning actions, ongoing password management, delegated administration, and related processes.

- Leverage role and policy analysis, and certification processes from CA Role and Compliance Manager (CA RCM) to enable more accurate and secure provisioning and deprovisioning decisions.
- Use powerful wizards and graphical tools that make it easy to adjust policies and applications when your business changes—without coding them manually.

Integration Details

CA SDM integrates with CA Identity Manager to support the self-service functionality that CA SDM provides in its web interface. After the integration, users can reset their passwords from the CA SDM user interface using the password reset capabilities that CA Identity Manager provides.

Integration Points and Functionality from CA SDM

From the CA SDM user interface, users can reset the password using the Password Management/Password Reset functionality of CA Identity Manager. Users are challenged with three self-authentication questions that must first be answered, either during self-registration or by modifying their user profile. After the users answer the questions correctly, the users must change their passwords. The new password must meet complex requirements that are defined in the Password Policy. When the password is changed, it is synchronized to the correlated user account.

Integration Points and Functionality from CA Identity Manager

After users change their passwords, they are redirected from CA Identity Manager to the CA SDM web interface.

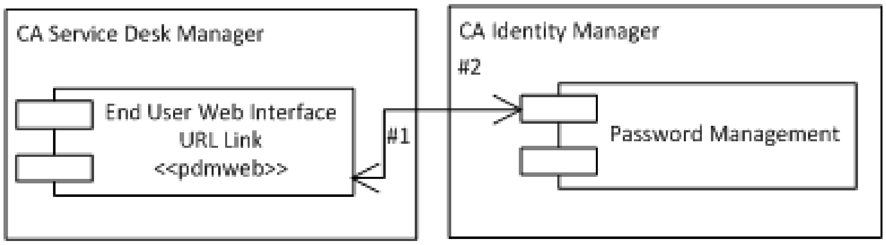
Integration Value

The CA Identity Manager integration provides the following value:

- Gain significant cost savings by allowing users to reset and manage their passwords. CA Identity Manager lets users choose question and answer pairs that will be used for self-authentication and subsequent password change and synchronization. Organizational password policies are enforced when the user selects a password.
- Reduce the volume of low complexity calls, freeing up analysts for more important activities.
- Improve security, enhance regulatory compliance and governance, and increase user satisfaction.

How the Integration Works

The following diagram illustrates how the integration between CA Identity Manager and CA SDM works.



The integration between CA Identity Manager and CA SDM works as follows:

1. The CA SDM self-service web interface displays a link to the CA Identity Manager Password Management interface.

2. The users click the link to access the password management functionality to reset the passwords.

Integration Example

Business Problem

Michael Reed, the Service Desk Manager for Forward, Inc., analyzes the Incident Reports that were generated by the CA SDM Dashboard. Michael finds that 20 to 35 percent of all incidents fall into the password reset category. The most frequent occurrences are on Monday mornings and when users return from vacation. Michael thinks this issue is affecting the productivity of his team, as resetting one password typically takes an analyst an average of 15 minutes. The reset can sometimes take more time because the operating system administrators, who have to reset the passwords manually, are involved in other critical activities. So the administrators push password resets into a pending status. Another concern is that some offices are staffed to work 24 hours a day, 7 days a week, but the Forward, Inc. service desk only operates from 8 a.m. until midnight. Employees may not know how to proceed if they have forgotten their passwords and they are unable to access important information and systems during the off hours. Michael decides that this problem needs to be taken care of immediately.

CA Approach

Forgotten passwords can increase the total operational cost in any organization, as users cannot do their job for extended periods of time. CA Identity Manager lets users choose question and answer pairs that will be used for self-authentication and subsequent password change and synchronization. Organizational password policies are enforced when the user selects a password.

Forward, Inc. plans to implement the password reset functionality that is available in CA Identity Manager, and then integrate it with the CA SDM self-service interface. This plan will allow Forward, Inc. users to reset their passwords and will provide tremendous business value for all users, particularly those users whose work hours are outside of the scheduled hours of the service desk.

Configuring a Solution

Michael Reed has asked the security department to provide the URL that allows CA Identity Manager Self Service Password functionality to be started in context. After Michael receives this information, he can go through the reset password functionality configuration task.

Configure the Integration from CA Identity Manager

To configure the integration, the CA Identity Manager Administrator must configure the self-service password reset functionality in CA Identity Manager. The Administrator must then provide the URL that starts the self-service password reset user interface. In this example, the URL appears as follows:

```
http://ForwardInc.domain.com:8080/idm/pub/ca/index.jsp?task.tag=ForgottenPasswordReset
```

Configure the Integration from CA SDM

Follow these steps:

1. Log in to CA SDM as a ServiceDesk user or an Administrator.
2. Click the Administration tab and choose Options Managers, Security, url_etrust_password_reset.
3. In the Option Value field, enter the URL that you received from the CA Identity Manager Administrator.
4. Click Install.

5. Click Save.

6. Restart the CA SDM server services.

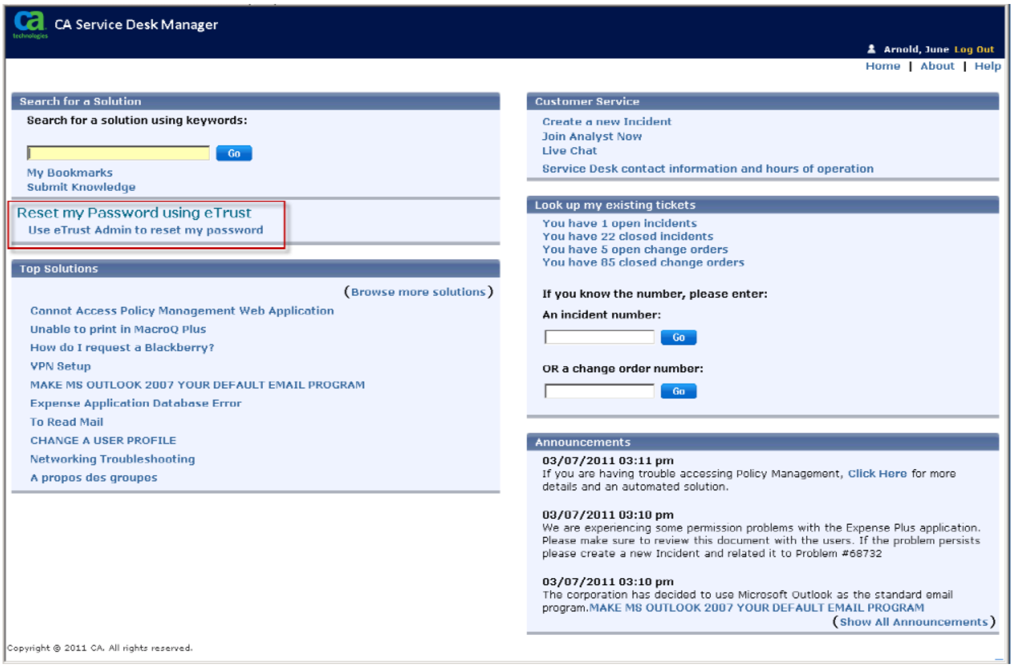
Test the Integration

Test the integration to verify that the integration is working correctly.

Follow these steps:

1. Log in to the CA SDM web interface as an employee user.

   The link for Reset my Password using eTrust is now displayed in the CA SDM user interface.


CA Service Desk Manager
Arnold, June Log Out
Home | About | Help
Search for a Solution
Search for a solution using keywords:
Go
My Bookmarks
Submit Knowledge
Reset my Password using eTrust
Use eTrust Admin to reset my password
Top Solutions
(Browse more solutions)
Cannot Access Policy Management Web Application
Unable to print in MacroQ Plus
How do I request a Blackberry?
VPN Setup
MAKE MS OUTLOOK 2007 YOUR DEFAULT EMAIL PROGRAM
Expense Application Database Error
To Read Mail
CHANGE A USER PROFILE
Networking Troubleshooting
A propos des groupes
Customer Service
Create a new Incident
Join Analyst Now
Live Chat
Service Desk contact information and hours of operation
Look up my existing tickets
You have 1 open incidents
You have 22 closed incidents
You have 5 open change orders
You have 85 closed change orders
If you know the number, please enter:
An incident number:
Go
OR a change order number:
Go
Announcements
(Show All Announcements)
Copyright © 2011 CA. All rights reserved.

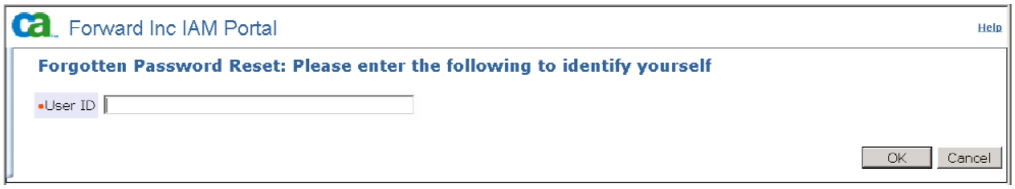
03/07/2011 03:11 pm
If you are having trouble accessing Policy Management, Click Here for more details and an automated solution.

03/07/2011 03:10 pm
We are experiencing some permission problems with the Expense Plus application. Please make sure to review this document with the users. If the problem persists please create a new Incident and related it to Problem #68732

03/07/2011 03:10 pm
The corporation has decided to use Microsoft Outlook as the standard email program.MAKE MS OUTLOOK 2007 YOUR DEFAULT EMAIL PROGRAM

2. Click Use eTrust Admin to reset my password.

   The following dialog opens, challenging you with the self-authentication questions to reset the password.


Forward Inc IAM Portal
Help
Forgotten Password Reset: Please enter the following to identify yourself
•User ID
OK
Cancel

   The testing of the integration is complete.

Integration Summary

The web interface of CA SDM for Employee, Customer, and Guest users includes a Password Reset link when configured. When users click the link, a CA Identity Manager web session is started so that users can answer questions to verify their identity (for example, password reset hints) and interactively reset their passwords.

Chapter 7: CA SiteMinder

CA SiteMinder Integration

This chapter discusses how CA SDM Release 12.6 and CA SiteMinder can be configured to work together. The following key topics are discussed:

- Integration points and functionality from CA SDM
- Integration points and value from CA SiteMinder to CA SDM
- How the integration works
- Integration instructions
- Extending the integration to include CA Identity Manager and CA Process Automation

Overview of CA SiteMinder

CA SiteMinder provides a centralized security management foundation that enables the secure use of the web to deliver applications and cloud services to customers, partners, and employees.

CA SiteMinder provides the following functionalities:

- Single sign-on
- Strong authentication management
- Centralized policy-based authorization and audit
- Identity federation
- Enterprise manageability

CA SiteMinder supports various directory services and user stores, eliminating redundant administration of user information. This support simplifies administration and provides unique and comprehensive security capabilities. CA SiteMinder fully leverages existing user directories, from LDAP directories and relational databases to mainframe security directories.

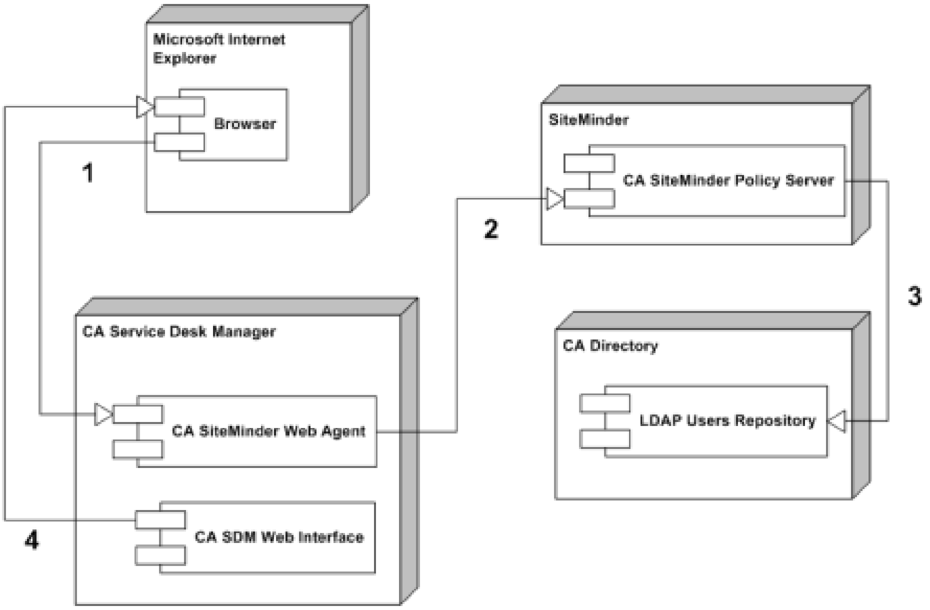
Integration Details

The CA SiteMinder integration with CA SDM enables security administrators to assign authentication schemes. The integration also allows for the defining and managing of authorization privileges for protected resources, such as the CA SDM pdmweb.exe URL. The authorization privileges are defined and managed by creating rules and policies to implement the authorization permissions against the appropriate LDAP or Administrative Domain (AD) user store.

The following CA SiteMinder integrations are described in this chapter:

- **Resource Protection**: Configure CA SiteMinder to protect the CA SDM main resources, such as pdmweb.exe.
- **User Directory Reference**: In an environment where CA SDM is configured to authenticate through CA EEM, CA EEM is configured to reference the global users and global groups from CA SiteMinder.

The following diagram illustrates how the CA SDM and CA SiteMinder integration works.



The following information applies to the preceding diagram:

1. CA SDM is configured to use external authentication as a security setting for its users. The CA SiteMinder Web Agent is configured to protect several web resources for the organization. A user attempts to start the CA SDM web interface.

2. The CA SiteMinder Web Agent checks with the CA SiteMinder Policy Server to see whether the /CAisd/pdmweb.exe is a protected resource. If yes, the user is challenged for credentials.

3. The user enters the credentials in the CA SiteMinder login window. The CA SiteMinder Policy Server validates the credentials against the CA Directory-LDAP repository of users, evaluates the entitlements of the user, and grants the appropriate access.

4. The user context is passed to CA SDM and the user is granted access to the secured CA SDM web interface.

Using CA SiteMinder for Resource Protection

This integration uses CA SiteMinder to protect the CA SDM URL resources by creating rules and policies that the CA SiteMinder agent follows. A rule identifies and allows or denies access to specific resources, such as pdmweb.exe, that are included in the policy. A CA SiteMinder policy binds rules and responses to users, groups, and roles. The responses in a policy enable the solution to customize the delivery of content for each user.

Policies reside in the policy store, which is the data source that contains all the CA SiteMinder entitlement information.

The following process provides an overview of how the CA SDM and CA SiteMinder integration works:

1. The user attempts to access a protected resource pdmweb.exe, which is the CA SDM web interface.

2. The user is challenged to enter credentials. The credentials are then sent to the CA SiteMinder Web Agent or to the secure CA SiteMinder Proxy Server.

3. The user credentials are passed to the CA SiteMinder Policy Server.

4. The user is authenticated against the appropriate user store (that is, LDAP or AD).

5. The policy server evaluates the entitlements of the user and grants access.

6. User profile and entitlement information is passed to the CA SDM application.

7. The user receives access to the secured CA SDM web interface.

Integration Points

The integration points from CA SDM and CA SiteMinder include the following points:

- From CA SDM: CA SDM can use external authentication definitions based on CA SiteMinder rules and policies for each CA SDM Access Type.

- From CA SiteMinder: User profile and entitlement information is passed from CA SiteMinder to CA SDM to grant users access to the web interface.

Integration Value

The CA SiteMinder integration provides the following value:

- CA SiteMinder offers the type of solution that organizations need to meet the challenge of building and managing secure websites and reducing the total cost of ownership.

- CA SiteMinder integrates with various directory services and user stores, eliminating redundant administration of user information. This integration simplifies administration and provides unique and comprehensive security capabilities. CA SiteMinder fully leverages existing user directories, from leading LDAP directories and relational databases to mainframe security directories.

- CA SiteMinder supports a comprehensive set of password services, including password composition, dictionary checking, and expiration rules, allowing you to implement robust password management rules. When combined with CA Identity Manager, CA SiteMinder provides self-service password reset services and password synchronization. The integration complements the CA SDM self-service functionality.

Configure Resource Protection for pdmweb.exe

This section describes how to implement the CA SiteMinder integration with CA SDM to centralize the management of user entitlements for CA SDM users across all web servers, through shared services. This integration enforces security policies across the enterprise and eliminates the need for redundant user directories.

The following prerequisites apply to this example:

- CA SDM must be running on IIS as a web server and using Microsoft Internet Explorer as a web browser.

- CA SiteMinder and CA SDM must have been successfully installed and configured.

- LDAP or AD functionality must be already running with all users that can potentially connect to CA SDM belonging to the LDAP or AD domain.
- The CA SDM and CA SiteMinder servers must be able to ping each other.
- The required CA SiteMinder agent ports (44441, 44442, 44443) must be open.

The high-level steps to configure resource protection include the following steps:

1. Configure CA SiteMinder by creating the following items:
   - CA SiteMinder Web Agent
   - CA SiteMinder User Directory
   - CA SiteMinder Domain
   - CA SiteMinder Realm and Rule
   - CA SiteMinder Policy
2. Install a CA SiteMinder Agent on the CA SDM server.
3. Configure the IIS Web Agent.
4. Configure CA SDM.

Configure CA SiteMinder

The following sections describe how to create the Agent, User Directory, Domain, Realm, Rule, and Policy in CA SiteMinder. The procedures in these sections explain just one of a few different ways that you can create these objects. These procedures are included as examples only.

Create a CA SiteMinder Agent: smdemoagent

The following procedure provides an example of how to create a CA SiteMinder agent.

Follow these steps:

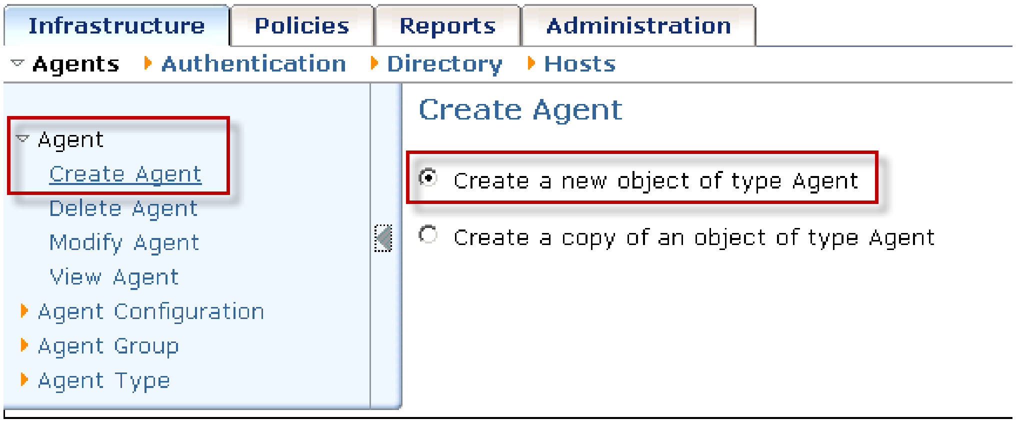
1. Log in to the CA SiteMinder Policy Server as the CA SiteMinder Administrator user. The following URL is the default login URL:

   `http://`*`servername`*`.domain:8080/iam/siteminder/console`

   or

   `https://`*`servername`*`.domain:8443/iam/siteminder/console`
2. Click the Agents link on the Infrastructure tab.

3. Select Create a new object of type Agent and click OK.



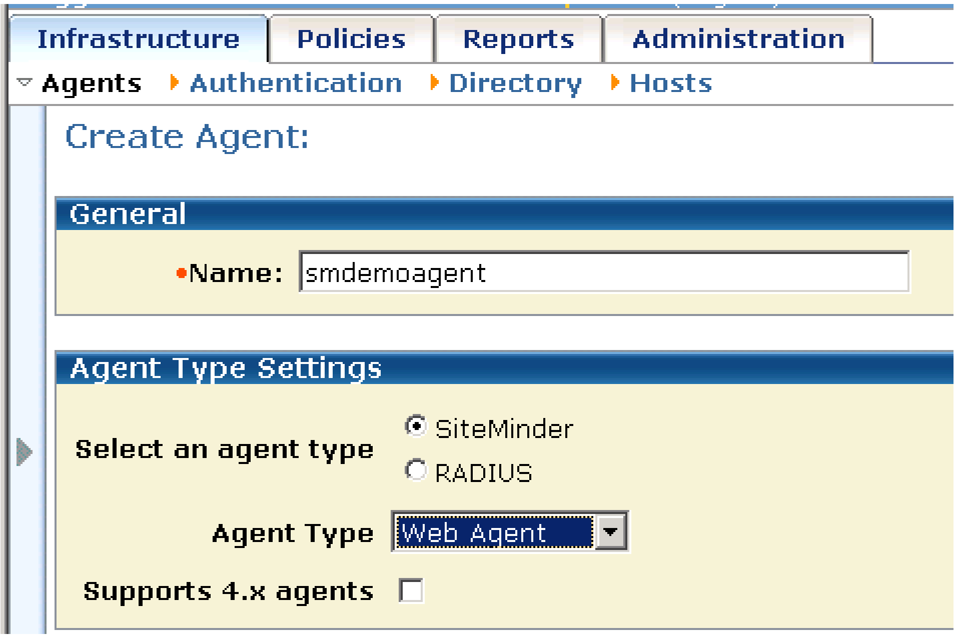
Create Agent

● Create a new object of type Agent

○ Create a copy of an object of type Agent

4. Complete the following fields in the General section:

- Enter a Name for the agent (for example, smdemoagent)
- Select the agent type: SiteMinder
- Select the Agent Type: Web Agent



Create Agent:

General

•Name: smdemoagent

Agent Type Settings

Select an agent type ● SiteMinder ○ RADIUS

Agent Type: Web Agent

Supports 4.x agents □

5. Click Submit.

Create an Agent Configuration: SMDemoACO

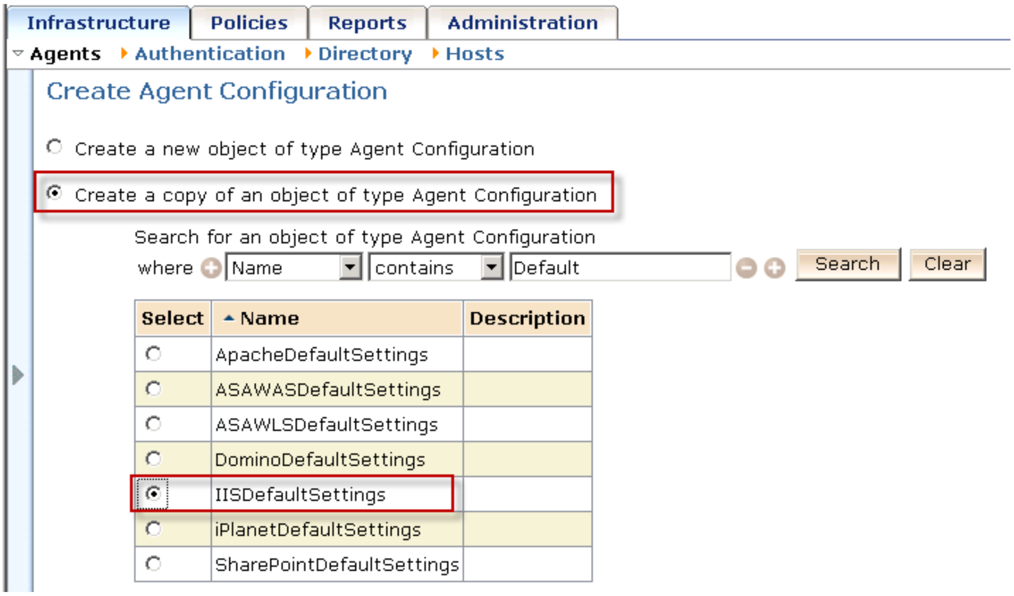
The following procedure provides an example of how to create a CA SiteMinder agent configuration. You can either create an agent configuration or copy an existing one. This integration example uses an existing agent configuration.

Follow these steps:

1. Click the Agents link on the Infrastructure tab.

2. Click Agent Configuration and select Create Agent Configuration.

3. Click Create a copy of an object of type Agent Configuration, select the IISDefaultSettings object, and click OK.



Create Agent Configuration

○ Create a new object of type Agent Configuration

● Create a copy of an object of type Agent Configuration

Search for an object of type Agent Configuration

where Name contains Default

Select	Name	Description
○	ApacheDefaultSettings	
○	ASAWASDefaultSettings	
○	ASAWLSDefaultSettings	
○	DominoDefaultSettings	
●	IISDefaultSettings	
○	iPlanetDefaultSettings	
○	SharePointDefaultSettings	

4. Specify the object name (for example, SMDemoACO).

5. Modify the parameters (Parameters Name) as follows:

CssChecking

Uncomment the parameter name, if commented. Remove the pound sign (#) from the name and set this parameter value to Yes.

DefaultAgentName

Uncomment the parameter name, if commented. Remove the pound sign (#) from the name and set the value of this parameter to the name of the Agent that you created (that is, smdemoagent).

DefaultPassword

Uncomment the parameter name, if commented. Remove the pound sign (#) from the name and set the value of this parameter to the password of the proxy user account that is defined on the IIS web server host.

DefaultUserName

Uncomment the parameter name, if commented. Remove the pound sign (#) from the name and set the value of this parameter to the name of the proxy user account that is defined on the IIS web server host (for example, smproxy).

SetRemoteUser

Set this parameter value to Yes.

Create a User Directory

Create a CA SiteMinder User Directory for authorization, which CA SDM uses to retrieve LDAP attributes. Verify that the UniversallD field uniquely identifies a user in the directory on the User attributes tab.

This example shows how to create a User Directory for Active Directory.

Follow these steps:

1. From the CA SiteMinder Administrative user interface, click the Directory link on the Infrastructure tab.
2. Select User Directory.

   The existing user directories are listed.
3. Select Create User Directory.
4. In the General section, enter a Name for the User Directory, for example, MyADDomain.
5. Under Directory Setup, enter the following details:

   Namespace

   Select the appropriate Namespace. For Active Directory, select AD.

   Server

   Specify the Active Directory host name or IP Address.

6. Under Administrator Credentials, select Require Credentials and enter a user name, such as Administrator. Enter a password that has access to the domain.

7. Under LDAP Settings, enter the LDAP Search and LDAP User DN Lookup information that pertains to your environment. For example:

   - LDAP Search Root: CN=Users,DC=mydomain,DC=com

   - LDAP User DN Lookup Start: (sAMAccountName=

   - LDAP User DN Lookup End:)

8. Under User Attributes, enter a value for Universal ID (R) and Password (RW). These values must match the values in the LDAP. For example, attributes that are defined by Active Directory include uid, sAMAccountName, and userPassword.

   - UniversalID (R): uid or sAMAccountName

   - Password (RW): LDAP directory attribute that CA SiteMinder uses to authenticate a user password (for example, userPassword).

   The following table lists common AD Attributes:

AD Attribute	Description
sAMAccountName	The login name that is used to support clients and servers that are running older versions of the operating system, such as Windows NT 4.0, Windows 95, Windows 98, and LAN Manager.
Uid	A user ID
userPassword	The user password in UTF-8 format. This attribute is a write-only attribute.

9. Save the User Directory.

   The user directory is created.

Create a new Domain

The following procedure provides an example of how to create a CA SiteMinder domain.

Follow these steps:

1. From the CA SiteMinder Administrative user interface, select the Domains link on the Policies tab.
2. Select the Create Domain link under the Domain node.
3. Enter a name for the domain (for example, ServiceDesk).
4. Verify that the Global Policies Apply option is selected.
5. Under User Directories, click Add/Remove, select the user directory that you created, and click OK.
6. Click Submit.

   The domain is created and is associated with the user directory.

Create the Authentication Scheme

An authentication scheme is used as a login page for CA SDM.

Follow these steps:

1. From the CA SiteMinder Administrative user interface, select the Authentication link on the Infrastructure tab.
2. Select the Create Authentication Scheme link under the Authentication node.
3. Select Create a new object of type Authentication Scheme and click OK.
4. Under the General section, complete the following fields:

   Name

      Select a name, for example, Forms Based.

   Authentication Scheme Type

      Select an authentication scheme type, for example, HTML Form Template.

Protection Level

Select a protection level, for example, 5.

Password Policies enabled for this Authentication Scheme

Select this check box.

5. Under Scheme Setup, complete the following fields:

   Web Server Name

   Select the FQDN of the CA SDM server, for example, servername.domain.com.

   Target

   Select the target, for example, /siteminderagent/forms/login.fcc.

6. Click Submit.

   The authentication scheme is created.

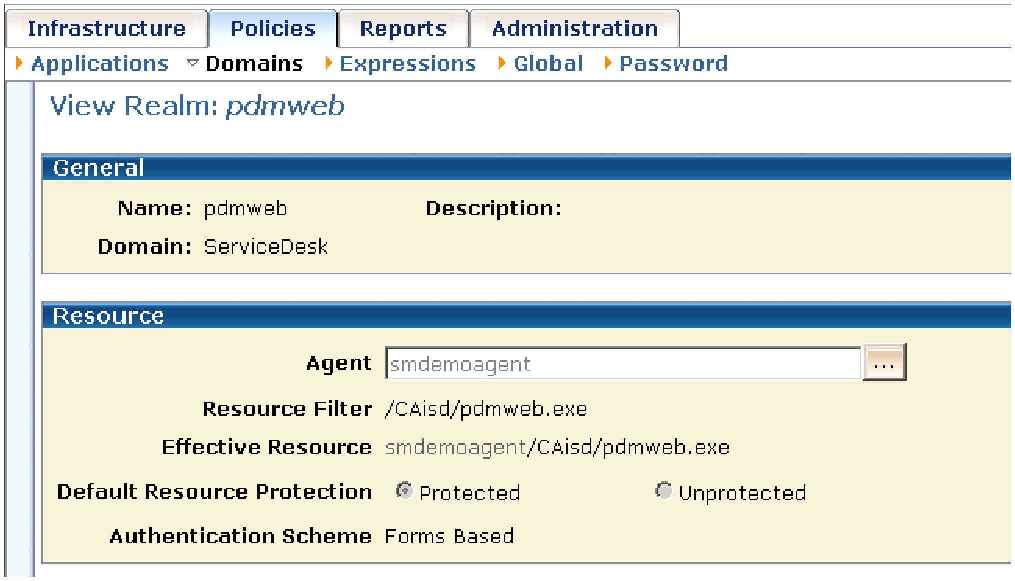
Create a Realm and Rules

A realm protects a resource, for example, pdmweb.exe.

Follow these steps:

1. From the CA SiteMinder Administrative user interface, select the Domains link on the Policies tab.
2. Select the Create Realm link under the Realm node to create the Realm.
   a. Select the Domain created in the previous step (ServiceDesk for example) and click Next.
   b. In the General section, enter a realm Name (servicedesk.realm for example).
   c. Under Resource, select the Agent that was previously created (Smdemoagent for example).
   d. Verify that the Resource filter contains the following information: /CAisd/pdmweb.exe.
   e. Select Protected in the Default Resource Protection option.

f. Select the Authentication Scheme that was created previously (Forms Based for example).



View Realm: *pdmweb*

General

Name: pdmweb

Description:

Domain: ServiceDesk

Resource

Agent: smdemoagent

Resource Filter: /CAisd/pdmweb.exe

Effective Resource: smdemoagent/CAisd/pdmweb.exe

Default Resource Protection: ● Protected ○ Unprotected

Authentication Scheme: Forms Based

3. Create two rules using the following steps and associate the rules with the domain (ServiceDesk) and realm (servicedesk.realm) that you previously created.

4. Under the Rules section, create a rule with the following properties:

   a. Enter a name, for example, ServiceDesk.Protect.

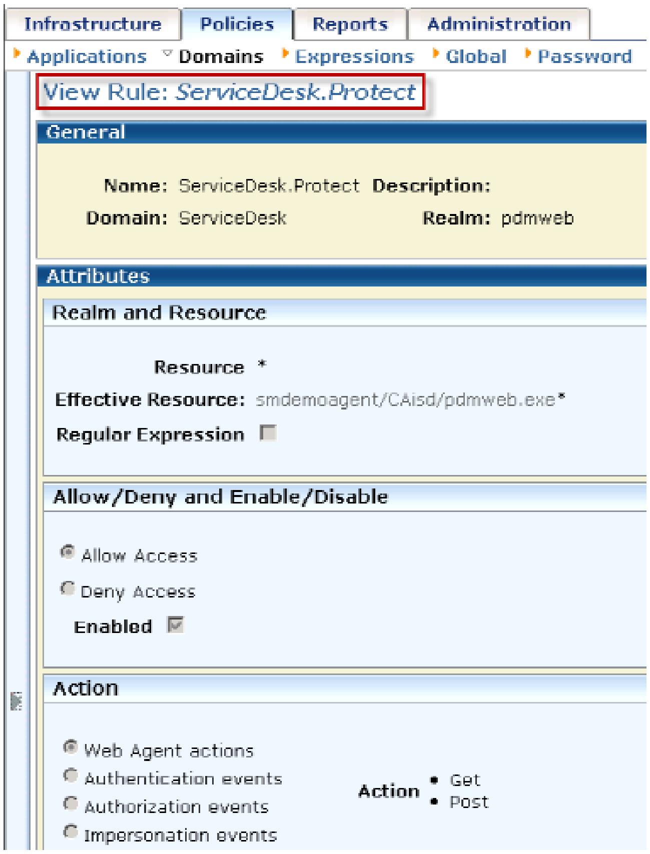
   b. Select the asterisk (*) in the Resource field.

   c. Select Web Agent actions in the Action field, and select Get and Post.

   d. Select Allow Access and Enable options.

e. Click OK.

The following example shows the ServiceDesk.Protect rule with the properties that were previously mentioned.



View Rule: *ServiceDesk.Protect*

General

Name: ServiceDesk.Protect Description:

Domain: ServiceDesk Realm: pdmweb

Attributes

Realm and Resource

Resource *

Effective Resource: smdemoagent/CAisd/pdmweb.exe*

Regular Expression □

Allow/Deny and Enable/Disable

● Allow Access

○ Deny Access

Enabled ☑

Action

● Web Agent actions

○ Authentication events

○ Authorization events

○ Impersonation events

Action
- Get
- Post

5. Create a second rule with the following properties:

   a. Enter a name, for example, ServiceDesk.onAuthAccep.setRemoteUser.

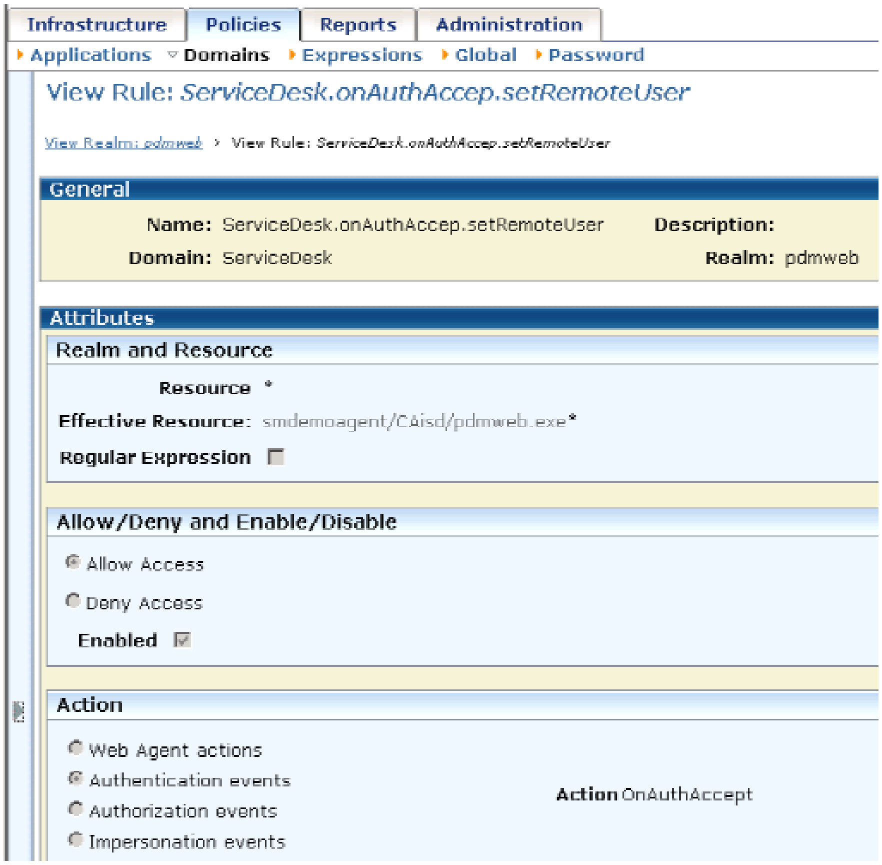
   b. Select the asterisk (*) in the Resource field.

   c. Select the Allow Access and Enabled options.

   d. Select Authentication events under Action and select OnAuthAccep from the drop-down list.

e. Click OK and click Submit.

The following example shows the ServiceDesk.onAuthAccep.setRemoteUser rule with the properties mentioned previously.



View Rule: *ServiceDesk.onAuthAccep.setRemoteUser*

View Realm: *pdmweb* > View Rule: *ServiceDesk.onAuthAccep.setRemoteUser*

General

Name: ServiceDesk.onAuthAccep.setRemoteUser **Description:**

Domain: ServiceDesk **Realm:** pdmweb

Attributes

Realm and Resource

Resource *

Effective Resource: smdemoagent/CAisd/pdmweb.exe*

Regular Expression □

Allow/Deny and Enable/Disable

● Allow Access

○ Deny Access

Enabled ☑

Action

○ Web Agent actions

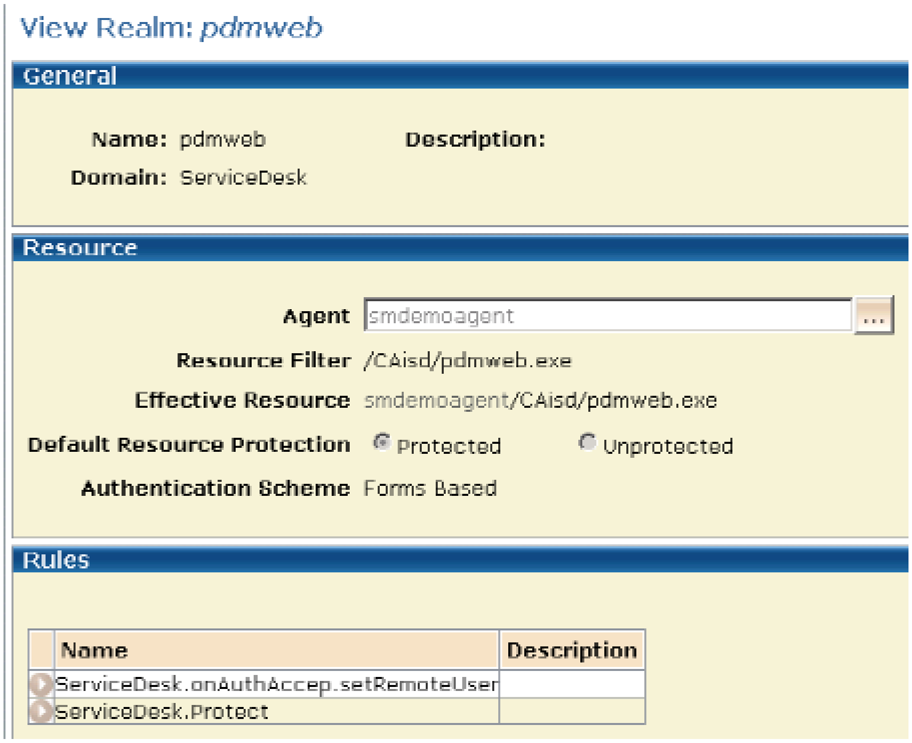
● Authentication events

○ Authorization events

○ Impersonation events

Action OnAuthAccept

The following example shows the realm after the rules have been added.



View Realm: *pdmweb*

General

Name: pdmweb

Description:

Domain: ServiceDesk

Resource

Agent: smdemoagent

Resource Filter: /CAisd/pdmweb.exe

Effective Resource: smdemoagent/CAisd/pdmweb.exe

Default Resource Protection: ● Protected ○ Unprotected

Authentication Scheme: Forms Based

Rules

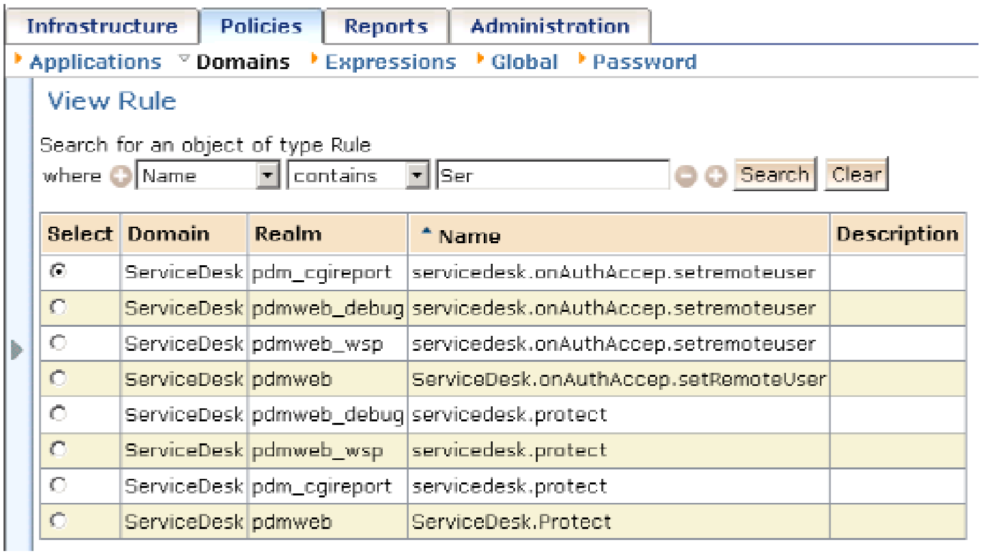
Name	Description
ServiceDesk.onAuthAccep.setRemoteUser	
ServiceDesk.Protect	

6. (Optional) Create additional realms for any other CA SDM URL that needs to be protected, following the same steps as defined in Step 2. You can create the following Resource filters:

   - /CAisd/pdmweb_debug.exe (debug)
   - /CAisd/pdm_cgireport.exe (Report cgi)
   - /CAisd/pdmweb_wsp.exe (Web Screen Painter)
   - /CAisd/pdmweb_d.exe (Web director)
   - /CAisd/pdmweb2.exe (Secondary Servers)

   Note: Each of the new realms will have the same two rules as defined in step 3.

The list of rules could look like the following example.



Search for an object of type Rule

where Name contains Ser

Select	Domain	Realm	Name	Description
●	ServiceDesk	pdm_cgireport	servicedesk.onAuthAccep.setremoteuser	
○	ServiceDesk	pdmweb_debug	servicedesk.onAuthAccep.setremoteuser	
○	ServiceDesk	pdmweb_wsp	servicedesk.onAuthAccep.setremoteuser	
○	ServiceDesk	pdmweb	ServiceDesk.onAuthAccep.setRemoteUser	
○	ServiceDesk	pdmweb_debug	servicedesk.protect	
○	ServiceDesk	pdmweb_wsp	servicedesk.protect	
○	ServiceDesk	pdm_cgireport	servicedesk.protect	
○	ServiceDesk	pdmweb	ServiceDesk.Protect	

Create a Policy

The following procedure provides an example of how to create a CA SiteMinder policy.

Follow these steps:

1. From the CA SiteMinder Administrative user interface, select the Domains link on the Policies tab.
2. Select the Create Policy link under the Policy node.
   a. Select the Domain created in the previous step (ServiceDesk for example) and click Next.
   b. Specify a name for the policy (servicedesk.policy, for example) and select the Enabled option.
   c. Click Next and select the user or group that will require access. For example, select Add All.
   d. Click Next, click Add Rule, and select the two rules that were previously created:
   - ServiceDesk.Protect
   - ServiceDesk.onAuthAccep.setRemoteUser
3. Click OK, Next, and Finish.

Install a CA SiteMinder Agent on the CA SDM Server

The CA SiteMinder Agent must be installed on the CA SDM server where CAisd virtual directory is running. You can download the agent from http://ca.com/support.

Follow these steps:

1. Verify the version of CA SiteMinder that is running on the CA SiteMinder Policy Server before downloading the agent.

   The version information is located in the *SMPS_ROOT*\install_config_info\ca-ps-version.info file. *SMPS_ROOT* is C:\Program Files\CA\siteminder by default.

2. Log in to http://ca.com/support and navigate to the CA SiteMinder product page.

3. Under Recommended Reading, click the "CA SiteMinder Hotfix/Cumulative Release Index".

4. Click the SiteMinder Web Access Manager Agents link. Download the agent level that is at the same version as or below the version of Policy Server.

5. Unzip the appropriate zip file after the download is complete. For example, unzip one of the following files:

■ smwa-12.0.1.XX-win32.zip	for Windows 2003, 32 bit x86
■ smwa-12.0.1.XX-win64.zip	for Windows 2003, 64 bit x64

6. Run the executable.

7. Run the CA SiteMinder Web Agent executable and follow the instructions in the wizard. Remember to select the following options in the installation wizard:

   a. If you are prompted to overwrite existing files, click No to All.

   b. On the Host Registration screen, select No and click Next.

8. Restart the CA SDM server.

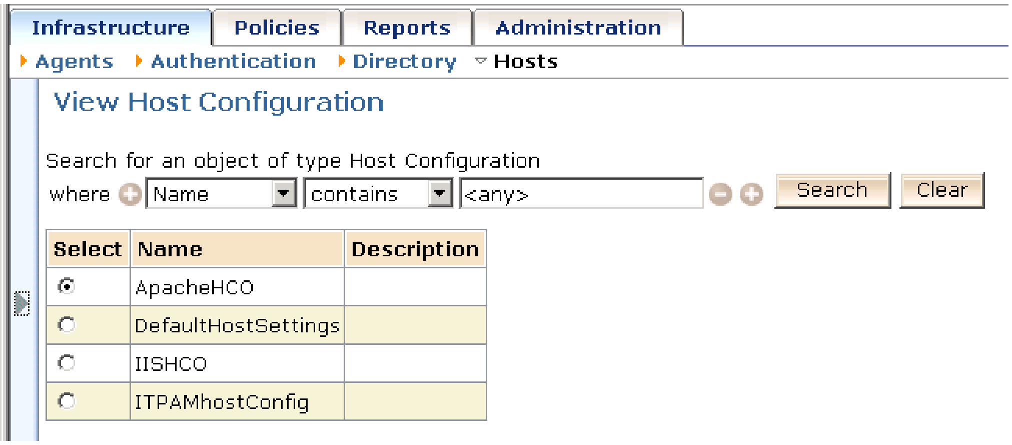
   The CA SiteMinder agent is installed.

Configure the IIS Web Agent

Follow these steps:

1. Run the CA SiteMinder Web Agent Configuration.
2. Execute the client configuration that is located in the following directory structure:

   ```
   C:\Program Files\CA\webagent\install_config_info\ca-wa-config.exe
   ```
3. Select Yes for host registration and click Next.
4. Enter the Admin User Name, for example SiteMinder. Enter the password in the Admin Registration page and click Next.
5. Provide the following information on the Trusted Host Name and Configuration Object page:
   - Enter the hostname of your CA SDM server in the Trusted Host Name field.
   - Enter the name of the Host Configuration Object. Log in to the CA SiteMinder user interface and view the Host Configuration list to verify the Host Configuration Object name to use.

   View Host Configuration

   Search for an object of type Host Configuration

   where Name contains <any>

Select	Name	Description
●	ApacheHCO	
○	DefaultHostSettings	
○	IISHCO	
○	ITPAMhostConfig	

6. Click Next. In the Policy Server IP Address, enter the hostname or IP address of the CA SiteMinder Policy server and click Next.
7. Select the FIPS Compatibility Mode and click Next.
8. Enter SmHost.conf for File name on the Host Configuration file location page and select C:\Program Files\CA\webagent\config as the path for the host configuration file. Click Next.
9. Select the web server to configure (that is, Microsoft IIS 6.0 or 7.0) on the Select Web Server(s) page.

10. Verify the Agent Configuration Name and enter it on the Agent Configuration Object window (that is, SMDemoACO).

11. Select No on the Self Registration page and click Next.

12. Click Install on the Web Server Configuration Summary page.

13. Click Done on the Configuration Complete page.

Note: There is no downloadable CA SiteMinder Tomcat agent, so the CA SDM installation must be configured with IIS. If IIS is not in the environment, a custom CA SiteMinder Tomcat agent can be obtained and implemented with the assistance of CA Technologies Services. You can also use a CA SiteMinder secure proxy server, instead of IIS. You can also set up Apache to redirect requests to Tomcat and use the CA SiteMinder Apache agent. These options are not discussed further in this chapter, but they can be implemented with the help of CA Technologies Services.

Configure CA SDM

The following section describes how to configure CA SDM for this integration.

Configure User Authentication through CA SiteMinder IIS Agent

You must configure the user authentication for CA SDM contacts to allow an external authentication system to authenticate the users. Complete the following procedure for each CA SDM Access Type that will use CA SiteMinder for authentication (for example, Administration, Employee, Analyst, IT Staff).

Follow these steps:

1. Log in to CA SDM as an Administrator.

2. From the Administration tab, expand the Security and Role Management node and select Access Types.

3. Open an Access Type in edit mode and click the Web Authentication tab.

4. Select the Allow External Authentication check box.

5. Click OK.

Set up External Authentication using IIS

Complete the following steps to set up external authentication using IIS on the CA SDM server hosting the virtual directory.

Follow these steps:

1. Create a proxy user that can access the CA SDM virtual directory.

   Note: An example proxy user can be *smproxy*. This user should be created in Active Directory if there is one, or on the local server hosting CA SDM.

2. Add the proxy user *smproxy* as a member of the Administrators group. Also add either the Users of the local server, if the account is a local non-domain account, or Domain Users of the AD Domain.

3. Update the User Rights Assignment policy.

   a. If AD is installed on the CA SDM server, click Start, All Programs, Administrative Tools, Domain Security Policy. Expand the Local Policies node and click User Rights Assignment.

   b. If AD is not installed on the CA SDM server, click Start, All Programs, Administrative Tools, Local Security Policy. Double-click the option named Act as part of the Operating System. Add the smproxy user or DOMAIN\smproxy.

Set the CA SDM Logout URL

Update the logout URL to prevent a user from logging out and then having access to the out-of-the-box CA SDM login screen. This access would bypass the CA SiteMinder authentication.

Follow these steps:

1. On the CA SDM server, find and open the web.cfg file that is located under the install directory in \bopcfg\www.

2. Search for the Logout URL parameter and update the value of the URL to something other than the default login screen for CA SDM. The URL can be set to a portal, your company main web page or intranet site, or the CA SiteMinder login screen that is used to authenticate CA SDM users.

3. Recycle the CA SDM server service.

Block Access to the Tomcat Login Screen

If CA SiteMinder is protecting the login to CA SDM on IIS only, you must block access to login through Tomcat. Using Windows Firewall or a similar tool, block the port that is used to log in to CA SDM through Tomcat. The default port for the Tomcat login is 8080. The default Tomcat login URL is http://*servername*:8080/CAisd/pdmweb.exe.

Enable the CA SiteMinder agent

Follow these steps:

1. Open the WebAgent.conf file under *install directory*\webagent\bin\IIS.
2. Specify Yes for the EnableWebAgent option and save the file.
3. Restart IIS or the World Wide Web Publishing Service. The CA SiteMinder agent process, LLAWP.exe, will run when a request to access the CA SDM interface is made. The agent automatically starts when the request comes through IIS.

Test the Integration

Test the integration to verify that the CA SiteMinder integration has been set up correctly.

Follow these steps:

1. Log in to the CA SDM web client and validate that a CA SiteMinder login window opens.
2. Enter the user name and password to log in to CA SDM.
3. Validate that the CA SDM web interface main window opens.

Integration Summary

Organizations can manage access to CA SDM by integrating with CA SiteMinder. Real-time transactional security and integrated web services with CA SiteMinder eTelligent rules enable security policies that evaluate dynamic data from various local or external sources, including web services and databases, in real time. Cost and complexity are reduced by eliminating advanced security logic from web applications and centralizing it within CA SiteMinder policies.

User Directory Reference: CA EEM References CA SiteMinder Users

The second integration scenario allows CA SDM contacts to authenticate using CA EEM. This scenario is documented in the *CA Service Desk Manager Administration Guide*. In this scenario, CA EEM is configured to reference CA SiteMinder as the external directory.

Integration Points

The following points are the integration points from CA SDM:

- CA SDM contacts are authenticated by CA EEM while CA EEM is configured to point to CA SiteMinder for directory information.
- The CA SDM login page is used in this scenario.

The following point is the integration point from CA SiteMinder:

- CA SiteMinder directory information is shared with CA EEM to authenticate CA SDM users accessing the web interface.

Integration Value

The CA SiteMinder integration provides the following value:

- CA SiteMinder integrates with various directory services and user stores, eliminating redundant administration of user information. This integration simplifies administration and provides unique and comprehensive security capabilities. CA SiteMinder fully leverages existing user directories, from leading LDAP directories and relational databases to mainframe security directories.
- CA SiteMinder supports a comprehensive set of password services, including password composition, dictionary checking, and expiration rules, allowing you to implement robust password management rules. When combined with CA Identity Manager, it provides self-service password reset services, and password synchronization. The integration complements the CA SDM self-service functionality.

How to Configure User Directory Reference

CA EEM is a central repository of user information known as identities. CA EEM defines user authentication and access to other applications. If you have several CA products installed, some of them can use CA EEM to store identities and access policies. CA SDM uses only CA EEM for authentication. Additionally, the CA EEM server can be configured to reference global users and global groups from CA SiteMinder. For more information about how to configure CA SDM to authenticate users through CA EEM, see the *CA Service Desk Manager Administration Guide*.

This section describes how to integrate CA SiteMinder and CA EEM for CA SDM authentication. The following high-level steps are involved in the configuration:

1. Configure CA SiteMinder by creating the following items:
   - CA SiteMinder Web Agent
   - CA SiteMinder User Directory
   - CA SiteMinder Domain
   - CA SiteMinder Realm and Rule
   - CA SiteMinder Policy
2. Configure CA EEM to use the CA SiteMinder user store.
3. Configure CA SDM to authenticate through CA EEM.

To perform the steps in this section, you must have CA SiteMinder, CA EEM, and CA SDM installed and working. For information about installing CA EEM, see the *CA Embedded Entitlements Manager Implementation Guide*.

Configure CA SiteMinder

The following sections document in detail how to create the Agent, User Directory, Domain, Realm, Rule, and Policy in CA SiteMinder. The steps in these sections are just one of a few different ways to create these objects and are included as examples only.

Create a CA SiteMinder Agent

From the CA SiteMinder Administrative user interface, create a CA SiteMinder Web Agent for communication between CA EEM and CA SiteMinder policy server.

Follow these steps:

1. From the CA SiteMinder Administrative user interface, select the Agents link on the Infrastructure tab.
2. Select Create a new object of type Agent, and click OK.
3. Provide the following information in the General section:
   a. Enter a name for the agent (for example, eemagent).
   b. Select the agent type as SiteMinder.
   c. Select the Agent Type as Web Agent.
   d. Select the Supports 4.x agents option.
   e. Enter the IP Address of the CA EEM server.
   f. Enter a Shared Secret. This entry must match what will be entered in CA EEM when configuring the CA EEM Server Global Users/Global Groups.
4. Click Submit.

Create a User Directory

Create a CA SiteMinder User Directory for authorization, which is used by CA EEM to retrieve LDAP attributes. Ensure that the UniversalID field uniquely identifies a user in the directory on the User attributes tab.

For more information about creating a user directory, see Create a User Directory (see page 194).

Create a Domain

Create a domain for CA EEM and associate the user directory that you created for CA EEM. For more information about creating a domain, see Create a new Domain (see page 196).

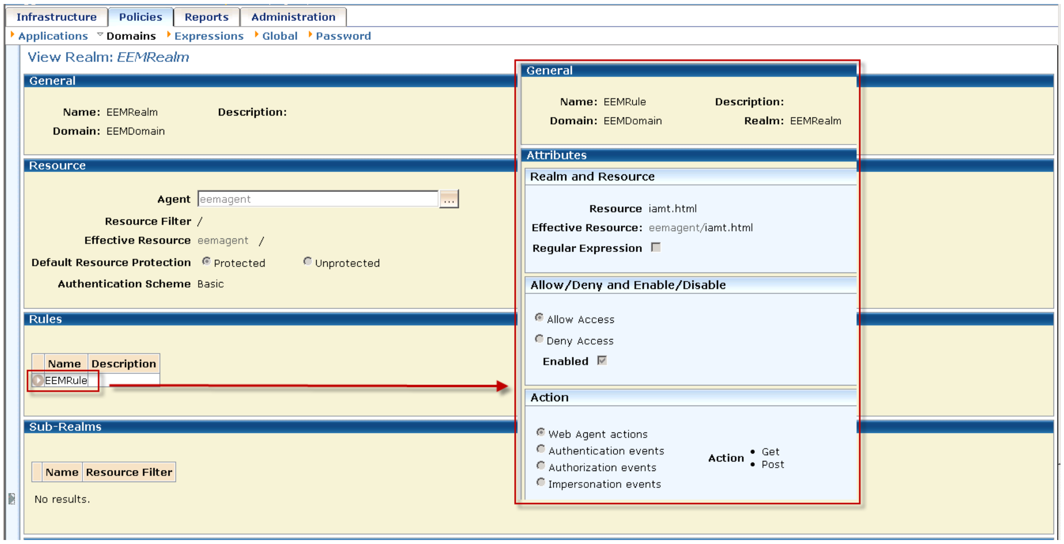
Create the Realm and Rule

Follow these steps:

1. From the CA SiteMinder Administrative user interface, select the Domains link on the Policies tab.
2. Select the Create Realm link under the Realm node to create the realm.
    a. Select the Domain created in the previous procedure and click Next.
    b. In the General section, enter a realm name (for example, EEMRealm).
    c. Under Resource, select the Agent that was previously created (for example, Eemagent).
    d. Enter a backslash (\) for the Resource filter.
    e. Select Protected in the Default Resource Protection field.
    f. Select an Authentication Scheme (for example, Basic).
3. Create a Rule for the realm by clicking Create and providing the following information:
    a. Enter a Name (for example, EEMRule).
    b. Under Attributes, enter iamt.html as the Resource.
    c. Select the Allow Access and Enabled options.
    d. Under Action, select Web Agent actions and select Get and Post in the Action box.

The realm and rule are created.

The following example shows a new Realm and Rule.



View Realm: *EEMRealm*

General

Name: EEMRealm **Description:**
Domain: EEMDomain

Resource

Agent eemagent
Resource Filter /
Effective Resource eemagent /
Default Resource Protection ● Protected ○ Unprotected
Authentication Scheme Basic

Rules

Name	Description
EEMRule	

Sub-Realms

Name	Resource Filter

No results.

General

Name: EEMRule **Description:**
Domain: EEMDomain **Realm:** EEMRealm

Attributes

Realm and Resource

Resource iamt.html
Effective Resource: eemagent/iamt.html
Regular Expression □

Allow/Deny and Enable/Disable

● Allow Access
○ Deny Access
Enabled ☑

Action

● Web Agent actions
○ Authentication events
○ Authorization events
○ Impersonation events

Action • Get • Post

Create a Policy

Follow these steps:

1. From the CA SiteMinder Administrative user interface, select the Domains link on the Policies tab.
2. Select the Create Policy link under the Policy node.
3. Select the Domain that you previously created, EEMDomain for example, and click Next.
4. Under the General section, enter the policy name (for example, EEMPolicy) and click Next.
5. Create the User Directories by selecting the Members to include in each User Directory. For example, click the Add All button under the user directory that you just created.
6. Click Next. Add a Rule for the Policy by selecting the Add Rule button.
7. Select the Rule in the list you just created and click OK.
8. Click Next and click Finish.

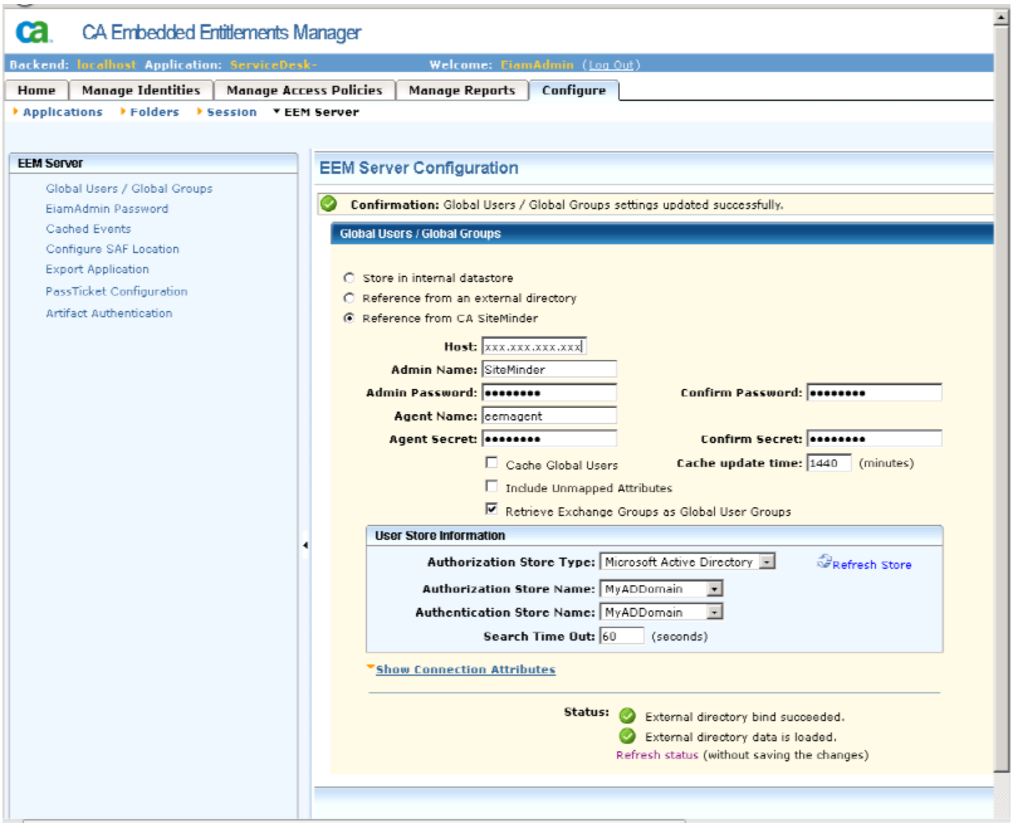
Configure the EEM Server to Reference CA SiteMinder

Follow these steps:

1. Log in to the CA EEM user interface.
2. On the Configure tab, select EEM Server.
3. On the left pane, select Global Users/Global Groups.
4. On the right pane, select Reference from CA SiteMinder and enter the following values:
   - Host: IP Address of the CA SiteMinder server
   - Admin Name: CA SiteMinder Administrator name (for example, SiteMinder)
   - Admin Password: CA SiteMinder Administrator password
   - Agent Name: SiteMinder Web Agent created (for example, Eemagent)
   - Agent Secret: Secret entered during Web Agent creation (for example: secret)
5. Select the Retrieve Exchange Groups as Global User Groups check box.
6. Click Save.

7. Click Refresh Store under User Store Information and select the appropriate Store Name from the drop-down list.

   The status must confirm a successful bind, as shown in the following example.



EEM Server Configuration

Confirmation: Global Users / Global Groups settings updated successfully.

Global Users / Global Groups

○ Store in internal datastore
○ Reference from an external directory
● Reference from CA SiteMinder

Host: xxx.xxx.xxx.xxx
Admin Name: SiteMinder
Admin Password: •••••••• Confirm Password: ••••••••
Agent Name: eemagent
Agent Secret: •••••••• Confirm Secret: ••••••••
□ Cache Global Users Cache update time: 1440 (minutes)
□ Include Unmapped Attributes
☑ Retrieve Exchange Groups as Global User Groups

User Store Information

Authorization Store Type: Microsoft Active Directory
Authorization Store Name: MyADDomain
Authentication Store Name: MyADDomain
Search Time Out: 60 (seconds)

Status: External directory bind succeeded.
External directory data is loaded.
Refresh status (without saving the changes)

8. Navigate to the Users node on the Manage Identities tab and click the Go button.

9. Validate that the users are listed.

Configure CA SDM to Authenticate Using CA EEM

CA SDM uses CA EEM only for authentication. If you integrate CA SDM with CA EEM, the operating system authentication is replaced with CA EEM authentication for CA SDM users.

To integrate CA EEM and CA SDM, you must set the *eiam_hostname*, *use_eiam_artifact*, and *use_eiam_authentication* options in Options Manager, Security. For more information about these options, see the CA SDM Online Help.

In addition, you must configure an Access Type in CA SDM to authenticate through CA EEM. Configure an Access Type with a Validation Type of CA EEM. Set a user in CA SDM to use that Access Type.

Test the Integration

To test the integration, log in to CA SDM with a user account that meets the following conditions:

- The user exists in CA SDM as a contact.
- The user has an Access Type set with a Validation Type of CA EEM.
- The user exists in the User Directory that is referenced by the CA SiteMinder agent.

A successful login indicates that the integration was successful.

Integration Summary

Organizations can manage access to CA SDM by integrating CA EEM with CA SiteMinder. The CA EEM repository of user records can be configured to use an external LDAP directory such as CA SiteMinder.

If your organization uses a directory server, such as CA SiteMinder, consider configuring CA EEM to use the directory for its user base. This configuration makes the users in your directory accessible by any other application that uses CA EEM to centralize access management.

Troubleshooting

Enable Logging

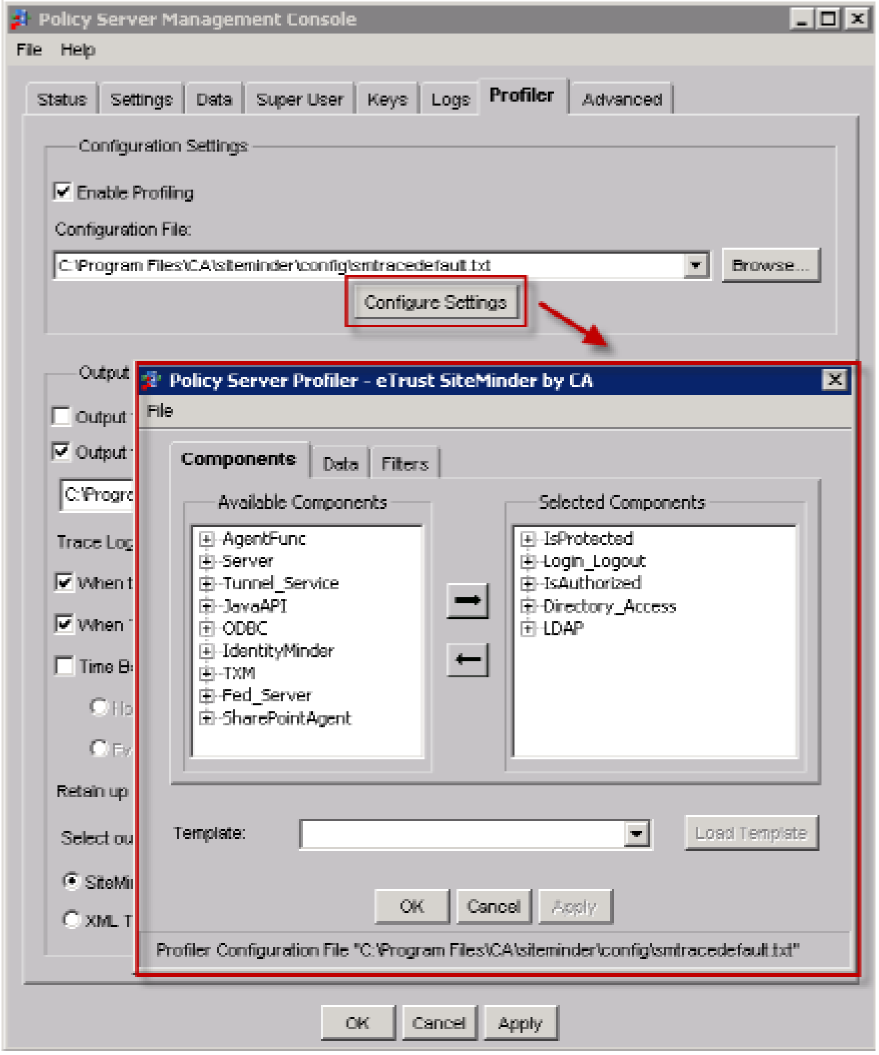
You can add some additional components to the Policy Server Profiler to enable logging for help in troubleshooting.

Follow these steps:

1. Log in to the CA SiteMinder Policy Server Management Console.
2. Click the Profiler tab and select Enable Profiling under the Configuration Settings.

3. Click Configure Settings.

   The Policy Server Profiler dialog opens with the selected components. In the following example, IsProtected, Login_Logout, and IsAuthorized are included in the Selected Components.



☑ Enable Profiling

Configuration File: C:\Program Files\CA\siteminder\config\smtracedefault.txt

Selected Components:

- IsProtected
- Login_Logout
- IsAuthorized
- Directory_Access
- LDAP

Profiler Configuration File "C:\Program Files\CA\siteminder\config\smtracedefault.txt"

Review Log Files

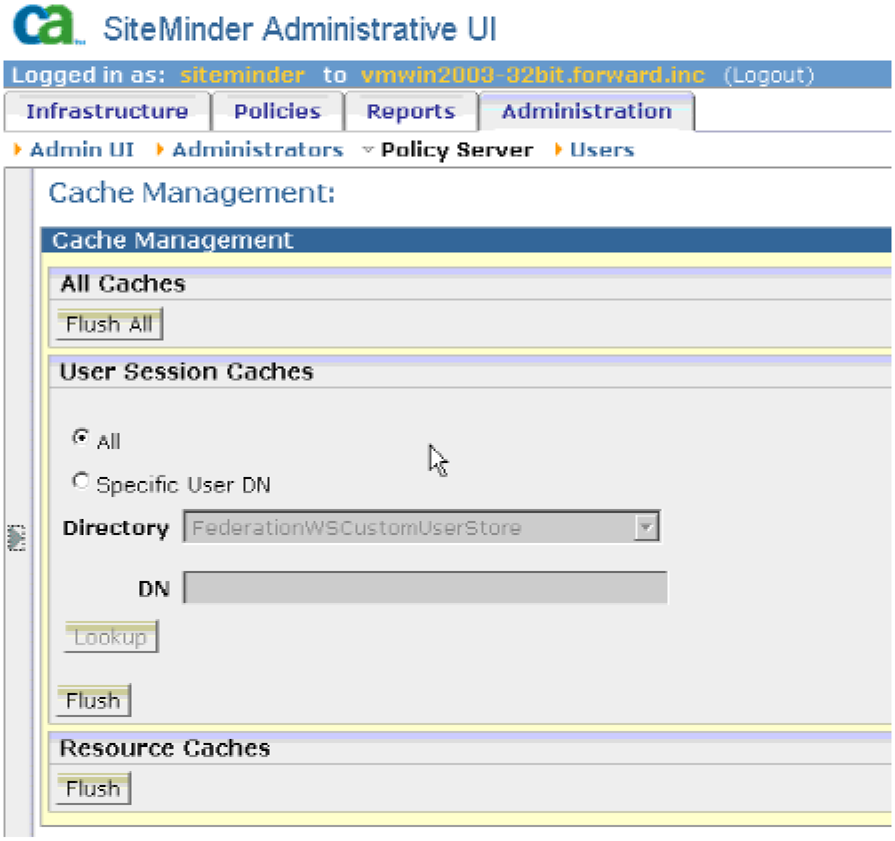
CA SiteMinder Agent log and trace file information can be added through the Agent Configuration parameters. Define the following parameters for the Agent Configuration to turn on logging for CA SiteMinder Agents:

- Logfile: yes
- LogFileName: Enter a path location for the file (for example, C:\temp\sm.log).

- TraceFile: yes
- TraceFileName: Enter a path for the file (for example, C:\temp\smtrace.log).

Flush the Cache

If recent policy changes are not being read by the agent, flush the Policy Server cache. Then restart the World Wide Web Publishing Service on the CA SDM server. The following example shows how to flush the cache.



Logged in as: siteminder to vmwin2003-32bit.forward.inc (Logout)

● All

○ Specific User DN

Directory: FederationWSCustomUserStore

DN:

Extending the Integration to Include CA Identity Manager

CA SiteMinder supports a comprehensive set of password services including password composition, dictionary checking, and expiration rules, allowing you to implement robust password management rules. When combined with CA Identity Manager, it provides self-service, forgotten password services, and password synchronization. The integration complements the CA SDM self-service functionality.

See the CA Identity Manager integration chapter in this book for instructions on configuring this integration with CA SDM.

Extending the Integration to Include CA Process Automation for Single Sign On

This section provides the instructions for extending the integration to include CA Process Automation in the single sign-on environment managed by CA SiteMinder.

Prerequisites for the Integration

The following list includes the prerequisites for the integration:

- CA SDM Release 12.5 or 12.6 is installed, configured, and working.
- LDAP-compatible server is a repository of users/groups (for example, Apache OpenLDAP or Microsoft Active directory) for both CA EEM and CA SiteMinder user data stores.
- CA SiteMinder Policy Server Release 12.0 SP3 is installed, configured, and integrated with an LDAP source.
- Single Sign-on for CA SDM through CA SiteMinder is configured with either of the following agents:

  – IIS SiteMinder Agent working in the environment where CA SDM uses Tomcat and IIS http servers that are configured for the web interfaces.

  – Apache SiteMinder Agent working in the environment where CA SDM uses a Tomcat http server that is configured for the web interfaces with Apache redirect configured.
- CA Process Automation 3.0 SP01 is configured with an orchestrator cluster on two nodes with Apache HTTP Load balancer deployed on a third server or a standalone CA Process Automation server is configured and working.
- CA EEM Release 8.4.217 is installed on a separate server, integrated with the LDAP server.

How to Configure CA SiteMinder to Handle Sign-on Requests

You can configure CA SiteMinder to handle sign-on requests from the CA Process Automation Apache Load Balancer. The configuration involves the following high-level procedures:

1. Create an agent. (see page 220)
2. Create an agent configuration. (see page 221)
3. Create a host configuration. (see page 221)
4. Create a user directory. (see page 222)
5. Create an authentication scheme. (see page 222)
6. Create a domain. (see page 223)
7. Create a realm. (see page 223)

CA SiteMinder Prerequisites

CA SiteMinder provides Single Sign-on capability across single- and multiple-cookie domains. This capability lets users access applications across different web servers and platforms with a single sign-on.

To install CA Process Automation with CA SiteMinder, ensure that the following prerequisites are met:

- A CA EEM server is integrated with the same LDAP/AS that is used as a user store in the policy server.
- A CA SiteMinder Web Agent must be integrated with either IIS or Apache.

For more information, see the *CA SiteMinder WebAgent Installation Guide*.

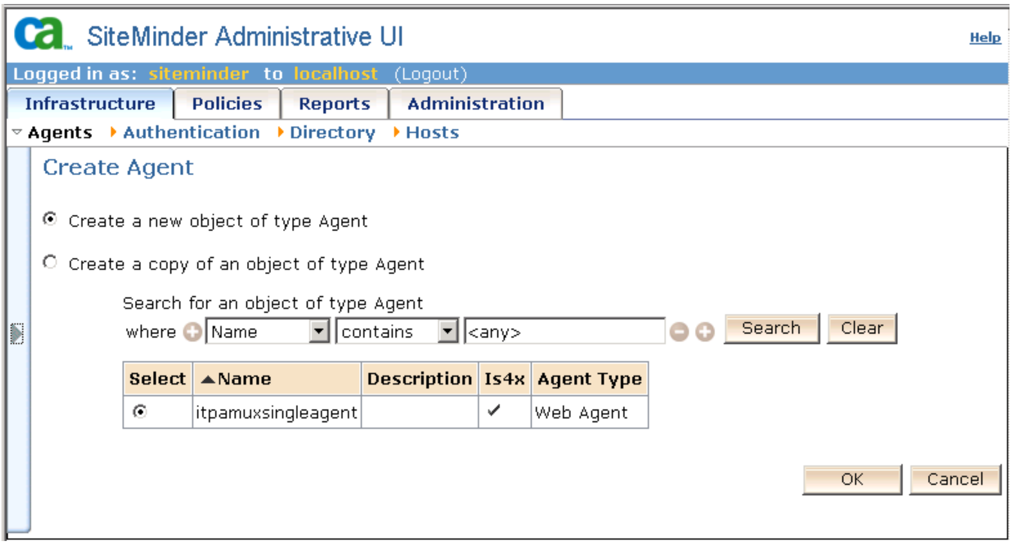
Note: The configuration settings in the following sections are performed using the CA SiteMinder Administrative user interface web-based application. The application is available as a separate download from the Support site and runs on a separate instance of the JBoss server that needs to be downloaded and installed as well.

Create an Agent

Follow these steps:

1. Start the CA SiteMinder Policy Server user interface.
2. Click Start, Programs, CA, SiteMinder, SiteMinder Administrative User Interface.
3. Log in as a CA SiteMinder administrative user (for example, SiteMinder).
4. Click the Infrastructure tab.
5. Click the Agent and select Create Agent.
6. Select Create a new object of type Agent and click OK.

   The following example shows the Create Agent page with the details.



Create Agent

● Create a new object of type Agent

○ Create a copy of an object of type Agent

Search for an object of type Agent

where Name contains <any>

Select	Name	Description	Is4x	Agent Type
●	itpamuxsingleagent		✓	Web Agent

7. Provide the following information for the agent on the next page:
   a. Name: itpamagent
   b. Select an agent type: SiteMinder
   c. Agent Type: Web Agent
   d. Supports 4.x agents: Selected
   e. IP Address: IP Address of the CA Process Automation Load Balancer
   f. Shared Secret: Secret for agent registration authentication
8. Click Submit.

Create an Agent Configuration

Follow these steps:

1. Click the Agent Configuration menu and select Create Agent Configuration.
2. Specify the following information:
    a. Select Create a Copy of an Object of type Agent Configuration.
    b. Select ApacheDefaultSettings as the source of Agent configuration.
    c. Click OK.
3. Change the name to ITPAMagentConfig.
4. Select #Default Agent Name and perform the following steps:
    a. Remove the # sign from the name.
    b. Set the Value to ITPAMagent.
    c. Click OK.
5. Navigate to the BadUrlChars property and remove the "/." and "//" from the value.
6. Navigate to the IgnoreExt property and remove the ".gif, .jpg, .jpeg, .png" from the value.
7. Navigate to the LogoffUri property, remove the # sign from the name, if necessary, and add the value /itpam/Logout.
8. Click Submit in the Agent Configuration form.

Create a Host Configuration

Follow these steps:

1. Click Hosts on the Infrastructure tab.
2. Click Host Configuration and select Create Host Configuration.
3. Specify the following information:
    a. Select Create a copy of an object of type Host Configuration.
    b. Select DefaultHostSettings.
    c. Click OK.

4. Change the Name to ITPAMhostConfig.
5. Enter the Policy Server IP addresses and change ports as needed.
6. Click Submit.

Create a User Directory

Follow these steps:

1. Click Directory on the Infrastructure tab.
2. Click User Directory and select Create User Directory.
3. Enter the name as ITPAMuserDirectory and provide the following information:

    a. Namespace: Enter the namespace (for example, LDAP).

    b. Server: IP or hostname of the LDAP server

    c. Use authenticated user's security context: Selected

    d. For LDAP settings, set Root: dc=forward, dc=inc (You can change this value depending on the LDAP root level in your environment.)

    Note: You can create an alternative layout for this screen by using the following values for the LDAP Root: ou=Global Groups, ou=system

    e. Start: (uid=

    f. End:)

4. Click Submit.

Create an Authentication Scheme

Follow these steps:

1. Click Authentication on the Infrastructure tab.
2. Click Authentication Scheme and select Create Authentication Scheme.

3. Select Create a new object of type Authentication Scheme and click OK.

4. Complete the following fields:

   a. Name: ITPAMauthenScheme

   b. Authentication Scheme Type: HTML Form Template

   c. Web Server Name: Web Server where CA SiteMinder WebAgent software is installed.

   d. Port: 80, by default

   e. (Optional) Use SSL connection: Selected (if HTTP server is set up for SSL communication)

5. Click Submit.

Create a Domain

Follow these steps:

1. Click the Policies tab.

2. Click Domains on the Policies tab.

3. Click Domain and select Create Domain.

4. Enter a Name (for example, ITPAMdomain).

5. Click Add/Remove under User Directories.

6. Select the ITPAMuserDirectory that you previously created.

7. Click the right directional arrow to add the user directory to the right column.

8. Click OK.

Create a Realm

Follow these steps:

1. Click the Realms tab, under Create Domain.

2. Click Create Realm.

3. Enter a name for the Realm (for example, ITPAMrealm).

4. Click the ellipsis (…) button to select an agent.

5. Select the itpamagent.

6. Click OK and provide the following information:

    a. Resource Filter: /itpam/

    b. Authentication Scheme: ITPAMauthenScheme

7. Click Create under Rules and provide the following information:

    a. Name: ITPAMrule

    b. Resource: "*"

    c. Resources value: itpamagent/itpam/*

    d. Web Agent Actions: Select all actions (Get, Post, Put, ProcessSOAP, ProcessXML)

8. Click OK.

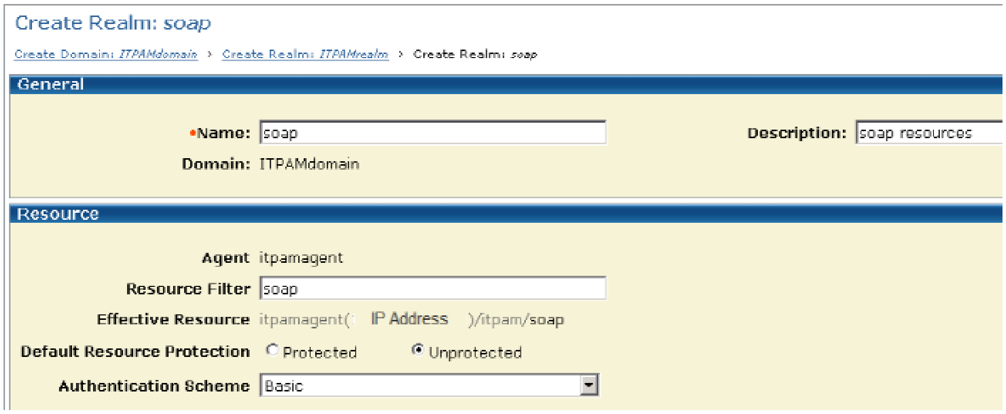
9. Create unprotected subrealms within the ITPAMRealm. Use the following subrealm settings as a sample.

10. Create additional protected subrealms as shown in the following table:

Domain	Name	Agent	Resource Filter
ITPAMdomain	soapAttachment	itpamagent	soapAttachment
ITPAMdomain	genericNoSecurity	itpamagent	genericNoSecurity
ITPAMdomain	swaref	itpamagent	swaref.xsd
ITPAMdomain	js	itpamagent	js
ITPAMdomain	css	itpamagent	css
ITPAMdomain	Images	itpamagent	images
ITPAMdomain	StartAgent	itpamagent	StartAgent
ITPAMdomain	ServerConfigurationRequest Servlet	itpamagent	ServerConfigurationRequest Servlet
ITPAMdomain	Itpamclient	itpamagent	itpamclient
ITPAMdomain	AgentConfigurationRequest Servlet	itpamagent	AgentConfigurationRequest Servlet
ITPAMdomain	MirroringRequestProcessor	itpamagent	MirroringRequestProcessor

Note: The ITPAMrealm contains the resources that end with "/". You do not need to add a leading "/" before the resource names.

The following example shows a sample subrealm.



Create Realm: *soap*

Create Domain: *ITPAMdomain* › Create Realm: *ITPAMrealm* › Create Realm: *soap*

General

•Name: soap

Description: soap resources

Domain: ITPAMdomain

Resource

Agent itpamagent

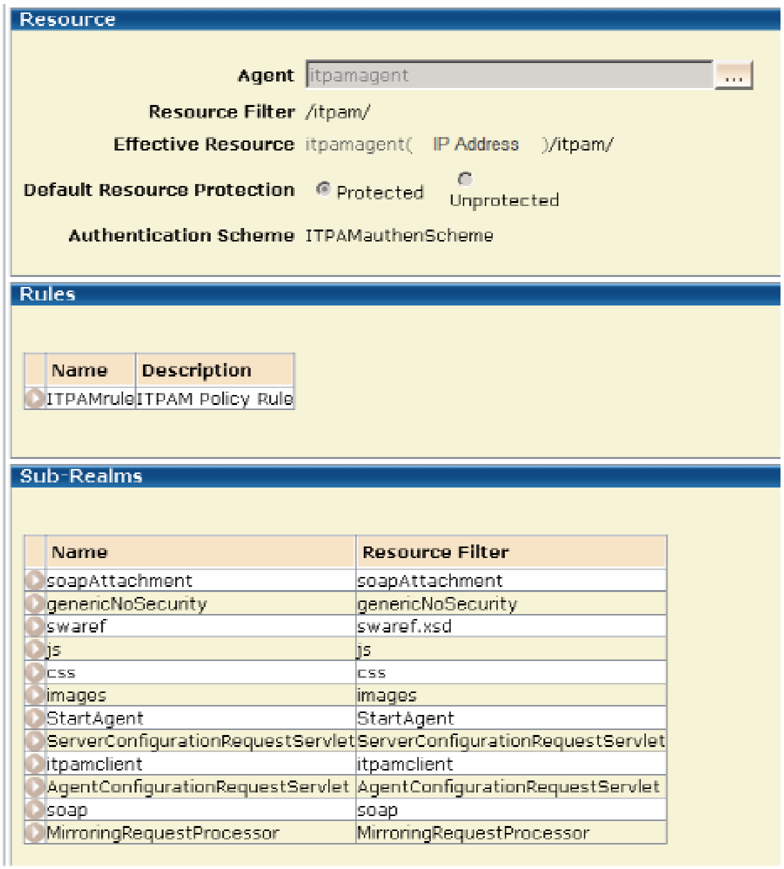
Resource Filter soap

Effective Resource itpamagent(IP Address)/itpam/soap

Default Resource Protection ○ Protected ● Unprotected

Authentication Scheme Basic

When all subrealms are created and changes are saved, the ITPAMdomain shows the following properties:



Resource

Agent itpamagent

Resource Filter /itpam/

Effective Resource itpamagent(IP Address)/itpam/

Default Resource Protection ● Protected ○ Unprotected

Authentication Scheme ITPAMauthenScheme

Rules

Name	Description
ITPAMrule	ITPAM Policy Rule

Sub-Realms

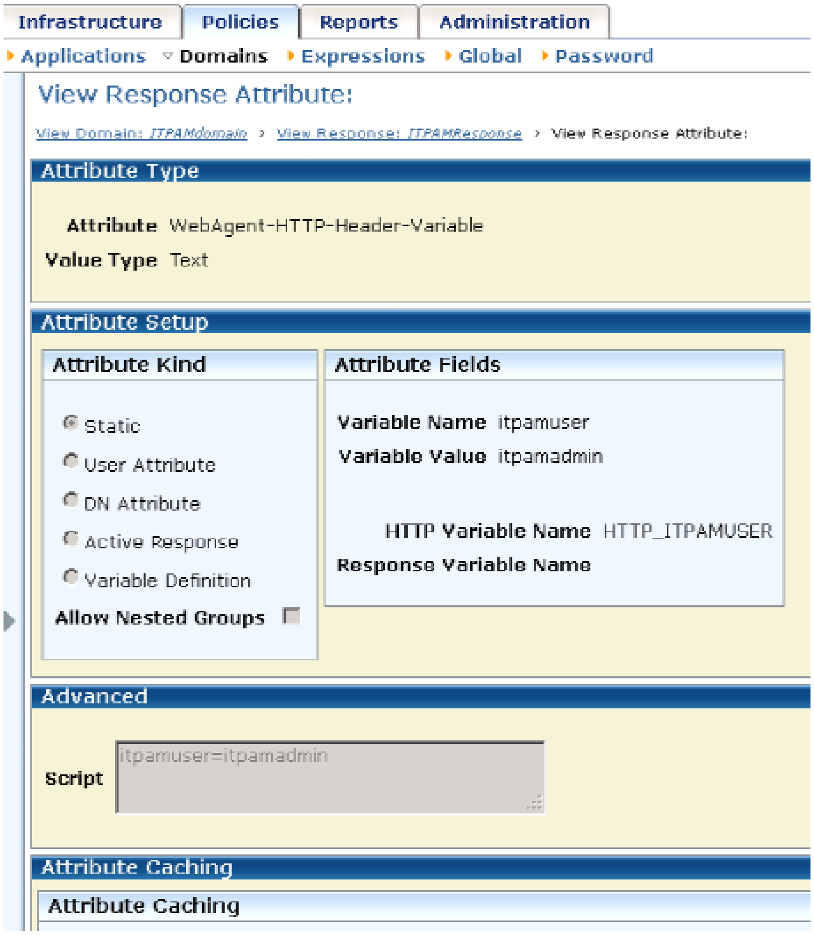
Name	Resource Filter
soapAttachment	soapAttachment
genericNoSecurity	genericNoSecurity
swaref	swaref.xsd
js	js
css	css
images	images
StartAgent	StartAgent
ServerConfigurationRequestServlet	ServerConfigurationRequestServlet
itpamclient	itpamclient
AgentConfigurationRequestServlet	AgentConfigurationRequestServlet
soap	soap
MirroringRequestProcessor	MirroringRequestProcessor

11. (Optional) Create Responses. Follow the instructions for creating a custom response variable in the *CA Process Automation Installation Guide*. Use the variable as the SSO Authentication Parameter. Remember to set the following properties:

    a. Create a custom response attribute named itpamuser of the type WebAgent-HTTP-Header-Variable in CA Process Automation.

    b. Set the Variable Value as the parameter used for LDAP/ActiveDirectory user-ID.

    c. Add this custom response to the rule you created. The response must look similar to the following example.



View Response Attribute:

View Domain: *ITPAMdomain* > View Response: *ITPAMResponse* > View Response Attribute:

Attribute Type

Attribute WebAgent-HTTP-Header-Variable
Value Type Text

Attribute Setup

Attribute Kind

● Static
○ User Attribute
○ DN Attribute
○ Active Response
○ Variable Definition
Allow Nested Groups □

Attribute Fields

Variable Name itpamuser
Variable Value itpamadmin
HTTP Variable Name HTTP_ITPAMUSER
Response Variable Name

Advanced

Script itpamuser=itpamadmin

Attribute Caching

Attribute Caching

Install and Configure CA SiteMinder Web Agent on Apache Load Balancer Server

The Load Balancer runs on the Apache server in our sample architecture. Download and install the CA SiteMinder agent. When installing the agent, select Support for Apache Web server.

The following samples include WebAgent.conf and SmHost.conf SM Web Agent configuration files. You must set these files on the server where Web Agent is installed and registered with the CA SiteMinder Policy server.

Webagent.conf

```
# WebAgent.conf - configuration file for SiteMinder Web Agent
# Web Agent Version = 12QMR3, Build = 256, Update = 00

#agentname="<AgentName>, <IPAddress>"
AgentName="itpamagent,<IP Address>" (name of agent set in SM Policy server and IP address of its host)
HostConfigFile="C:\Program Files\CA\webagent\config\SmHost.conf"
AgentConfigObject="ITPAMagentConfig" (Agent configuration object set in SM policy server)
# DZ: Change to YES in order to enable Web Agent
EnableWebAgent="NO"
ServerPath=""
#localconfigfile="C:\Program Files\Apache Software Foundation\Apache2.2\conf\LocalConfig.conf"
LoadPlugin="C:\Program Files\CA\webagent\bin\HttpPlugin.dll"
#LoadPlugin="C:\Program Files\CA\webagent\bin\Affiliate10Plugin.dll"
#LoadPlugin="C:\Program Files\CA\webagent\bin\SAMLAffiliatePlugin.dll"
#LoadPlugin="C:\Program Files\CA\webagent\bin\eTSSOPlugin.dll"
#LoadPlugin="C:\Program Files\CA\webagent\bin\IntroscopePlugin.dll"
```

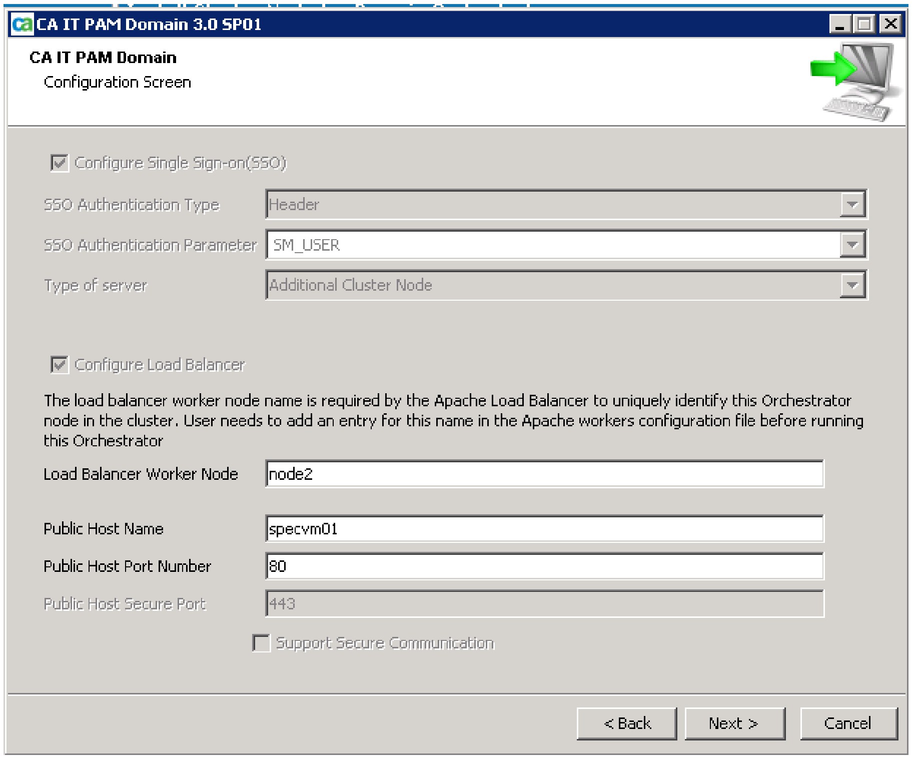
Smhost.conf

```
# Host Registration File - C:\Program Files\CA\webagent\config\SmHost.conf
#
# This file contains bootstrap information required by
# the SiteMinder Agent API to connect to Policy Servers
# at startup. Be sure the IP addresses and ports below
# identify valid listening Policy Servers. Please do not
# hand edit the encrypted SharedSecret entry.
#

hostname="<hostname>" (host name)
sharedsecret="{RC2}5kMYZRiU67HFbZG774UwJF3TZT53X2aN/yMwbMlE8voyJvrvmC7/jnx8DPRHWofaL6CFEh
r3IUcQnZm5BBrYNYDH1OuWama7Y/AGIb4XD44hi9+z4XbsMgs7dVNyGZe8ZyU/N05Wx0nQp/LCXlD/uvixh+HIdU9
NYKIqbTWYnVgemwZGt6xDffAlDHI1or1Q"
sharedsecrettime="0"
enabledynamichco="NO"
hostconfigobject="ITPAMhostConfig"
# Add additional bootstrap policy servers here for fault tolerance.
policyserver="<IP Address>,44441,44442,44443" (SiteMinder policy server IP address)
requesttimeout="60"
cryptoprovider="ETPKI"
fipsmode="COMPAT"

# <EOF>
```

Reinstall CA Process Automation Orchestrator

Follow these steps:

1. Reinstall the CA Process Automation Orchestrator cluster nodes, specifying SSO Authentication parameters as shown in the following example.



CA IT PAM Domain 3.0 SP01

CA IT PAM Domain

Configuration Screen

☑ Configure Single Sign-on(SSO)

SSO Authentication Type: Header

SSO Authentication Parameter: SM_USER

Type of server: Additional Cluster Node

☑ Configure Load Balancer

The load balancer worker node name is required by the Apache Load Balancer to uniquely identify this Orchestrator node in the cluster. User needs to add an entry for this name in the Apache workers configuration file before running this Orchestrator

Load Balancer Worker Node: node2

Public Host Name: specvm01

Public Host Port Number: 80

Public Host Secure Port: 443

□ Support Secure Communication

Note: The SSO Authentication Parameter field is case-sensitive and SM_USER must be specified in all capital letters.

2. Upon completion of the installation wizard, verify that the following SSO settings are present in the OasisConfig.properties files for the CA Process Automation cluster nodes:

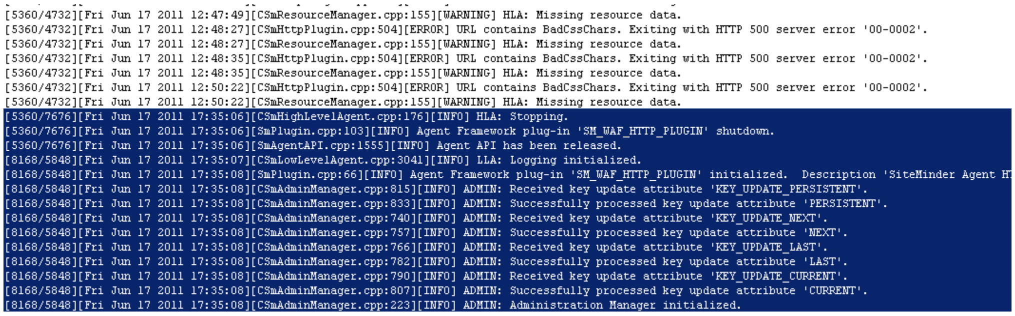
```
ISSSOENABLED=true
SSOAUTHENTICATIONTYPE=HEADER
SSOAUTHENTICATIONPARAM=SM_USER
ALLOW_SSO_LOGOUT=false  //true if we need to see "Sign Out" button on the PAM client
```

Verify that CA SiteMinder Started Logging

Follow these steps:

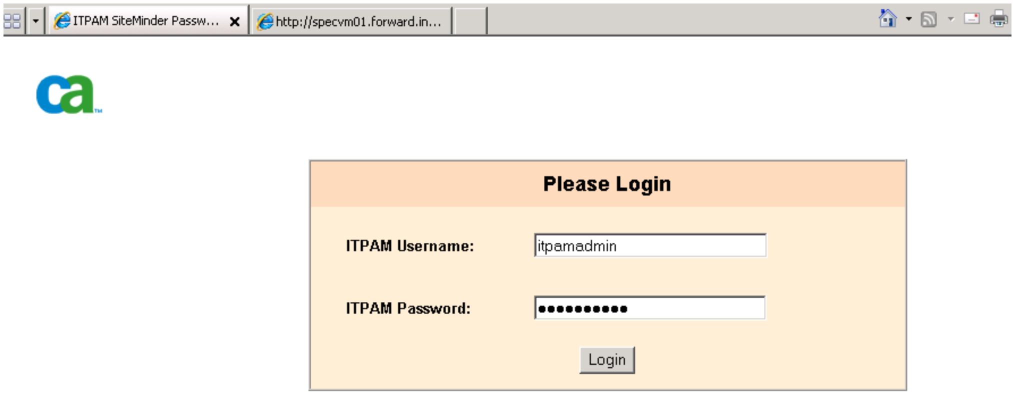
1. Start the CA Process Automation cluster nodes and restart the Apache web service to verify that CA SiteMinder has started logging through its log files.

   If you configured logging for the Web Agent, you will see the following information in the WebAgent.log file:



```
[5360/4732][Fri Jun 17 2011 12:47:49][CSmResourceManager.cpp:155][WARNING] HLA: Missing resource data.
[5360/4732][Fri Jun 17 2011 12:48:27][CSmHttpPlugin.cpp:504][ERROR] URL contains BadCssChars. Exiting with HTTP 500 server error '00-0002'.
[5360/4732][Fri Jun 17 2011 12:48:27][CSmResourceManager.cpp:155][WARNING] HLA: Missing resource data.
[5360/4732][Fri Jun 17 2011 12:48:35][CSmHttpPlugin.cpp:504][ERROR] URL contains BadCssChars. Exiting with HTTP 500 server error '00-0002'.
[5360/4732][Fri Jun 17 2011 12:48:35][CSmResourceManager.cpp:155][WARNING] HLA: Missing resource data.
[5360/4732][Fri Jun 17 2011 12:50:22][CSmHttpPlugin.cpp:504][ERROR] URL contains BadCssChars. Exiting with HTTP 500 server error '00-0002'.
[5360/4732][Fri Jun 17 2011 12:50:22][CSmResourceManager.cpp:155][WARNING] HLA: Missing resource data.
[5360/7676][Fri Jun 17 2011 17:35:06][CSmHighLevelAgent.cpp:176][INFO] HLA: Stopping.
[5360/7676][Fri Jun 17 2011 17:35:06][SmPlugin.cpp:103][INFO] Agent Framework plug-in 'SM_WAF_HTTP_PLUGIN' shutdown.
[5360/7676][Fri Jun 17 2011 17:35:06][SmAgentAPI.cpp:1555][INFO] Agent API has been released.
[8168/5848][Fri Jun 17 2011 17:35:07][CSmLowLevelAgent.cpp:3041][INFO] LLA: Logging initialized.
[8168/5848][Fri Jun 17 2011 17:35:08][SmPlugin.cpp:66][INFO] Agent Framework plug-in 'SM_WAF_HTTP_PLUGIN' initialized.  Description 'SiteMinder Agent H
[8168/5848][Fri Jun 17 2011 17:35:08][CSmAdminManager.cpp:815][INFO] ADMIN: Received key update attribute 'KEY_UPDATE_PERSISTENT'.
[8168/5848][Fri Jun 17 2011 17:35:08][CSmAdminManager.cpp:833][INFO] ADMIN: Successfully processed key update attribute 'PERSISTENT'.
[8168/5848][Fri Jun 17 2011 17:35:08][CSmAdminManager.cpp:740][INFO] ADMIN: Received key update attribute 'KEY_UPDATE_NEXT'.
[8168/5848][Fri Jun 17 2011 17:35:08][CSmAdminManager.cpp:757][INFO] ADMIN: Successfully processed key update attribute 'NEXT'.
[8168/5848][Fri Jun 17 2011 17:35:08][CSmAdminManager.cpp:766][INFO] ADMIN: Received key update attribute 'KEY_UPDATE_LAST'.
[8168/5848][Fri Jun 17 2011 17:35:08][CSmAdminManager.cpp:782][INFO] ADMIN: Successfully processed key update attribute 'LAST'.
[8168/5848][Fri Jun 17 2011 17:35:08][CSmAdminManager.cpp:790][INFO] ADMIN: Received key update attribute 'KEY_UPDATE_CURRENT'.
[8168/5848][Fri Jun 17 2011 17:35:08][CSmAdminManager.cpp:807][INFO] ADMIN: Successfully processed key update attribute 'CURRENT'.
[8168/5848][Fri Jun 17 2011 17:35:08][CSmAdminManager.cpp:223][INFO] ADMIN: Administration Manager initialized.
```

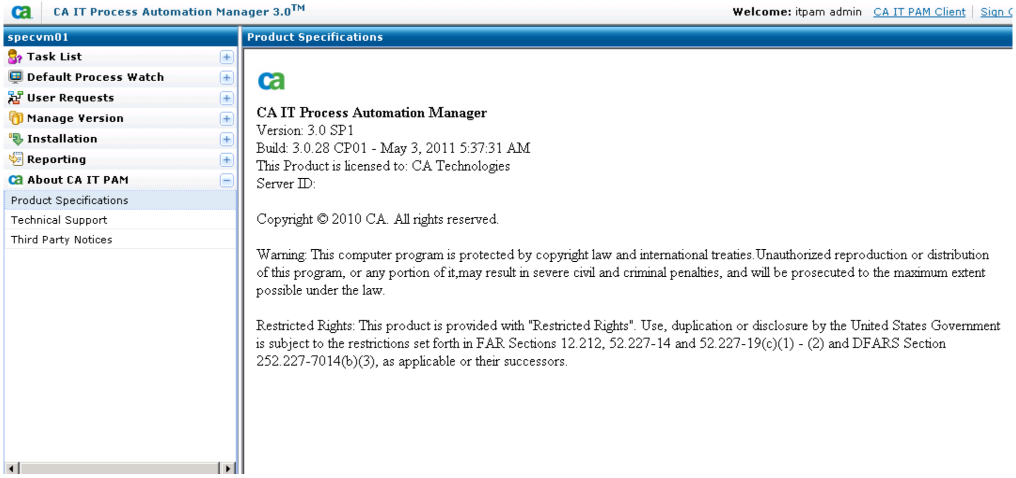
   When you navigate to the CA Process Automation Web user interface entry URL on the Apache Load Balancer server, you will see the CA SiteMinder login prompt. The following example shows the CA SiteMinder login page for CA Process Automation.



ITPAM Username: itpamadmin

ITPAM Password: •••••••••••

After you log in (using credentials of LDAP users that were also linked to respective ITPAMUsers /ITPAMAdmin groups in CA EEM), the CA Process Automation home page opens. This step may take some time to complete.



CA IT Process Automation Manager
Version: 3.0 SP1
Build: 3.0.28 CP01 - May 3, 2011 5:37:31 AM
This Product is licensed to: CA Technologies
Server ID:

Copyright © 2010 CA. All rights reserved.

Warning: This computer program is protected by copyright law and international treaties.Unauthorized reproduction or distribution of this program, or any portion of it,may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

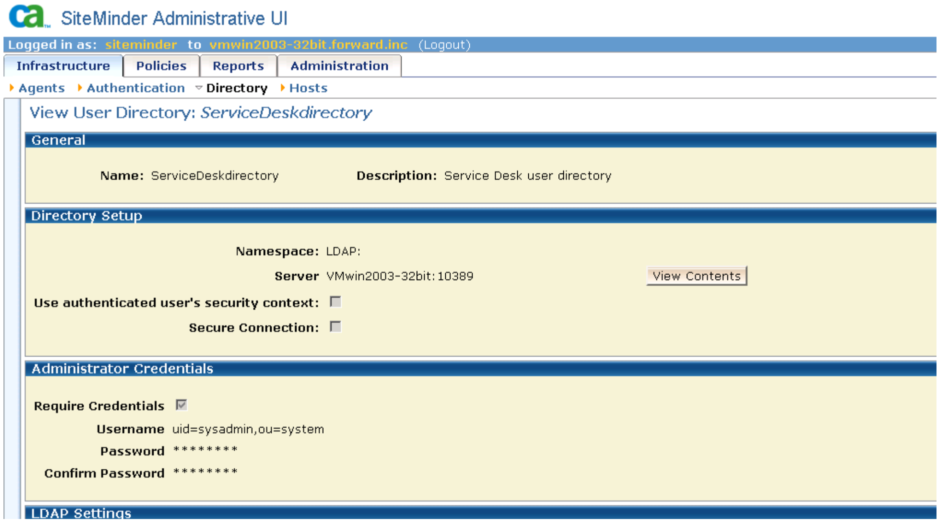
Restricted Rights: This product is provided with "Restricted Rights". Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14 and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable or their successors.

Note: The login page will not appear when you open subsequent browser windows (with cookies supported) or while using the same URL.

Integration between CA SDM and CA Process Automation Protected by CA SiteMinder Web Agents

Similar to the CA Process Automation single sign-on that was described previously, you can configure single sign-on for CA SDM with WebAgent for IIS. In this case, CA SDM must be configured to use the IIS-based user interface on port 80.

- You must create similar Policy Server entries (such as Agent, Agent configuration, User Directory, Domain with Policies and Realms) for the CA SiteMinder Policy server. The user directory for that Domain will point to the same LDAP server that was used for the CA Process Automation Policy and use the same settings as shown in the following example.


SiteMinder Administrative UI
Logged in as: siteminder to vmwin2003-32bit.forward.inc (Logout)
Infrastructure
Policies
Reports
Administration
Agents
Authentication
Directory
Hosts
View Contents

View User Directory: *ServiceDeskdirectory*

General

Name: ServiceDeskdirectory **Description:** Service Desk user directory

Directory Setup

Namespace: LDAP:
Server VMwin2003-32bit:10389
Use authenticated user's security context: ☐
Secure Connection: ☐

Administrator Credentials

Require Credentials ☑
Username uid=sysadmin,ou=system
Password ********
Confirm Password ********

LDAP Settings

- With proper configuration, the users from the LDAP directory who are also configured as contacts in CA SDM must be able to log in to CA SDM through the SSO Web Agent login.

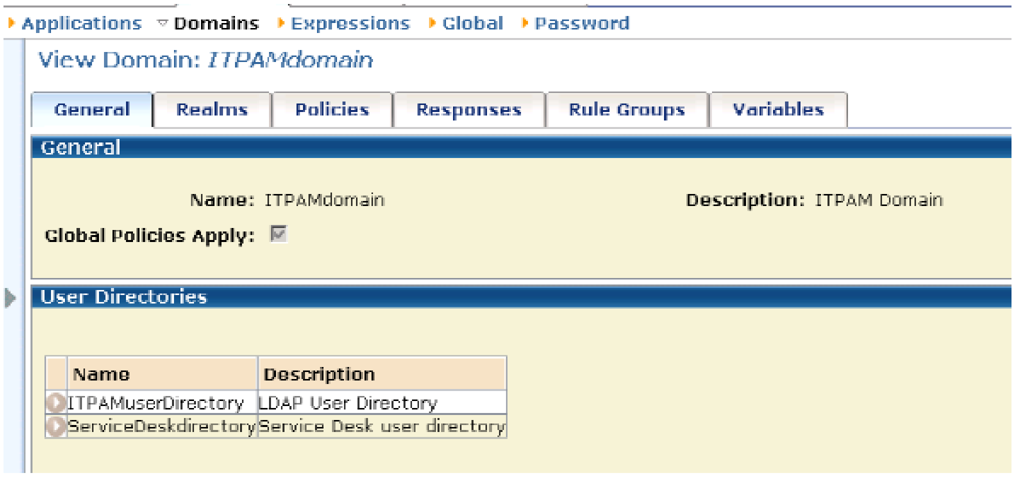
- Install Option Manager values for the CA Process Automation Workflow to enable interface level integration between CA SDM and CA Process Automation and to navigate between change categories that are associated with CA Process Automation process definitions. For more information about installing Option Manager with the required options, see the CA Process Automation integration chapter in the *CA Service Desk Manager Integration Best Practices* Green Book, Volume 2.
    - The same CA EEM hostname that is used for CA Process Automation authentication or authorization services must be specified in these options.
    - Also, under the Option Manager Security node, the settings that define CA EEM for authentication/authorization must have the same CA EEM host.

Enable SSO between CA SDM and CA Process Automation

After you enable SSO between CA SDM and CA Process Automation, you can launch the CA Process Automation web user interface and client from the links on the CA SDM ticket without providing authentication to access CA Process Automation.

Follow these steps:

1. Verify that the ITPAMDomain that was configured previously has access to the user directories of *both* CA SDM and CA Process Automation. The following example shows that the CA Process Automation domain has access to both CA SDM and CA Process Automation user directories.



Name: ITPAMdomain

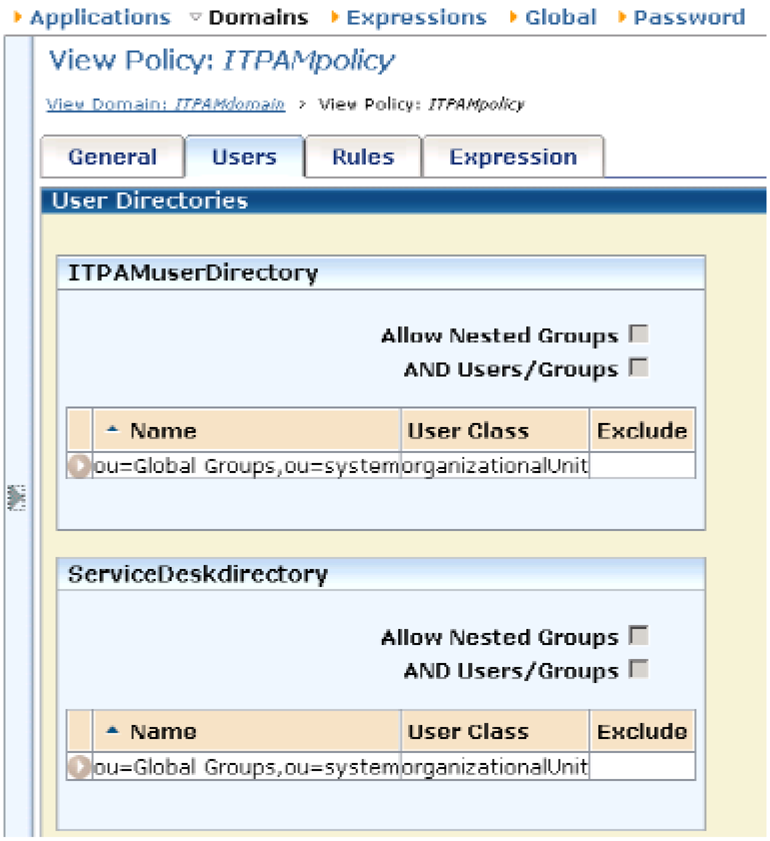
Description: ITPAM Domain

Global Policies Apply: ☑

User Directories

Name	Description
ITPAMuserDirectory	LDAP User Directory
ServiceDeskdirectory	Service Desk user directory

2. Add users from ServiceDeskdirectory to the ITPAMpolicy in the ITPAMDomain as shown in the following example.



View Policy: *ITPAMpolicy*

View Domain: *ITPAMdomain* > View Policy: *ITPAMpolicy*

User Directories

ITPAMuserDirectory

Allow Nested Groups □

AND Users/Groups □

	Name	User Class	Exclude
	ou=Global Groups,ou=system	organizationalUnit	

ServiceDeskdirectory

Allow Nested Groups □

AND Users/Groups □

	Name	User Class	Exclude
	ou=Global Groups,ou=system	organizationalUnit	

Adding the user directories to the same domain is important for the following reasons:

- A user from one user directory is considered different from another, even if the user name is the same. This difference is to prevent Jim@abc.com from being able to impersonate Jim@xyz.com.

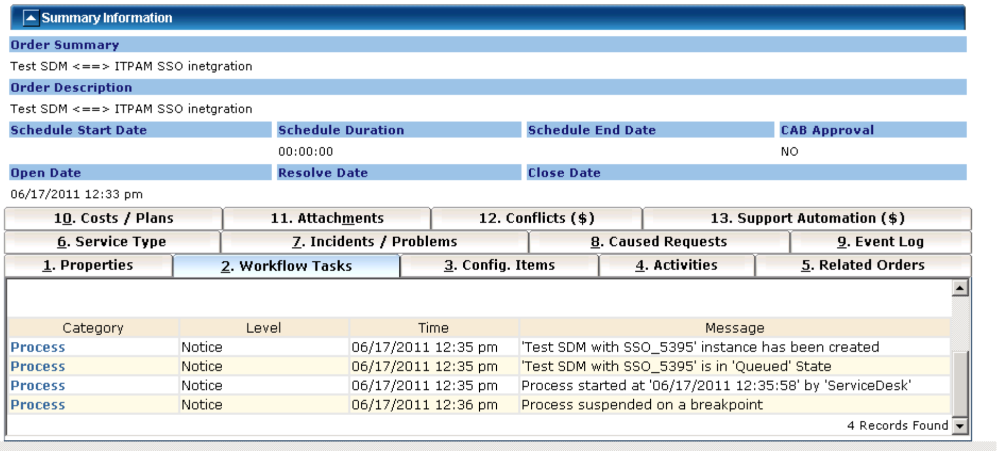
- When a user logs in to CA SDM through the SSO credential collector, the user is authenticated to the ServiceDeskdirectory since it is a part of the CA SDM realm.

- When that same user navigates to the ITPAMdomain, access is rejected and the user is redirected to the CA SiteMinder credential collector (SSO login page). The access is rejected because the users in the ServiceDesk directory are not originally defined in the ITPAMdomain/policy.

After you add both user directories to the ITPAMdomain, users from the ServiceDesk directory are authorized to access the ITPAMrealm and will not be prompted for another login.

3. Apply the settings to the ITPAMdomain defined in the CA SiteMinder Policy Server and clear the cache.

   The users must now be able to navigate from the CA SDM ticket to the CA Process Automation web user interface using Process links in CA SDM.



Summary Information

Order Summary

Test SDM <==> ITPAM SSO inetgration

Order Description

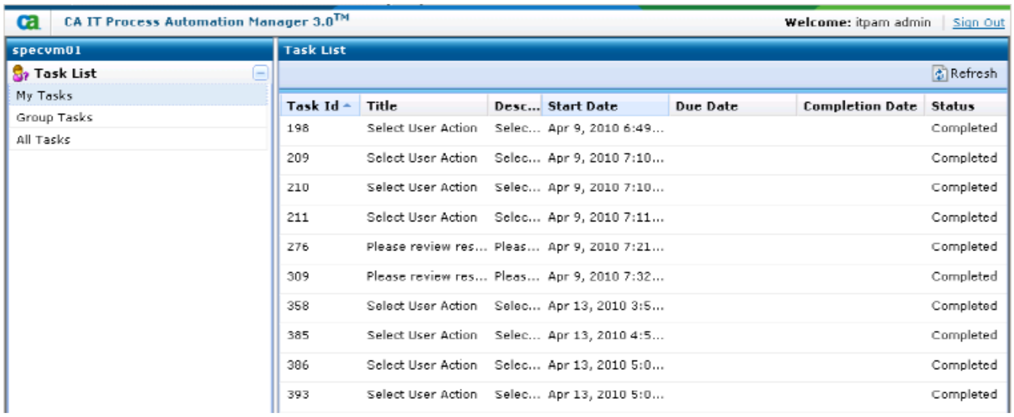
Test SDM <==> ITPAM SSO inetgration

Schedule Start Date	Schedule Duration	Schedule End Date	CAB Approval
	00:00:00		NO

Open Date	Resolve Date	Close Date
06/17/2011 12:33 pm		

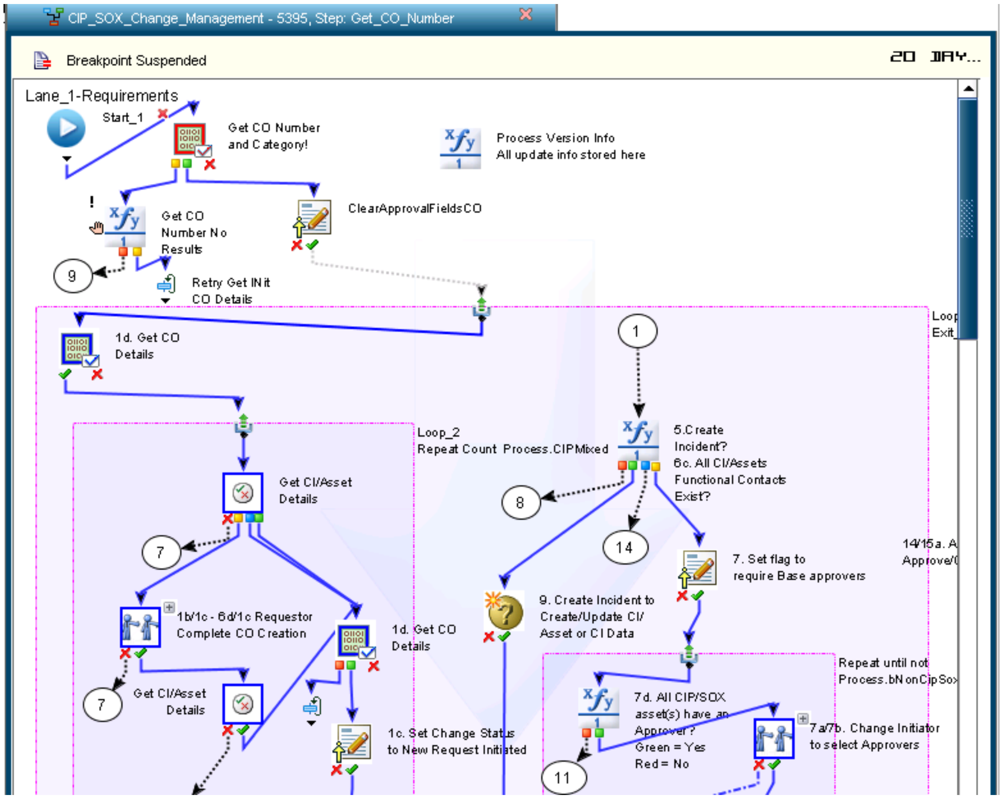
Category	Level	Time	Message
Process	Notice	06/17/2011 12:35 pm	'Test SDM with SSO_5395' instance has been created
Process	Notice	06/17/2011 12:35 pm	'Test SDM with SSO_5395' is in 'Queued' State
Process	Notice	06/17/2011 12:35 pm	Process started at '06/17/2011 12:35:58' by 'ServiceDesk'
Process	Notice	06/17/2011 12:36 pm	Process suspended on a breakpoint

4 Records Found



Task Id	Title	Desc...	Start Date	Due Date	Completion Date	Status
198	Select User Action	Selec...	Apr 9, 2010 6:49...			Completed
209	Select User Action	Selec...	Apr 9, 2010 7:10...			Completed
210	Select User Action	Selec...	Apr 9, 2010 7:10...			Completed
211	Select User Action	Selec...	Apr 9, 2010 7:11...			Completed
276	Please review res...	Pleas...	Apr 9, 2010 7:21...			Completed
309	Please review res...	Pleas...	Apr 9, 2010 7:32...			Completed
358	Select User Action	Selec...	Apr 13, 2010 3:5...			Completed
385	Select User Action	Selec...	Apr 13, 2010 4:5...			Completed
386	Select User Action	Selec...	Apr 13, 2010 5:0...			Completed
393	Select User Action	Selec...	Apr 13, 2010 5:0...			Completed

4. Click View Process on the Workflow Tasks tab in CA SDM to launch the CA Process Automation client. The workflow process diagram is displayed as shown in the following example.


CIP_SOX_Change_Management - 5395, Step: Get_CO_Number
Breakpoint Suspended
Lane_1-Requirements
Start_1
Get CO Number and Category!
Process Version Info
All update info stored here
Get CO Number No Results
ClearApprovalFieldsCO
9
Retry Get INit CO Details
1d. Get CO Details
1
Loop Exit
Loop_2
Repeat Count Process.CIPMixed
5.Create Incident?
6c. All CI/Assets Functional Contacts Exist?
Get CI/Asset Details
8
7
14
7. Set flag to require Base approvers
14/15a. A Approve/
1b/1c - 6d/1c Requestor Complete CO Creation
1d. Get CO Details
9. Create Incident to Create/Update CI/ Asset or CI Data
Repeat until not Process.bNonCipSox
Get CI/Asset Details
7
7d. All CIP/SOX asset(s) have an Approver?
Green = Yes
Red = No
7a/7b. Change Initiator to select Approvers
1c. Set Change Status to New Request Initiated
11

Integration Summary

The integration of CA SDM, CA SiteMinder, CA EEM, and CA Process Automation allows for an end-to-end Single Sign-on functionality.

Configuring IIS to Redirect Traffic to Tomcat

This section describes how to configure IIS to redirect traffic to Tomcat, so that the CA SiteMinder IIS agent can be used for CA Process Automation. These instructions are valid for a Windows environment using IIS 6.0. Some IIS configuration steps change slightly when older versions of IIS are used, but the high-level steps are the same.

Note: The configuration steps are not necessary for CA SDM. CA SDM can be configured to use IIS as a web server by running pdm_configure on the CA SDM Primary server.

Prerequisites for the configuration

Before you configure IIS, verify that the following prerequisites are met:

- IIS is installed and working.
- CA Process Automation is installed and working with Tomcat as the web server.

Configure IIS to Redirect to Tomcat

Follow these steps:

1. Verify that the IIS web server is installed and working.
2. Locate the folder TomcatRedirector.
3. Copy the folder TomcatRedirector (TomcatRedirector.zip) to the computer where IIS is installed, preferably to the C:\Program Files\CA\SharedComponents folder.
4. Edit the isapi_redirect.properties file in the bin directory to reflect the correct path for the parameters extension_uri, worker_file, worker_mount_file (if the path is not correct). The following excerpt is from a sample isapi_redirect.properties file.

```
# Configuration file for the Jakarta ISAPI Redirector
# The path to the ISAPI Redirector Extension, relative to the website
#This must be in a virtual directory with execute privileges. For example, "TomcatRedirector"
listed below in the extension_uri path would be the name of the virtual directory.
extension_uri=/TomcatRedirector/isapi_redirect.dll
# Full path to the log file for the ISAPI Redirector
log_file=C:\Program Files\CA\SharedComponents\TomcatRedirector\logs\isapi_redirect.log
# Log level (debug, info, warn, error or trace)
log_level=error
# Full path to the workers.properties file
worker_file=c:\Program
Files\CA\SharedComponents\TomcatRedirector\conf\workers.properties
# Full path to the uriworkermap.properties file\
worker_mount_file=c:\Program
Files\CA\SharedComponents\TomcatRedirector\conf\uriworkermap.properties
```

5. Modify the host name in the ...\TomcatRedirector\conf\workers.properties file to reflect the correct host name. Replace the references to localhost. The following excerpt is from a sample workers.properties file.

   ```
   # statement and uncomment the three worker.ajp13w02 lines.
   ######################################################################
   # The workers that jk should create and work with
   worker.list=ajp13w01
   # Defining a worker named ajp13w01 and of type ajp13
   # Note that the name and the type do not have to match.
   worker.ajp13w01.type=ajp13
   worker.ajp13w01.host=<Hostname where ITPAM is Installed>
   worker.ajp13w01.port=8009
   ```

6. Open the IIS Manager console and perform the following steps:

   a. Right-click the Default Web Site, and select New Virtual Directory.

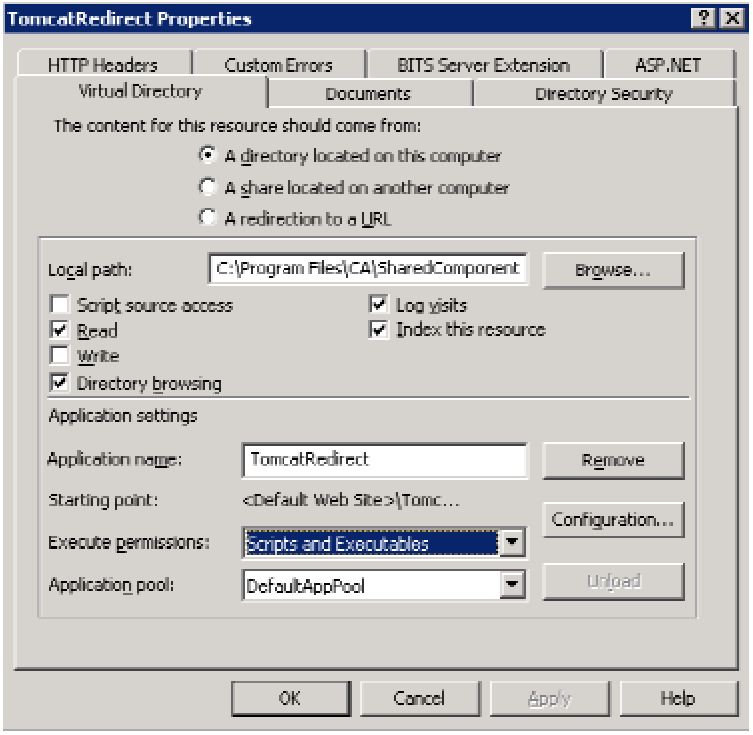
   b. Enter the path to the TomcatRedirector\bin folder.

   c. Select the Run scripts and Execute permissions.

7. Modify the security for the TomcatRedirector\logs folder (in Windows Explorer) and give full permissions for the log file to the Network Service user.

8. Right-click the newly created virtual directory and select Properties.

9. Select Scripts and Executables in the Execute permissions field as shown in the following example and click OK.



TomcatRedirect Properties

The content for this resource should come from:

● A directory located on this computer

○ A share located on another computer

○ A redirection to a URL

Local path: C:\Program Files\CA\SharedComponent

□ Script source access

☑ Read

□ Write

☑ Directory browsing

☑ Log visits

☑ Index this resource

Application settings

Application name: TomcatRedirect

Starting point: <Default Web Site>\Tomc...

Execute permissions: Scripts and Executables

Application pool: DefaultAppPool

10. Add a Web Service Extension in IIS using the following steps:

    a. Right-click Web Service Extensions.

    b. Enter an extension name that matches the virtual directory that was created previously, for example, TomcatRedirector.

11. Browse to the TomcatRedirector\bin\isapi_redirect.dll file in the Required fields window and provide the following information:

    – Select the Set Extension Status to Allowed option.

    – Select WWW Publishing Service in the Recycle IIS Admin Service field.

12. Open the IIS Manager tool, right-click the Web Sites folder, and select Properties.

13. Click the ISAPI Filters tab and add and select isapi_redirect.dll as the Executable.

14. Verify that the requests are being forwarded to Tomcat by connecting to CA Process Automation on port 80.